TABLE OF CONTENTS

INTRODUCTION

1. What is the HIPAA Privacy Rule? To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") was enacted by Congress. HIPAA included what are called "Administrative Simplification" provisions that required the U.S. Department of Health and Human Services ("**HHS**") to adopt national standards for electronic health care transactions, such as health care claims that are filed electronically. Congress mandated the adoption of the HIPAA Standards for Privacy of Individually Identifiable Health Information ("**Privacy Rule**" or **"Rule**") because advances in electronic technology could make it difficult to protect the privacy of health information. Congress subsequently enacted the HIPAA Security Rule ("**Security Rule**") and, more recently, the Health Information Technology for Economic and Clinical Health ("**HITECH**") Act. In addition, the State of Texas has enacted laws regarding patient privacy and protected use and disclosure of patient health information numbers, including the Texas Health and Safety Code Chapters 181 and 182 and Texas Business and Commerce Code Section 521, both as amended by HB 300 (82nd Legislature) effective September 1, 2012, including any implementing regulations (collectively, "**Texas Law**"). The state laws do not replace other federal, state or other laws that give individuals even greater privacy protections, and are not pre-empted by the Privacy Rule.

The Privacy Rule establishes national protections for the privacy of Protected Health Information ("**PHI**"), and applies to three types of HIPAA covered entities: health plans, health care clearinghouses, and health care providers, like The Kingsley Clinic PLLC ("**Practice**"), which conduct certain health care transactions electronically. The Rule requires that Covered Entities implement policies and procedures to protect and guard against the misuse of PHI. This HIPAA Privacy Policy & Procedure Manual ("**Privacy Manual**") reflects our commitment to compliance with the Privacy Rule.

2. Privacy Officer. The Privacy Rule requires that we designate a person who will serve as the "Privacy Officer" and who is responsible for the development and implementation of our privacy policies and procedures. We must also designate a person to serve as the contact person responsible for receiving complaints under the Privacy Rule and who can make further information available to patients about matters covered by our Notice of Privacy Practices.

We have designated a Privacy Officer for Practice, to be responsible for the development and implementation of our privacy policies and procedures, and to be the contact person to answer questions and receive complaints related to our privacy practices.

3. Definitions. Every staff person at Practice should review and consult the Glossary of Terms contained in this Privacy Manual when reviewing or consulting this Privacy Manual as capitalized words not otherwise defined in a policy are defined in the Glossary of Terms.

4. **What does HIPAA Privacy mean to Practice and our Workforce?** Each staff member of our Workforce needs to understand what our basic privacy policies and procedures are and how to request help if further information is needed. We will make a copy of this Privacy Manual available to each staff member of our Workforce and require that each member review it and participate in the training we offer on the Privacy Rule. If the Privacy Rule changes, or new guidance is issued that requires a change in this Privacy Manual, we will have each member of our Workforce review the changed policies. Together we will commit to providing quality health care to our patients, while maintaining the privacy of their protected health information and complying with the Privacy Rule.

PRIVACY OFFICER
APPOINTMENT AND ACCEPTANCE

The Privacy Officer is the chief compliance officer responsible for the development and implementation of policies and procedures required to ensure that Practice complies with the requirements of applicable Federal and State laws relating to the protection of private patient information.

Practice desires to appoint you to serve as the Privacy Officer. Accordingly, your signature indicates you have reviewed the statements below and accept the appointment as Privacy Officer.

1. I acknowledge and agree that I have: (i) been provided a copy of Practice's HIPAA Privacy Policy & Procedure Manual, including the Privacy Officer Job Description, and reviewed it in its entirety, (ii) been given the opportunity to ask questions, and (iii) had all my questions answered to my satisfaction.

2. I acknowledge, accept and consent to the appointment to serve as the Privacy Officer for Practice and understand that I will serve as the Privacy Officer at the discretion of Practice's management.

3. I agree to use my best efforts to fulfill the duties described in the Privacy Officer Job Description for as long as I remain the Privacy Officer.

APPOINTED OFFICER:	**EFFECTIVE DATE:**
OFFICER SIGNATURE:	

PRIVACY OFFICER JOB DESCRIPTION

The Privacy Officer is the chief compliance officer responsible for the development and implementation of policies and procedures required to ensure that Practice complies with the requirements of applicable Federal and State laws relating to protection of PHI. The Privacy Officer may delegate any task required in this Privacy Manual but will provide proper supervision to ensure the policies and procedures contained in this Privacy Manual are followed. The Privacy Officer retains the ultimate responsibility for the development and implementation of policies and procedures in this Privacy Manual.

1. Responsibilities The Privacy Officer's responsibilities include:

(a) Acting as Practice's primary contact for questions or issues relating to PHI or the policies and procedures described in this Privacy Manual and addressing such questions or issues timely, coordinating with Practice's management and legal counsel as necessary.

(b) Developing, documenting, communicating and implementing the policies and procedures described in this Privacy Manual in cooperation with Practice's management.

(c) Ensuring requests from individuals relating to their PHI are timely and properly fulfilled in accordance with this Privacy Manual.

(d) Receiving, reviewing, investigating and documenting all reported or suspected incidents of improper use or disclosure of PHI or breach of security compromising PHI, regardless of source or severity.

(e) Developing, documenting, and conducting training programs to educate all Practice Staff and new hires on the policies and procedures contained in this Privacy Manual.

(f) Establishing appropriate sanctions for violations of the policies and procedures in this Privacy Manual and ensuring sanctions are consistently applied to all qualifying instances, coordinating with Practice's management and legal counsel as necessary.

(g) Coordinating with the Security Officer to ensure that all privacy policies are aligned with the security policies.

(h) Conducting annual (or quarterly or bi-annual) audits of the policies and procedures in this Privacy Manual and developing and implementing updates as necessary to reflect changes in the law or circumstances.

2. Qualifications The Privacy Officer must:

(a) Possess a thorough understanding of Practice's operations and have access to Practice's management.

(b) Be readily available to Practice staff and individuals in order to answer questions or address any PHI-related issues.

(c) Have the capacity to continually implement, review, update and document the policies and procedures in this Privacy Manual.

(d) Possess superior organizational, communication and leadership skills.

(e) Possess knowledge of and experience with HIPAA and the policies and procedures in this Privacy Manual.

POLICIES

NOTICE OF PRIVACY PRACTICES

Policy Number 1
HIPAA §§ 164.520, 514

PURPOSE: Establish a Policy for Notifying Patients of our Privacy Practices

APPROVED: _____ **DATE:** _____, 2019

Policy: The HIPAA Privacy Rule provides that patients have a right to notice of how we may use and disclose a patient's PHI and e-PHI, as well as the patient's rights and our obligations regarding their PHI and e-PHI. We have developed a Notice of Privacy Practices ("**Notice**") to meet these requirements and will make the Notice available to our patients as described in this policy. Practice will strive to abide by the terms of our Notice as currently in effect.

Procedure:

1. **Content of Notice.** Our Notice has been written in plain language to contain all of the elements required by the Privacy Rule, including the following:

   (a) A description of how we use and disclose patients' PHI, including:

      (1) A description, with at least one example, of the types of uses and disclosures that we are permitted to make for treatment and health care operations;

      (2) A description of each of the other purposes for which we are permitted or required by HIPAA to use or disclose PHI without the patient's written authorization;

   (b) A statement that other uses and disclosures will be made only with the patient's written authorization (see Policy No. 3 in this Privacy Manual), including;

      (1) A description of the most uses and disclosures of psychotherapy notes;

      (2) A description of the uses and disclosures of PHI for marketing purposes;

      (3) A description of disclosures of PHI that constitute a sale.

   (c) If applicable to our operations, a statement that we may use or disclose certain PHI for fundraising communications but that the patient will have the opportunity to opt out of future fundraising communications as specified in the communication made to the patient;

   (d) A description of the individual rights of our patients regarding access and control of their PHI, and how a patient may exercise those rights, including:

(1) The right to request restrictions on certain uses and disclosures and whether Practice is required to agree to a requested restriction, including agreeing to the request of a patient to restrict disclosure of PHI about him/her to a health plan if the disclosure is for the purpose of carrying out health care operations and is not otherwise required by law and the PHI pertains solely to a health care item or service for which the patient, or person other than the health plan, has paid us in full for the item or service;

(2) The right to receive certain confidential communications;

(3) The right to inspect and obtain a copy of PHI;

(4) The right to request an amendment of PHI;

(5) The right to receive an accounting of certain disclosures of PHI;

(6) The right to revoke an authorization;

(7) A description of our complaint procedure for addressing problems the patient may have with our privacy practices;

(8) The right to obtain a paper copy of the Notice, upon request;

(9) If we maintain an electronic health record, the right to: a) access to or obtain a copy of PHI in an electronic form and format requested by the patient, if it is readily producible or, if not, in a readable electronic form and format as agreed to between us and the patient; b) have us transmit such copy directly to a person or entity the patient designates, provided that choice is clear, conspicuous, and specific; c) request that we provide an accounting of the disclosures we have made of the patient's PHI (including disclosures related to treatment and health care operations) contained in an electronic health record for no more than 3 years prior to the date of the request (and depending on when we acquired an electronic health record); and

(10) Notice of any allowed fees related to the above;

(e) A description of our legal duties regarding PHI, including our legal obligation to maintain the privacy of PHI and our obligation to notify affected individuals following a breach of their unsecured PHI;

(f) Identification of the individual at Practice a patient may contact for more information about our privacy practices; and

(g) The effective date of the Notice and any revisions of the Notice, with the effective date of such revisions.

2. Providing the Notice

(a) We will present the Notice to each patient at their first date of service delivery by us and will make a good faith attempt to obtain each patient's acknowledgment of receipt of the Notice.

(1) We will have a patient acknowledge receipt by signing an acknowledgment form.

(2) If the patient refuses to provide such acknowledgment, we will document in the patient's chart our efforts to obtain the patient's acknowledgment and the reason why the acknowledgment was not obtained.

(3) If there is an emergency treatment situation, we will provide the Notice to the patient as soon as reasonably practicable after the emergency situation. No acknowledgment of receipt of the Notice need be obtained in an emergency situation.

(b) We will post our entire current Notice in a prominent location in our office(s).

(c) We will provide a paper copy of the Notice upon a patient's request.

(d) When our first treatment encounter with a patient is not face-to face, we will follow the following procedures:

(1) If we first treat a patient over the telephone (not simply obtain information to schedule an appointment or procedure), we will mail the Notice to the patient the same day, if possible, with a request to sign an enclosed acknowledgment and return it to our office. We will maintain a file copy of the acknowledgment form sent to the patient as documentation of our efforts to obtain the patient's acknowledgment, in case the patient fails to return the acknowledgment form.

(2) We may e-mail our Notice to a patient if the patient agrees to receive an electronic notice. An electronic return receipt will serve as the patient's acknowledgment of receipt of the Notice.

(3) If our first service delivery to a patient is provided over the Internet, through e-mail, or otherwise electronically, we will send an electronic notice automatically and contemporaneously in response to the patient's first request for service. An electronic return receipt will serve as the patient's acknowledgment of receipt of the Notice.

(e) If the patient has a personal representative acting on the patient's behalf at the time Notice is provided, we will provide the Notice to the representative and make a good faith effort to obtain the representative's acknowledgment of receipt of the Notice.

3. Revisions to our Notice

(a) Practice will advise patients in the Notice that we reserve the right to change the terms of the Notice and to make the new Notice provisions effective for all PHI that we maintain.

(b) We will review our Notice at least annually. If we determine at any time that there is a material change to our privacy practices, or there is a change in law that requires a change in our Notice, we will revise our Notice, date it with the effective date of the revision, post the revised Notice in our office(s), then implement the changes (unless a change in law requires that we implement the change sooner), and provide the revised Notice pursuant to this policy. We will advise patients in our Notice that they can obtain a revised Notice upon request on or after the effective date of any revision. No acknowledgement is necessary for providing a revised Notice to a patient who has received a prior version of our Notice. Patients can access our revised Notice on our website, if we maintain one.

4. Documentation

(a) The Privacy Officer will maintain a file containing a copy of our Notice and every revised Notice that is issued by Practice.

(b) We will place in the patient's medical record a copy of the acknowledgment of receipt (which will also contain a reference to the version of the Notice they received), whether provided by hard copy or electronically, or documentation of our good faith efforts to obtain such written acknowledgment.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION NOT REQUIRING PATIENT AUTHORIZATION

Policy Number 2
HIPAA §§ 164.502, 506, 512, 514

PURPOSE: Establish a Policy for the Use and Disclosure of PHI without Patient Authorization

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice may use and disclose PHI in certain situations where it is not necessary to obtain the patient's authorization, as allowed under the Privacy Rule. We will follow Policy No. 4 in this Privacy Manual (regarding application of the Minimum Necessary principle) whenever using or disclosing PHI without patient authorization.

Procedure: In the following situations, Practice may use or disclose PHI without obtaining the patient's authorization:

1. <u>For Treatment or Health Care Operations:</u>

(a) A patient's authorization is not required when we use or disclose the patient's PHI for our purposes in order to treat the patient or conduct our own business operations, including disclosure to our business associates (as further described in this Privacy Manual).

(1) A patient is permitted to request, in writing, that we restrict the uses or disclosures of his or her PHI for treatment or health care operations, or when disclosing information to persons involved in the patient's care, or for notification purposes. Except as set forth below, we are not required to agree to the patient's request, but we are bound by any restrictions to which we agree unless and until we withdraw from such agreement, where permitted. Such requests will be directed to the Privacy Officer.

(2) A patient is permitted to request, in writing, that the patient receive communications of PHI from us by alternative means or at alternative locations (other than the usual way we send communications to our patients). We must accommodate a patient's reasonable request for such confidential communications. Such requests will be directed to the Privacy Officer.

(3) Special rules apply if we intend to use the PHI for marketing purposes or if we intend to use PHI in a manner that would be considered a Sale of PHI (see Glossary of Terms). Such cases will be referred to the Privacy Officer.

(b) We may disclose PHI for the treatment activities of another health care provider. Where PHI is disclosed to, or requested by, other health care providers for Treatment purposes, our minimum necessary policy (see Policy No. 4 in this Privacy Manual) does not apply.

(c) Any use or disclosure of PHI for Treatment or Health Care Operations must be consistent with our current Notice of Privacy Practices.

2. **Required Uses and Disclosures Not Requiring Patient Authorization** Other than for disclosures to the patient, no disclosure under this Section 2 will be made without the prior review and approval of the Privacy Officer who may consult with our legal counsel.

(a) **To the Patient**. Under the law, except as provided in Policy No. 6 in this Privacy Manual, we must make disclosures *to the patient* who requests such disclosure and no authorization is required. If the patient requests a copy of his or her record, refer to Policy No. 6 in this Privacy Manual.

(b) **To the Secretary of HHS.** We must make disclosures of PHI when required by the Secretary of the Department of Health and Human Services ("**HHS**") or to Office of Civil Rights ("**OCR**") to investigate or determine our compliance with the requirements of the Privacy Rule.

(c) **As Required By Law**. To the extent that the use or disclosure of PHI is required by an applicable law, we may do so without the patient's authorization, in compliance with, and limited to, the relevant requirements of such law.

(d) **Public Health Activities**. We may use or disclose a patient's PHI, without the patient's authorization, for the following public health activities and purposes:

(1) **Public Health Authorities**: Disclosure to a public health authority that is legally authorized to receive such information for the purpose of preventing or controlling disease, injury or disability, such as reporting of injury or communicable disease; vital events such as birth and death; public health surveillance; public health investigation; and public health intervention; or, if directed by the public health authority, to a foreign government agency that is collaborating with the public health authority.

(2) **Communicable Diseases**. In addition to reporting communicable disease information to a public health authority, we may disclose a patient's PHI, as authorized by state law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

(3) **Abuse or Neglect**.

i. Except for vulnerable adults, if we believe that an adult patient has been a victim of abuse, neglect or domestic violence, we may disclose a patient's PHI to the governmental entity or agency authorized by law to receive such information. No disclosure of information about the victim of domestic violence or abuse may be made to law enforcement without the patient's authorization.

ii. Vulnerable Adults: When we believe a vulnerable adult is the subject of abuse, neglect, or exploitation, we may disclose the patient's PHI to the appropriate government adult protective services provider.

(4) **Food and Drug Administration**. We may disclose a patient's PHI to a person or entity authorized by the U.S. Food and Drug Administration ("**FDA**") to receive information related to the quality, safety or effectiveness of an FDA-regulated product or activity for which the person or entity has responsibility.

(5) **Workplace Medical Surveillance**. We may disclose PHI to an individual's employer without the individual's authorization only in very specific circumstances where the individual is a member of the employer's workforce and we provide health care to the individual at the request of their employer to conduct an evaluation related to medical surveillance of the workplace or an evaluation to determine whether the individual has a work-related illness or injury. (Note that, where the employer is requesting an evaluation of an individual for purposes other than those stated in this Subsection, or otherwise allowed in this policy, or where some third party other than the individual's employer is requesting an evaluation of the individual, we will follow Policy No. 3 in this Privacy Manual regarding uses and disclosures requiring an authorization.)

(e) **Health Oversight** We may disclose PHI to a health oversight agency for activities authorized by law, such as audits; civil, criminal or administrative investigations, proceedings or actions; inspections; or licensure or disciplinary actions.

(f) **Legal Proceedings**. We may disclose PHI in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (but only that PHI for which disclosure is expressly authorized), and, under certain conditions, in response to a subpoena, discovery request or other lawful process. Workforce members should direct all subpoenas, and other requests for disclosures for purposes of legal proceedings, to the Privacy Officer who may consult our legal counsel.

(g) **Law Enforcement**. We may disclose PHI for law enforcement purposes, without

a patient's authorization, so long as specific legal requirements are met. Some of these law enforcement purposes include: warrants and other legal process; limited information requests for identification and location purposes; and information related to a crime (including a medical emergency where it is likely that a crime has occurred).

(h) **Coroners, Medical Examiners, Funeral Directors, and Organ Donation.**

(1) We may disclose PHI to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other official duties.

(2) We may disclose PHI to a funeral director, as authorized by state law, in order to permit the funeral director to carry out his or her duties, including disclosure prior to, and in reasonable anticipation of, the death of a patient, if necessary for the funeral director to carry out his or her duties.

(3) We may use a patient's PHI, or disclose a patient's PHI to appropriate entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue, for the purpose of facilitating such activities, as authorized under state law.

(i) **Research**. If Practice is called upon to use or disclose PHI for research purposes, such use and disclosure will be under the direction of the Privacy Officer who will consult with Practice's legal counsel.

(j) **Serious Threat to Health or Safety**. Under certain circumstances, we may use a patient's PHI, or disclose it to another health care professional or to a law enforcement agency, if we believe, in good faith, that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or to others or is necessary in certain situations for law enforcement authorities to identify or apprehend an individual who is a serious threat to public safety. If the PHI contains identifying information about a person who has AIDS or an HIV infection, we will not disclose such information without the patient's authorization, unless authorized by state law, or pursuant to a court order.

(k) **Specialized Government Functions**. When the appropriate conditions apply, we may use or disclose a patient's PHI for certain military, national security or intelligence activities, or when needed for correctional institutions and other law enforcement custodial situations.

(l) **Workers' Compensation**. A patient's PHI may be disclosed by us as authorized under state law to comply with workers' compensation laws and other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault. If we routinely make disclosures for workers' compensation purposes, we have developed standard protocols for those

disclosures as part of our minimum necessary policy and procedures (see Policy No. 4 in this Privacy Manual).

(m) **Schools; Immunization Records**. We may disclose a patient's PHI to a school when the patient is a student or a prospective student of the school if: (I) the PHI that is disclosed is limited to proof of immunization, (ii) the school is required by state law (or other law) to have proof of immunization prior to admitting the individual and (iii) we obtain and document the oral agreement for such disclosure from the parent, guardian or other person acting *in loco parentis* of an unemancipated minor or from the individual, if the individual is an adult or emancipated minor.

3. Verification of the Identity of an Authorized Person

(a) Prior to any disclosure of PHI under this policy, we will verify the identity of the person requesting the PHI and the authority of any such person to have access to the patient's PHI, if the identity or any such authority of the person is not known to us.

(b) We will obtain and/or document any pertinent credentials, documentation, statements or representations, whether oral or written, from the person requesting the PHI.

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REQUIRING PATIENT AUTHORIZATION

Policy Number 3
HIPAA §§ 164.508, 514

PURPOSE: Establish a Policy for the Use and Disclosure of PHI with Patient Authorization

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice may use or disclose a patient's PHI for those purposes specified in Policy No. 2 in this Privacy Manual without obtaining the patient's authorization. Other uses and disclosures of PHI, as addressed in this policy, will be made only with the patient's written authorization. Practice will not condition treatment on the provision by the patient of a requested authorization except as allowed under this policy.

Procedure:

1. Whenever Practice needs to use or disclose a patient's PHI for purposes unrelated to Treatment or Health Care Operations (or as otherwise described in Policy No. 2 in this Privacy Manual), or if a patient requests disclosure of his or her PHI to a specified third party, we will obtain the patient's prior written authorization for such use or disclosure.

2. We will only release that PHI consistent with the scope of the authorization.

3. **Authorization Form:** Practice's authorization form will provide for the following:

(a) The name of the person or entity, or category of persons/entities authorized to make the requested use or disclosure;

(b) The name of the person or entity, or category of persons/entities, to whom the use or disclosure may be made;

(c) Specifically describe the information to be used or disclosed, including, but not limited to, specific detail such as date of service, type of service provided, level of detail to be released, origin of information, etc.;

(d) List the specific purposes for the use or disclosure. If the individual does not, or elects not to, provide a statement of the purpose, the form will state the purpose as "at the request of the individual";

(e) Specify that the authorization will be in force and effect until a specified date or event (stated in the authorization) that relates to the patient or to the purpose of the use or disclosure, at which time the authorization will expire;

(f) Provide for the patient's right to revoke the authorization as set forth in Subsection 4, below;

(g) Specify that Practice will not condition treatment upon the patient's execution of an authorization, as set forth in Subsection 5, below;

(h) Specify that the information disclosed pursuant to the authorization may be re-disclosed by the recipient and no longer subject to the protections of the Privacy Rule; and

(i) Provide for the patient's signature and date of execution or, if the patient's Personal Representative is signing on behalf of the patient, provide for a description of that person's authority to act and/or that person's relationship to the patient.

4. Revocation of Authorization

(a) A patient has the right to revoke an authorization at any time, in writing, by mailing such written notification to the attention of the Privacy Officer or by personal delivery to the Privacy Officer.

(b) A revocation is not effective to the extent that Practice has taken action in reliance on the patient's authorization.

5. Practice will not condition a patient's treatment on whether the patient provides authorization for the requested use or disclosure if to do so would be prohibited by federal or state law. If a reason exists under law for conditioning the patient's treatment on obtaining an authorization, the patient will be advised of that fact and of the consequences to the patient of refusing to sign the authorization. The Privacy Officer will determine if such reason exists.

6. Independent Medical Examination. In accordance with state law, if a third party has requested that Practice examine or evaluate a person ("**Examinee**") and the Examinee has signed an authorization for the release of our report of such examination or evaluation to the third party:

(a) The report will be consistent with the authorization, to avoid unnecessary disclosure of diagnoses or personal information which is not pertinent to the evaluation;

(b) The report will be forwarded only to the third party who requested the evaluation, in accordance with the Examinee's authorization and, if no specific individual is identified, the report will be marked "Confidential"; and

(c) We will not provide the Examinee with a copy of the report unless the third party requesting the examination consents to its release, except that should the examination disclose abnormalities or conditions not known to the Examinee, we will advise the Examinee to consult another health care professional for treatment

7. If an authorization is being requested for PHI for marketing purposes, we will refer the matter to the Privacy Officer for complying with such request in accordance with law.

8. If an authorization is being requested for PHI for research purposes, we will refer the matter to the Privacy Officer for complying with such request in accordance with law.

9. If an authorization is being requested for a use or disclosure considered a sale of PHI, we will refer the matter to the Privacy Officer for complying with such request in accordance with law.

10. We will not directly or indirectly receive remuneration in exchange for any PHI of a patient unless we have obtained from the patient a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the patient's PHI. This requirement will not apply if the purpose of the exchange is:

(a) For public health activities;

(b) For research and the price charged reflects the costs of preparation and transmittal of the data for such purposes;

(c) For treatment purposes;

(d) For the sale, transfer, merger or consolidation of all or part of Practice with another Covered Entity, and due diligence related to such activity;

(e) For remuneration that is provided by Practice to a Business Associate for activities involving the exchange of PHI that the Business Associate undertakes on our behalf and at our specific request pursuant to a Business Associate Agreement;

(f) To provide a patient with a copy of the patient's PHI pursuant to Policy 6 in this Privacy Manual;

(g) As required by law; or

(h) For any other purpose permitted by or in accordance with the Privacy Rule where the only remuneration received by Practice is a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI for such purpose or a fee otherwise expressly permitted by other law.

11. Any offer of remuneration in exchange for PHI will be directed to the Privacy Officer.

12. Prior to any disclosure of PHI under this policy, we will verify the identity of the person requesting the PHI and the authority of any such person to have access to the patient's PHI, if the identity or any such authority of the person is not known to us. We will obtain any documentation, statements or representations, oral or written, from the person requesting the PHI when such documentation, statement or representation is pertinent to the disclosure

13. We can accept a government agency's authorization form as long as it meets the requirements of Subsection 3, above.

14. The patient may receive a copy of the authorization, upon request.

15. Practice will document in the patient's medical record that the patient's authorization was obtained for the specific use or disclosure and will retain the signed authorization in the patient's medical chart, in either written or electronic form, for at least six years from the date when it last was in effect. If the patient revokes the authorization, we will document such revocation in the patient's medical record and retain the signed revocation in the same manner as an authorization.

"MINIMUM NECESSARY" USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Policy Number 4
HIPAA §§164.502(b), 514(d)

PURPOSE: Establish a Policy to Ensure Use and Disclosure of PHI is the Minimum Necessary

APPROVED: _____ **DATE:** _____, 2019

Policy: When using or disclosing PHI or when requesting PHI from another Covered Entity or Business Associate, Practice will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. At such time as the Secretary of HHS issues guidance on what constitutes "minimum necessary," Practice will follow that guidance when applying this policy.

Procedure:

1. **Exceptions to this policy** Our uses and disclosures of PHI, and requests for PHI, that are *not* subject to this policy requiring that the minimum necessary information be used or disclosed, are as follows:

   (a) Disclosures to or requests by a health care provider for Treatment purposes, including our own requests for disclosure of PHI for Treatment purposes;

   (b) Disclosures made to the patient, including but not limited to disclosures made to the patient pursuant to the patient's request to access his or her record or for an accounting of disclosures made by Practice of the patient's PHI;

   (c) Uses or disclosures made pursuant to a patient's authorization that adheres to Policy No. 3 in this Privacy Manual;

   (d) Disclosures made to the Secretary of HHS related to enforcement of the requirements of the HIPAA privacy standard;

   (e) Uses or disclosures required by other law as described in Policy No. 2 in this Privacy Manual;

   (f) Uses or disclosures that are required for compliance with the requirements of the HIPAA privacy standard; or

   (g) PHI that has been de-identified, as specified in the Privacy Rule.

2. Situations Where this Policy Does Apply

(a) Our Own Use of PHI

(1) Practice has established which persons or categories of persons need access to PHI to carry out their duties.

(2) For each such person or category, we have determined the types of PHI to which access is needed, including identification of those persons or classes of persons in Practice who need to see the entire medical record, and any conditions that exist for access (role-based access).

(3) We will make reasonable efforts to limit the access only to the amount of information needed by the person in order to carry out the duties of that position or to accomplish the required use.

(b) **Our Own Disclosures of PHI** For disclosures of PHI that we make on a *routine and recurring* basis, we have established a standard protocol for limiting the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure.

For *non-routine* disclosures, we have developed criteria designed to limit the PHI disclosed to the minimum information reasonably necessary to accomplish the purpose of the disclosure. We will review requests for such *non-routine* disclosures on an individual, case-by-case basis for conformance with these criteria.

The criteria for *non-routine* disclosures do not need to be applied when a request for disclosure is received in the following situations and the request appears to reasonably limit the disclosure to the minimum necessary under the particular circumstances of the request:

(1) Requests for disclosures received from a health care provider, health plan or health care clearinghouse;

(2) Requests for disclosures received from public officials in those situations identified in Policy No. 2 in this Privacy Manual (No Authorization Required) and the public official represents that the information requested is the minimum necessary;

(3) Requests for disclosures received from a professional member of Practice, or from one of our business associates for the purpose of providing professional services to Practice, if the professional represents that the information requested is the minimum necessary for the stated purpose; or

(4) Requests for disclosures received from a researcher with appropriate documentation from an Institutional Review Board or Privacy Board.

(c) For both routine and non-routine disclosures and requests, we have identified in our protocol the circumstances under which the entire medical record is reasonably necessary for particular purposes.

(d) We will reasonably rely on requests from the business associate of another health care provider, health plan or health care clearinghouse for the disclosure of PHI as meeting the minimum necessary requirement for the intended purpose.

3. **Our Own Requests for PHI** We will limit any request for PHI that we make to another health care provider, a health plan, or a health care clearinghouse to that which is reasonably necessary to accomplish our purposes.

For requests made on a *routine and recurring* basis, we have established a protocol that limits the PHI requested to the amount reasonably necessary to accomplish our purposes.

For requests on a *non-routine or non-recurring* basis, we have developed criteria designed to limit the request for PHI to the information reasonably necessary to accomplish our purposes. We will review such non-routine requests on an individual basis for conformance with these criteria.

Practice will make reasonable expenditures to implement technologically feasible approaches in complying with this policy (see Policy No. 10 in this Privacy Manual).

USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION WHERE THE PATIENT HAS AN OPPORTUNITY TO AGREE OR OBJECT

Policy Number 5
HIPAA §§ 164.510, 514

PURPOSE: Establish a Policy for Allowing Patients to Agree or Object to Use and Disclosure of their PHI

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice may use and disclose PHI in certain situations where it is necessary or beneficial to involve others in the patient's health care or to notify others of the patient's status or condition. In these situations, the patient has the opportunity to agree or object to the use or disclosure of all or part of the patient's PHI for these purposes.

Procedure:

1. We may make the following disclosures for involvement in the patient's care and notification purposes:

(a) Disclosing to a Family Member, other relative, close personal friend of the patient, or any other person identified by the patient, PHI that is directly relevant to that person's involvement in the patient's health care;

(b) Using or disclosing PHI to notify, or assist in the notification to a Family Member, a Personal Representative of the patient or another person who is responsible for the patient's care, of the patient's location, general condition or death; or

(c) Disclosing PHI to any person identified in Subsection 1(a) above who was involved in the patient's care, PHI of the patient that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to us.

2. If the patient is present or otherwise available prior to our using or disclosing their PHI in this way, and the patient has the capacity to make health care decisions, we will only disclose the information if we:

(a) Provide the patient with the opportunity to agree or object to the disclosure, and the individual does not express an objection (we can inform the patient orally and accept the patient's oral agreement or objection, but we will document such agreement or objection in the patient's medical record); or

(b) Can reasonably infer from the circumstances, based on the exercise of professional judgment that the patient does not object to the disclosure.

3. If the patient is not present, or it is impractical to offer the patient the opportunity to agree or object to a use or disclosure of their PHI in these situations, because the individual is incapacitated or an emergency exists:

(a) We may use our professional judgment to determine whether the disclosure is in the best interests of the patient; and

(b) If we determine disclosure is appropriate, will disclose only that PHI which is directly relevant to the person's involvement in the patient's care or needed for notification purposes.

4. If the patient is not present, we may use our professional judgment and experience with common practice to allow another person acting on the patient's behalf to pick up medical supplies, x-rays or other similar forms of PHI because it is in the patient's best interest.

5. We may use or may disclose a patient's PHI to a public or private entity authorized to assist in disaster relief efforts for coordinating with them in notifying Family Members or other individuals involved in the patient's health care. In such situations, we will still follow the procedures of Subsections 2 through 4 of this policy if, in our professional judgment, to do so will not interfere with the ability to respond to the emergency circumstances.

6. A patient may request that we restrict disclosures otherwise allowed under this policy. Any such requests will be directed to the Privacy Officer.

ACCESS OF INDIVIDUALS TO PROTECTED HEALTH INFORMATION

Policy Number 6
HIPAA § 164.524

PURPOSE: Establish a Policy for Patients to Gain Access to Their PHI

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice, in accordance with this policy, will provide a patient the right to inspect and obtain a copy of the patient's PHI for as long as Practice maintains the information.

Procedure:

1. General Procedure

(a) A patient of Practice can request to inspect or obtain a copy of their PHI that we maintain in a Designated Record Set and we will provide such access, unless access is to be limited as required in this policy.

(b) A Personal Representative of a patient may also be permitted to access the patient's PHI, in accordance with this policy.

(c) If we do not maintain the PHI that is the subject of the request, and we know where the requested information is maintained, we will inform the patient where to direct the request for access.

2. Requests for Access and Responding to Requests

(a) All requests for inspection or copying of a patient's PHI must be in writing. Patients will be advised of this requirement in our Notice of Privacy Practices. These requests will be directed to the Privacy Officer.

(b) We may choose to provide a summary of the requested information. Patients will be advised in our Notice of Privacy Practices of this alternative. We may only provide a summary of the PHI if the patient agrees in advance to receive a summary of their PHI and to the fee we would charge for a summary of the PHI.

(c) Practice will respond to a request for inspection or copying within 15 days of receipt of the written request.

(d) If the patient requests, we will mail the copy of the PHI or the summary of the PHI, as agreed upon, to another person specified by the patient if the patient's request is in a writing signed by the patient and clearly identifying the designated person and where to send the copy of the PHI

(e) If we maintain an electronic health record that contains the PHI requested by the patient, the patient has the right to obtain a copy of that information in an electronic form and format they request, if it is readily producible or, if not, in a readable electronic form and format as agreed between us and the patient. In addition, the patient may choose to direct us to transmit such copy directly to an entity or person designated by the patient, provided that any such choice is clear, conspicuous, and specific.

(f) We will charge a fee for the copy of the patient's PHI (or for a summary of the PHI) that is reasonable and cost-based, including in all cases any charge limits imposed by state law. Any fee we impose for providing a copy or summary of PHI in an electronic form will not be greater than our labor costs in responding to the request and the supplies for creating the electronic media if the individual requests that the electronic copy be provided on portable media, again as limited by state law. Patients will be notified in our Notice of Privacy Practices that a fee will be charged and patients will be advised of the fee.

(g) Practice will not refuse to provide a patient with a copy of his or her medical record due solely to the fact that the patient has an outstanding balance with Practice, when it is known to us that the record is needed by another health care professional for the purpose of rendering care to the patient. In all other cases, the copying fee must be paid prior to or at the time the copy is provided to the patient or personal representative.

(h) If the patient requests only to inspect his or her PHI, we will arrange with the patient for a convenient time (no later than 15 days from the request) and place (at our office or wherever the record is kept) for the inspection to take place. All inspections of PHI by patients or personal representatives will be under the personal supervision of a designated member of our staff.

(i) If any state or federal agency or official, by subpoena or by demand for statement in writing under oath or otherwise, requests a patient's PHI, the Privacy Officer will contact our legal counsel immediately.

3. Denying or Limiting Access

(a) Practice may deny or limit access to a patient's PHI, *without any right to a review* of our decision, if the information:

(1) Has been compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;

(2) Is that of an inmate in a correctional institution and our physician was acting under the direction of the correctional institution, and certain circumstances exist which prohibit providing a copy of PHI to the inmate (to be determined by the Privacy Officer);

(3) Was obtained by Practice in the course of research that includes treatment of the research participant, while the research is in progress, under certain circumstances (to be determined by the Privacy Officer);

(4) Is subject to the Privacy Act, as required by the Privacy Act; or

(5) Was obtained by Practice from someone other than a health care provider, under a promise of confidentiality, and the requested access would be reasonably likely to reveal the source of the information.

(b) Practice may deny or limit access to a patient's PHI, *with the right to a review* of our decision, in the following situations:

(1) A licensed health care professional in Practice has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

(2) The information references another person (unless such other person is a health care provider) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to that other person;

(3) Access is requested by a personal representative of the patient and a licensed health care professional has determined that access by that person is reasonably likely to cause substantial harm to the patient or another person; or

(4) A licensed health care professional has reason to believe that the patient's mental or physical condition will be adversely affected upon being made aware of the subjective information contained in the PHI (or a summary of the PHI); in this case, however, the PHI can be provided, if requested by the patient (with an accompanying notice setting forth the reasons for the original refusal) directly to the patient's attorney, another licensed health care professional, the patient's health insurance carrier (through an employee of the carrier), or to a governmental reimbursement program or to an agent of such program who has responsibility to review utilization and/or quality of care.

(c) The determination of whether to deny or limit access based on the grounds in Subsections 3(a) or 3(b), above, will be made by a licensed physician of Practice (or, if a physician is unavailable, by another licensed health care practitioner of Practice), in conjunction with the Privacy Officer.

(d) Practice will provide a patient with a written notice of denial or limitation of access (see Forms section of this Privacy Manual) which will contain: the reason for

such denial or limitation; a statement of the patient's right to a review of the denial, if such right exists; how to exercise the review rights; and a description of our complaint procedures (see Policy No. 12 in this Privacy Manual), including the name or title and telephone number of the Privacy Officer as the contact person.

(e) If we deny the patient access to some of his or her PHI, we will, to the extent possible, give the patient access to any other of the patient's PHI requested by the patient, where no grounds exist to deny such access.

4. <u>Appeal of a Decision to Deny Access</u>

(a) A patient may request a review of a denial of access that was made based on one of the reasons under Subsection 3(b) above.

(b) Requests for review of a denial of access will be directed to the Privacy Officer who will promptly refer the request for review by the person designated pursuant to subsection (c), below.

(c) Review of the denial of access will, within a reasonable period of time, be performed by a licensed health care professional designated by Practice and who did not participate in the original decision to deny access. Where available, another licensed physician of Practice will conduct such review. Where another licensed physician of Practice is not available, another licensed health care practitioner of Practice will conduct the review. Where no other physician or licensed health care practitioner of Practice exists or is available, the review will be conducted by another health care professional designated by the Privacy Officer.

(d) Practice will conduct the review within a reasonable period of time and will attempt to conduct the review within 30 days of the request for review. Once the review is complete, we will promptly provide a written response (see Forms) to the patient setting forth the decision of the reviewing professional and will provide access or deny access based on that decision.

(e) We will maintain a copy of the inspection/copying request form in the patient's medical record, including documentation on the form of our response, and the results of any appeal and review that may have occurred.

ACCOUNTING FOR DISCLOSURES OF PROTECTED HEALTH INFORMATION

Policy Number 7
HIPAA § 164.528

PURPOSE: Establish a Policy for Accounting for Disclosures of PHI

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will provide patients with an accounting of disclosures of their PHI as required under federal and state law and regulations.

Procedure:

1. A patient of Practice may request and has a right to receive an accounting of disclosures Practice has made of the patient's PHI, except as limited by this policy. A patient may request an accounting for a time period of up to 6 years prior to the date of his or her request. The accounting will include disclosures made to or by our business associates. Such requests must be in writing and will be directed to the Privacy Officer.

2. No accounting need include disclosures that we made:

   (a) To carry out Treatment, Payment and Healthcare Operations ("**TPO**") of Practice, except as set forth in subsection 3, below;

   (b) To patients about their own PHI;

   (c) Pursuant to an authorization made by the patient or the patient's personal

   (d) representative regarding the patient's PHI;

   (e) To individuals involved in the patient's care or for other allowed notification purposes;

   (f) Incident to a use or disclosure otherwise permitted or required by the Privacy Rule and this Privacy Manual;

   (g) For any facility directory maintained by Practice;

   (h) For national security or intelligence purposes;

   (i) To correctional institutions or law enforcement officials; or

   (j) As part of a Limited Data Set

3. If we use or maintain an electronic health record with respect to the PHI, the accounting must include disclosures made for Treatment and Health Care Operations of Practice but only for a time period of up to 3 years prior to the date of the patient's request. Since we acquired an electronic health record after January 1, 2009, we must provide an accounting of TPO disclosures made by us from such record on and after the date that we acquired the electronic health record.

4. In order to provide this accounting to our patients, Practice will maintain a log or record of all disclosures, other than those excluded under Section 2 above, of a patient's PHI, for a 6 year period (or for 3 years if an electronic health record is used or maintained), along with a copy of every accounting made to a patient.

5. A request for an accounting of disclosures will be acted upon within 60 days of receipt of the request. A one-time 30 day extension may be allowed if the patient has been notified, within the initial 60-day period, of the reasons for the delay and the date by which we will provide the accounting. We may choose to provide an accounting of all disclosures made by Practice and by any Business Associate acting on our behalf; or an accounting of all disclosures made by Practice and provide to the patient a list of all Business Associates acting on our behalf, including contact information for such Business Associates (such as mailing address, phone, and email address), in which case such Business Associates will provide an accounting of their disclosures upon a request made by our patient directly to the Business Associate. The Privacy Officer will determine which option we choose.

6. For each disclosure for which we are required to provide an accounting under this policy, we will maintain the following information and will provide the information in the accounting to the patient:

   (a) The date of the disclosure;

   (b) The name of the entity or person who received the PHI and, if known, the address of such entity or person;

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

   (d) 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 a written request by the Secretary for a disclosure to investigate or determine our compliance with the HIPAA privacy standard or a written request received for a disclosure made under Policy No. 2 in this Privacy Manual (Disclosures Where No Authorization is Required).

7. If, during the period covered by the accounting, we have made multiple disclosures of PHI to the same person or entity for a single purpose, the accounting may provide:

   (a) The information required in Section 6 of this policy for the first disclosure during

the accounting period;

(b) The frequency, periodicity, or number of the disclosures made during the accounting period; and

(c) The date of the last such disclosure during the accounting period.

8. If any disclosures of a patient's PHI involved a particular research purpose, the Privacy Officer will determine the manner of our log of disclosures and the manner of disclosing the accounting to the particular patient.

9. The first accounting provided to a patient in any 12-month period will be without charge. We will charge a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the 12-month period, provided that we have informed the patient in advance of the fee and provided the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

10. We will temporarily suspend a patient's right to receive an accounting of disclosures we have made to a health oversight agency or law enforcement official (see Policy No. 2 in this Privacy Manual), for the time specified by such agency or official, if such agency or official has provided us with a written statement that such an accounting to the patient would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required. If the agency or official statement is made orally, we will:

(a) Document the statement, including the identity of the agency or official making the statement;

(b) Temporarily suspend the patient's right to an accounting of disclosures subject to the statement; and

(c) Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless the appropriate written statement is submitted to us by the agency or official during that time.

AMENDMENT OF PROTECTED HEALTH INFORMATION

Policy Number 8
HIPAA § 164.526

PURPOSE: Establish a Policy Regarding a Patient's Right to Request an Amendment to their PHI

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice, in accordance with this policy, will provide our patients the opportunity to request amendment of their PHI that we maintain and, where appropriate under this policy, the right to have their PHI amended.

Procedure:

1. <u>Receiving and Acting Upon a Request for Amendment</u>

(a) A patient of Practice can request to have his or her PHI amended. Our Notice of Privacy Practices will advise our patients that such a request must be in writing and must state a specific reason supporting the requested amendment.

(b) All requests for amendment of PHI will be directed to the Privacy Officer.

(c) Action upon the request for amendment should occur within 60 days of receipt. A one-time extension of not more than 30 days may be allowed if Practice, before the end of the initial sixty-day period, provides a written notice to the requestor of the reason for the delay and the date by which Practice intends to complete its action on the request. The Privacy Officer will track the progress of each request for amendment to attempt to ensure compliance with these timeframes.

(d) The Privacy Officer will review the amendment request for the following elements:

(1) The reason for the requested amendment, such as how the information is incorrect or incomplete;

(2) Whether the requested amendment is to: 1) administrative information; and/or 2) medical information, including the source, if known, the date(s) of service, and the specific provider of service;

(3) Whether Practice was the originator of the information; and

(4) The specific wording requested to correct the alleged inaccuracy or incompleteness.

(e) The Privacy Officer will make a preliminary determination regarding whether an

amendment request should be honored, and will then consult with the physician, other health care professional, or administrative staff person of Practice who provided the care and/or made the entry that is the subject of the amendment.

(1) If that physician, health care professional or administrative staff person agrees with the Privacy Officer's preliminary determination, the Privacy Officer will obtain final approval from an Officer of Practice.

(2) If such final approval is obtained, the Privacy Officer will proceed with the amendment or denial of amendment, pursuant to this policy.

(3) If a determination as to whether to accept or deny the amendment cannot be made internally, the Privacy Officer will notify Practice's legal counsel and request a resolution of the disagreement.

2. <u>Denying a Request for Amendment</u>

(a) Practice may deny a request for an amendment in the following situations:

(1) Practice did not create the information, 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;

(2) The information is not part of our records for a patient;

(3) The information would not otherwise be available for inspection (see Policy No. 6 in this Privacy Manual regarding Access to PHI); or

(4) Practice determines that the information in dispute is neither inaccurate nor incomplete.

(b) If Practice determines to deny a request for amendment, in whole or in part, the Privacy Officer will provide written notice to the requestor, within the timeframe stated in Subsection 1(b) of this policy, advising of the decision to deny amendment, stating the reason for the denial, and advising of our complaint procedures (see Policy No. 12 in this Privacy Manual).

(1) The written notice will also advise the requestor that the individual may submit to the Privacy Officer a written statement of disagreement with the denial, stating the basis for such disagreement.

(2) In most cases, the length of the statement of disagreement will be limited to 1 page, unless it is unreasonable in the particular circumstance to impose such a limit.

(c) If the patient does not submit a statement of disagreement, the patient may request

that we provide the patient's request for amendment, and the denial, with any future disclosures of the PHI that is the subject of the requested amendment.

(d) If a statement of disagreement is received from a requestor, the Privacy Officer, in consultation with the pertinent physician, health care professional or administrative staff person, will determine whether to prepare a rebuttal statement. If a rebuttal statement is prepared, we will provide a copy to the requestor.

(e) The denial--and the disagreement and rebuttal statement, if any—will be linked to the PHI in dispute by physically attaching these documents to the disputed information in the patient's record.

(f) Whenever the disputed information is disclosed to another person or entity, the information will include the denial and, if any exists, the statement of disagreement and the rebuttal.

(1) Alternatively, we can provide a summary of any of the foregoing information.

(2) If the patient has not submitted a statement of disagreement, we will include the patient's request for amendment and our denial, or a summary of the information, with any future disclosure of the patient's PHI only if the patient has requested such action.

(3) If such a subsequent disclosure is made using a standard transaction under the HIPAA Transaction Rule that cannot accommodate the denial, disagreement and rebuttal, Practice will separately disclose the denial, disagreement, and rebuttal to the recipient of the transaction.

3. Accepting the Request for Amendment

(a) If a determination is made to make the requested amendment, the Privacy Officer will provide written notification to the requestor that the requested amendment has been approved and the exact wording of the amendment.

(b) The Privacy Officer will seek the requestor's identification of, and agreement to, the relevant persons identified by the Privacy Officer as persons or entities with whom the amendment needs to be shared.

(c) The requestor will have 10 days to object to the form of amendment or to the persons with whom the amendment will be shared. If no objection is received within that time period, the amendment will be made in the PHI and the identified parties notified.

(d) The Privacy Officer will identify the records in the designated record set for the patient that are affected by the amendment and append or otherwise provide a link to the location of the amendment.

(e) The Privacy Officer will, within a reasonable period of time (but no longer than 30 days), take reasonable efforts (such as send written notification by certified mail, return receipt requested) to provide the exact wording of the amendment to:

(1) Such persons or entities that the patient has identified as having received the relevant portion of the patient's PHI from Practice; and

(2) Such persons, including our business associates, who we have identified as having received the relevant portion of the patient's PHI from Practice and who may have relied, or could foreseeably rely, on such information to the detriment of the patient.

4. Making the Amendment

(a) The Privacy Officer, or his or her designee, will identify all media forms in which Practice maintains the information to be amended, i.e., paper, microfiche, microfilm, automated data processing or other electronic medium, and will cross check across all systems and applications maintained by Practice to ensure that the amendment is made, stored (as necessary), and susceptible to audit trails.

(b) In no case will the Privacy Officer, a physician or any other person of Practice delete, erase, "white out" or otherwise obliterate medical information in a patient's record. Any correction or addition to a patient's PHI will be clearly identified as a correction or addition to the original and will be dated and initialed by the physician or other person who made the initial entry.

5. Requests for Amendment where Practice was not the Originator of the Information

(a) If a request for amendment applies to information for which Practice was not the originator, the Privacy Officer will contact the requestor and advise the requestor to seek amendment from the originator of the information.

(b) If the requestor notifies us of a reasonable basis to believe that the originator is no longer available to act on a requested amendment, the Privacy Officer will make a reasonable attempt to confirm the unavailability. If the originator's unavailability is confirmed, Practice will act on the request for amendment as though Practice created the information.

6. Amendments Received from Other Covered Entities

(a) If we are informed by another health care provider, a health care plan or a health care clearinghouse of an amendment to a patient's PHI, we will amend the patient's PHI that we maintain, accordingly.

(b) The Privacy Officer will:

(1) Document in the patient's record that the approved amendment has been received from another sources and the identity of the source providing the amendment;

(2) Ensure that the amendment is property made in the PHI that is held by Practice; and

(3) If the patient whose PHI is amended is a current patient of Practice, alert the treating physician(s) for that patient of the amendment that has been made.

BUSINESS ASSOCIATES

Policy Number 9
HIPAA §§ 164.103, 502(e), 504(e), 532(d) & (e)

PURPOSE: Establish a Policy for Sharing PHI with Business Associates

APPROVED: _____ **DATE:** _____, 2019

Policy: Before Practice can disclose PHI to a Business Associate, or allow a Business Associate to create, receive, maintain or transmit PHI on our behalf, we will obtain satisfactory assurances that the Business Associate will use or disclose the PHI only as permitted or required by our Business Associate Agreement, will safeguard the PHI from misuse, will help Practice comply with its duties under HIPAA and the Data Breach Notification Rule, and will secure these same assurances from any Subcontractor of the Business Associate. The Business Associate cannot use or disclose PHI provided by us in any manner that would not be a permissible use or disclosure by Practice under the Privacy Rule.

Procedure:

1. <u>Business Associates; Business Associate Agreements</u>

(a) For each new arrangement where Practice plans to retain a person or entity to perform a function, activity or service on behalf of Practice, the Privacy Officer will first consult the definition of Business Associate in the Glossary of Terms to determine whether the person or entity is to be treated as a Business Associate of Practice.

(b) Practice will enter into a written Business Associate Agreement with every person or entity who meets the definition of a Business Associate as set forth in the Glossary of Terms. The Privacy Officer will consult our form of Business Associate Agreement and contact our legal counsel, as necessary, to assist in negotiation and/or preparation of the necessary agreement. Any Business Associate Agreement Practice enters into must meet the requirements of 45 C.F.R. §164.504(e) (1).

(c) If a Business Associate presents to Practice the Business Associate's own proposed Business Associate Agreement, the Privacy Officer will review the proposed agreement under our model form and contact our legal counsel, as necessary, to assist in negotiation of necessary revisions to the proposed agreement(s).

(d) If Practice has a Business Associate Agreement with an existing Business Associate Agreement that does not address requirements under the Data Breach Notification Rule or is not in compliance with the HITECH Act, we will enter into an Amended and Restated Business Associate Agreement and contact our legal counsel, as necessary, for assistance.

2. **Confidentiality Agreements** Where the Privacy Officer has identified that a person or entity is not a Business Associate but, nevertheless, may have more than incidental or inadvertent access or exposure to PHI held by Practice, the Privacy Officer will seek to enter into a confidentiality agreement with that person or entity and will obtain the advice of our legal counsel, as necessary.

3. **Responding to Violations by a Business Associate**

(a) If any person in Practice receives any information leading him or her to believe that one of our Business Associates (or an employee or agent of one of our Business Associates) is violating a provision of our Business Associate Agreement or is engaged in some activity that could result in a violation of our privacy policies and procedures, that person will immediately provide that information to the Privacy Officer.

(b) The Privacy Officer will keep a record of information provided to him or her pursuant to subsection 3(a). If the information provided appears credible, the Privacy Officer will contact the Business Associate to discuss the problem or may contact our legal counsel prior to contacting the Business Associate.

(c) If the information received by the Privacy Officer reflects a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the Business Associate's obligations under our agreement with that entity or person, the Privacy Officer will notify legal counsel for further action as required by the Privacy Rule.

SAFEGUARDING PROTECTED HEALTH INFORMATION

Policy Number 10
HIPAA § 164.530(c)

PURPOSE: Establish a Policy for Ensuring PHI Remains Private

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will have in place appropriate administrative, technical, and physical safeguards to try to reasonably safeguard our patients' PHI.

Procedure: Practice has implemented procedures pursuant to this policy, which are described in the Security Manual.

(a)

TRAINING

Policy Number 11
HIPAA § 164.530(b)

PURPOSE: Establish a Policy for Training all Workforce on Privacy & Security Policies

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will provide training to all Workforce members on the policies and procedures in this Privacy Manual and the Security Manual, as necessary and appropriate for them to carry out their function and duties within Practice.

Procedure:

1. The Privacy Officer will develop and implement a training program for our Workforce to include the following:

(a) Making a copy of this Privacy Manual and the Security Manual available to all Members of our Workforce for the purpose of reviewing each policy and procedure (such review to occur in a training meeting(s) of our entire Workforce and/or through individual review by each member of our Workforce) or for consulting our policies and procedures on an as-needed basis;

(b) Informal awareness training regarding privacy and security of PHI and e-PHI, including application of the minimum necessary principle (see Policy No. 4 in this Privacy Manual and Policy No. in the Security Manual);

(c) Periodic reminders about the need to make good faith efforts to maintain the privacy and security of our patients' PHI and e-PHI;

(d) Education concerning computer virus protection, detection, and response to a virus infection; and

(e) Education about the importance of a secure login and Practice's policy regarding creating, changing, and protecting the confidentiality of computer passwords.

2. Practice will provide this training as follows:

(a) To each member of our current Workforce;

(b) To each new member of our Workforce not later than the 90th day after the person joins Practice; and

(c) To each member of our Workforce whose job functions are affected by a material change in our policies or procedures or a material change in the HIPAA Privacy

Rule or HIPAA Security Rule, with such training to occur within a reasonable period of time, but not later than the first anniversary after the material change becomes effective.

3. All members of our Workforce must:

(a) Sign a log indicating the date and content of training received by such person; and

(b) Sign, electronically or in writing, a confidentiality agreement stating that the person has reviewed and understands Practice's privacy policies and procedures and will strive to comply with them, and to reinforce each person's responsibility to protect and maintain the privacy and security of our patients' PHI and e-PHI.

4. The Privacy Officer will maintain records documenting that the training required by this policy is provided until the sixth anniversary of the date the confidentiality agreement is signed by each member of the Workforce.

COMPLAINTS TO PRACTICE; MITIGATION

Policy Number 12
HIPAA § 164.530(d), (f)

PURPOSE: Establish a Policy Regarding Patient Complaints and Mitigation

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will provide a procedure for patients to make a complaint concerning Practice's privacy policies and procedures or Practice's compliance with such policies and procedures or with the HIPAA Privacy Rule.

Procedure:

1. A patient of Practice who has a complaint about our policies and procedures regarding the handling of PHI, about our compliance with such policies and procedures or with the Privacy Rule, may file a complaint with the Privacy Officer.

(a) A complaint must be in writing and must state the specific nature of the problem with our policies and procedures or the specific area of alleged non-compliance.

(b) The Privacy Officer will acknowledge to the patient, in writing, that we received the complaint and that it will be addressed appropriately and a response provided to the patient.

2. As specified in our Notice of Privacy Practices, a patient may also file a complaint directly with the Office for Civil Rights (see Glossary of Terms). The address for filing a complaint with the OCR will be provided to any person, upon request.

3. A complaint to Practice will be acted upon as soon as reasonably possible but in no case longer than 30 days of receipt.

4. Upon receipt of a complaint, the Privacy Officer will advise the managing physician of Practice, and, upon such review of the complaint, may notify our legal counsel for retention in reviewing, investigating, and formulating a response to the complaint.

5. Once the investigation into the complaint has been concluded, the Privacy Officer, in conjunction with legal counsel, will formulate an appropriate response to the complaining individual.

6. If the investigation of the complaint revealed a problem with our policies and procedures, or a failure to comply with such policies and procedures or with applicable law or regulations, the Privacy Officer, in conjunction with our legal counsel, will formulate corrective action intended to remedy the problem or non-compliance including, as appropriate, imposing sanctions pursuant to Policy No. 14 in this Privacy Manual.

7. If the violation is found to involve a Business Associate of Practice, we will take the steps required by Policy No. 9 in this Privacy Manual, regarding Practice's Business Associates.

8. The Privacy Officer will document all complaints received and their disposition.

9. Any correspondence or communication Practice receives from the OCR—whether regarding the investigation of a complaint, a compliance review, or otherwise—will be immediately provided to the Privacy Officer who will notify legal counsel for Practice to assist in responding to the OCR. Practice will cooperate with the OCR and provide access as required by the Privacy Rule.

10. The Privacy Officer will take reasonable efforts to mitigate, to the extent practicable, any harmful effect that is actually known to Practice of a use or disclosure of PHI by Practice or by one of our Business Associates, in violation of our policies and procedures or the requirements of law. The Privacy Officer will implement our Data Breach Notification Policy, to determine if any notice is required and what mitigation efforts should be undertaken.

NO RETALIATION FOR THE EXERCISE OF RIGHTS OR THE FILING OF A COMPLAINT; NO WAIVER OF RIGHTS

Policy Number 13
HIPAA § 164.530(g), (h)

PURPOSE: Establish a Policy to Ensure that there is No Retaliation for the Filing of a Complaint

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against any individual who exercises, or attempts to exercise, his or her rights under the HIPAA Privacy Rule or who files a complaint or otherwise participates in HIPAA compliance efforts as described in this policy. Practice will not require an individual to waive his or her rights under the HIPAA Privacy Rule as a condition of receiving treatment from Practice.

Procedure:

1. All requests for access, amendment, copying, authorizations, acknowledgments, and accountings related to the PHI of a patient of Practice will be handled in accordance with this Privacy Manual.

2. All complaints about our policies and procedures, or about our compliance with this Privacy Manual, will be handled in accordance with this Privacy Manual and no patient, Personal Representative, or Member of our Workforce will be retaliated against in any way for:

(a) Filing a complaint with the Privacy Officer or with the Secretary of Health and Human Services (Office for Civil Rights) pursuant to Policy No. 12 in this Privacy Manual;

(b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing related to the Privacy Rule; or

(c) Opposing any act or practice that is unlawful under the HIPAA Privacy Rule, provided the person has a good faith belief that Practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI made in violation of the HIPAA Privacy Rule.

3. Workforce members are encouraged to contact the Privacy Officer for clarification in the event of confusion or questions concerning any part of this Privacy Manual.

4. Workforce members are encouraged to and will immediately report, in good faith, to the Privacy Officer, or to our managing physician, any knowledge of a violation of this Privacy Manual by a member of our workforce or by a Business Associate, or a violation of this policy of non-retaliation and non-waiver of rights.

5. If Practice receives information that this policy may have been violated, the Privacy Officer, or managing physician, as appropriate to the complaint, will promptly investigate the report of retaliation and will consult with Practice's legal counsel regarding the matter, as necessary.

6. Any Member of our Workforce found to have violated this policy will be sanctioned according to the provisions of Policy No. 12 in this Privacy Manual and consistent with our personnel policies.

SANCTIONS FOR VIOLATIONS; EXCEPTIONS TO SANCTIONS

Policy Number 14
HIPAA §§ 164.530(e), (g)(2); 164.502(j)

PURPOSE: Establish a Policy for Sanctions for Privacy Violations

APPROVED: _____ DATE: _____, 2019

Policy: Practice will apply appropriate sanctions against any member of our Workforce who fails to comply with the policies and procedures in this Privacy Manual or the requirements of the Privacy Rule. Sanctions will not be imposed, however, under certain circumstances described in this policy.

Procedure:

1. General Sanction Policy

(a) Practice may receive complaints regarding our compliance with our Policies and Procedures or with the Privacy Rule. Such complaints will be handled in accordance with Policy No. 12 in this Privacy Manual. We may also learn of non-compliance issues through allegations of violations received internally from our Workforce members.

(b) Workforce members are encouraged to make the Privacy Officer or managing physician aware of any concerns about our compliance with our Privacy Policies or with the Privacy Rule. Any allegations of noncompliance should be made in good faith, and in accordance with this policy, as applicable.

(c) All allegations of a violation by a member of our Workforce of a provision of this Privacy Manual will be investigated. Appropriate disciplinary action will be taken whenever it is determined that a member of our Workforce has committed a significant violation of this Privacy Manual or the Privacy Rule. The established disciplinary procedures and processes are applicable to all Workforce members, whether an owner, employee or independent contractor.

(d) The determination of the disciplinary measures to be imposed will be made on a case-specific basis, appropriate to the nature of the violation, and in accordance with our personnel policies. We will consider factors such as:

(1) The severity of the violation;

(2) Whether it was intentional or unintentional; and

(3) Whether there has been a pattern of noncompliance by the member of our Workforce.

(e) Disciplinary actions may include counseling, verbal warning, written warning, suspension without pay, and/or discharge.

(f) As set forth in Policy No. 11 in this Privacy Manual, we will have procedures in place requiring our Workforce members to review and become familiar with our privacy policies and procedures so they will understand what is expected of them in the area of privacy and be aware that noncompliance could result in sanctions. Such training will include the specific requirements set forth in Section 2, below, regarding otherwise impermissible disclosures.

(g) The Privacy Officer will be responsible for documenting all sanctions and disciplinary action resulting from a violation.

2. **Exceptions to Sanctions** Sanctions will not apply to a member of our Workforce with respect to the following activities, where the specific requirements for each type of activity or disclosure is met:

(a) **Actions Taken In Pursuit Of Compliance With The Privacy Rule** Practice will not intimidate, threaten, coerce, discriminate against or take other retaliatory action against Workforce members or others who:

(1) File a complaint with the Secretary of Health & Human Services, or the Office for Civil Rights;

(2) Testify, assist or participate in an investigation or a compliance review, proceeding or hearing related to OCR's enforcement of the Privacy Rule;

(3) Oppose any act or practice made unlawful by the Privacy Rule, provided the person has a good faith belief that the act or practice is unlawful, and the manner of the opposition is reasonable and does not involve disclosures of PHI in violation of the Privacy Rule.

(b) **Whistleblowers** Practice will not impose sanctions or otherwise retaliate against a member of our Workforce or a Business Associate of Practice who discloses PHI in the following circumstances:

(1) The individual believes that the conduct at issue (which requires the disclosure of PHI in order for the individual to report the conduct) is unlawful or otherwise violates professional or clinical standards, or that the care, services or conditions provided by Practice potentially endangers one or more patients, workers or the public and if;

(2) The disclosure is made to one of the following:

i. A health oversight agency or public health authority authorized by

law to investigate or otherwise oversee the relevant conduct or conditions of Practice;

ii. An appropriate health care accreditation organization for the purpose of reporting the allegation of misconduct or failure to meet professional standards or misconduct by Practice; or

iii. An attorney retained by or on behalf of the member of our Workforce or Business Associate for the purpose of determining the person's legal options and/or obligations with regard to Practice's conduct.

(c) **Victims of Crime** Practice will not impose sanctions or otherwise retaliate against a member of our Workforce who is the victim of a criminal act and discloses PHI related to the crime, provided that:

(1) The disclosure is to a law enforcement official;

(2) The PHI disclosed is about the suspected perpetrator of the criminal act; and

(3) The PHI disclosed is limited to the following information:

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;

vii. Date and time of death, if applicable; and

viii. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

RESEARCH

Policy Number 15
HIPAA §§ 164.501; 164.508; 164.512

PURPOSE: Establish a Policy for When PHI may be Used for Research Purposes

APPROVED: _____ **DATE:** _____, 2019

Policy: HIPAA establishes privacy protections from human subjects research and establishes the conditions under which PHI may be used or disclosed by Practice for research purposes. This policy and procedure should be followed in addition to any applicable federal or state regulations governing the protection of human subjects research, as well as any applicable Institutional Review Board ("**IRB**") policies and procedures.

Procedure:

1. **Research.** Practice may use or disclose PHI for research, regardless of the source of the funding of the research, in the following circumstances:

(a) **Individual Authorization**. The individual has signed a valid authorization;

(b) **Board Approval of Waiver**. The IRB has approved a proper waiver of the need to obtain the individuals authorization;

(c) **Limited Data Set.** The health information is used or disclosed in a limited data set in accordance with a valid Data Use Agreement;

(d) **De-identification**. The health information has been de-identified;

(1) **Preparatory to Research**. PHI may be used or disclosed to a researcher as necessary to prepare a research protocol or for similar purposes preparatory to research if Practice obtains the following representations from the researcher: (i) the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research: no PHI will be removed from Practice by the researcher in the course of the review; and (ii) the PHI for which use or access is sought is necessary for the research purposes;

(2) **Decedent's Research**. PHI may be used or disclosed to a researcher for research on decedents if Practice obtains the following from the researcher: (i) a representation that the use or disclosure sought is solely for research on the PHI of decedents; (ii) documentation of the death of such individual(s) and/or research subject(s); or (iii) a representation that the PHI for which use or disclosure is sought is necessary for research purposes.

2. **Research Pursuant to an Authorization** Research authorizations must contain the same core elements as other authorizations, except for the following differences:

(a) Practice may condition the provision of research-related treatment on a provision of authorization for the use or disclosure of protected health information for such research;

(b) An authorization for use and disclosure of protected health information for a research study may be combined with any other type of written permission for the same research study, including another authorization for the use or disclosure of protected health information for such research or consent to participate in such research;

(c) A research authorization does not need to contain an expiration date or event as is required for other authorizations (the language "end of the research study" or "none" or similar language is sufficient).

3. **Revocation**

(a) A research authorization may be revoked by an individual.

(b) If an authorization is revoked, the Practice may continue its use or disclosure of the PHI already obtained pursuant to the valid authorization to the extent necessary to preserve the integrity of the research study.

4. **IRB Waiver Approval**

(a) For a use or disclosure to be permitted upon IRB approval, the IRB must document that all of the following criteria have been met:

(1) The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on the presence of the following elements: (i) an adequate plan to protect the identifiers from improper use and disclosure; (ii) an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and (iii) adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted under this policy;

(2) The research could not be conducted without the waiver or alteration; and

(3) The research could not be conducted without access to and use of the PHI.

(b) The documentation should include a statement identifying the IRB and the date on which the alteration or waiver of authorization was approved.

(c) The documentation should include a brief description of the PHI for which use or access has been determined to be necessary by the IRB.

(d) The documentation should include a statement that the alteration or waiver of authorization has been reviewed.

(e) The Chair of the IRB or other member designated by the Chair must sign the document.

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION

Policy Number 16
HIPAA §§ 164.502(d), 164.514(a) and (b)

PURPOSE: Establish a Policy Regarding De-identifying Patient Information

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice may use or disclose de-identified PHI without obtaining an individual's authorization. PHI will be considered de-identified if either of the two de-identification procedures set forth below are followed.

Procedure:

1. <u>Removal of Identifiers</u>

(a) De-identified PHI is rendered anonymous when identifying characteristics are completely removed and when Practice does not have any actual knowledge that the information could be used alone or in combination with other information to identify and individual.

(b) De-identification requires the elimination not only of primary or obvious identifiers, such as the individual's name, address, and date of birth, but also of secondary identifiers through which a user could deduce the individual's identity.

(c) For information to be de-identified the following identifiers must be removed:

(1) Names;

(2) All address information except for the state;

(3) Names of relatives and employers;

(4) All elements of dates (except year), including date of birth, admission date, discharge date, date of death; and all ages over 89 and all elements of dates including year indicative of such age except that such ages and elements may be aggregated into a single category of age 90 or older;

(5) Telephone numbers;

(6) Fax numbers;

(7) E-mail addresses;

(8) Social security numbers;

(9) Medical record numbers;

(10) Health plan beneficiary numbers;

(11) Account numbers;

(12) Certificate/license numbers;

(13) Vehicle identifiers, including license plate numbers;

(14) Device ID's and serial numbers;

(15) Web Universal Resource Locators (URL);

(16) Internet Protocol (IP) addresses;

(17) Biometric identifiers;

(18) Full face photographic images and other comparable images;

(19) Any other unique identifying number characteristics (except as otherwise permitted for re-identification purposes).

2. **Statistical Method** PHI is considered de-identified if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (a) determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (b) documents the methods and results of the analysis to justify such determination.

LIMITED DATA SETS

Policy Number 17
HIPAA § 164.514(e)

PURPOSE: Establish a Policy for the Disclosure of Limited Data Sets

APPROVED: _____ **DATE:** _____, 2019

Policy: A Covered Entity may use and disclose a limited data set without an individual's authorization for the purposes of research, public health, or health care operations if the Covered Entity enters into a Data Use Agreement with the intended recipient of the limited data set. A designated Covered Entity may use protected health information to create a limited data set, or to disclose protected health information to a Business Associate to create a limited data set on behalf of the Covered Entity. .

Procedure:

1. **Limited Data Set** A limited data set is PHI that excludes the following direct identifiers of the individual or relatives, employers, or household members of the individual:

   (a) Names;

   (b) Postal address information, other than town, city, state, and zip codes;

   (c) Telephone numbers;

   (d) Fax numbers;

   (e) Electronic mail addresses;

   (f) Social security numbers;

   (g) Medical record numbers;

   (h) Health plan beneficiary numbers;

   (i) Account numbers;

   (j) Certificate/license numbers;

   (k) Vehicle identifiers and serial numbers (including license plate number);

   (l) Web Universal Resource Locators (URLs);

   (m) Internet Protocol (IP) address numbers;

(n) Biometric identifiers, including finger and voiceprints; and

(o) Full face photographs and comparable images.

2. **Data Use Agreements** Data use agreements must:

(a) Establish the permitted uses and disclosures of the limited data set;

(b) Establish who is permitted to use or receive the limited data set; and

(c) Provide that the recipient of the information will:

(1) Not use or further disclose the information other than as permitted by the agreement;

(2) Use appropriate safeguards to prevent use or disclosure other than as permitted by the agreement;

(3) Report to Practice any uses or disclosures that recipient is aware of that is not provided for by the agreement;

(4) Ensure that the recipient's agents who have access to the information agree to the same restrictions as imposed on the recipient; and

(5) Not identify the information or contact the individuals.

RECORDS RETENTION

Policy Number 18
HIPAA § 164.530(j)

PURPOSE: Establish a Patient Record Retention Policy

APPROVED: _____ **DATE:** _____, 2019

Policy: Practice will maintain certain documentation regarding its HIPAA compliance, in written or electronic form.

Procedure:

1. Covered components must retain the following documentation for six years from the date of its creation or the date it was last in effect (whichever is later):

(a) **Policies and Procedures.** Any policy or procedural documentation, including notice of privacy practices, consents (if any) and authorizations, and other standard forms.

(b) **Patient Requests.** Patient requests for access, amendment, or accounting of disclosures.

(c) **Complaints.** The handling of any individual's complaints.

(d) **Workforce Training.** The processes for and content of workforce training.

(e) **Sanctions.** The handling of any sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered component.

2. If state laws require longer retention periods, the state requirements control.

RIGHT TO REQUEST CONFIDENTIAL COMMUNICATION

Policy Number 19
HIPAA § 164.522(b)

PURPOSE: Establish a Policy for Patient Requests for Confidential Communications

APPROVED: _____ **DATE:** _____, 2019

Policy: Individuals may request to receive communications of protected health information in a confidential manner (e.g., by alternative means or in alternative locations). Practice will accommodate reasonable requests to receive confidential communications, provided that an alternative address or other method of contact can be accommodated by all applicable systems and, where appropriate, information as to how payment will be handled is provided.

Procedure:

1. Requests for alternative means of confidential communications must be in writing.

2. Practice should accommodate all reasonable requests to receive confidential communications by alternative means or at alternative locations and will not require an explanation from the individual as to the basis for the request.

3. Reasonable requests include (but are not limited to) using alternative telephone numbers, alternative addresses, refraining from leaving messages on answering machines, and refraining from mailing information to the individual. Unreasonable requests are those that would be too difficult technologically or practically for the Practice HIPAA affected areas to accommodate.

4. Practice healthcare providers and/or designated staff will be responsible for receiving, processing, and responding to requests for confidential/alternative communications and for maintaining the request form in the medical record.

(a) If the request is for an alternative address, telephone or e-mail, the designated staff member may approve it at the time of request.

(b) Agreed upon requests for alternative communication must be communicated to all who may be involved in the use or disclosure of the individual's PHI.

(c) If the request for alternative communication is denied, the reason for the denial must be documented on the request form.

(d) The designated staff member will contact the patient to inform them the request was denied and the reason for the denial.

(e) Practice healthcare providers will document the acceptance or denial of an individual's request for confidential/alternative communications and maintain all documentation relating to the request in the individual's medical record.

RIGHT TO REQUEST RESTRICTIONS ON THE USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

Policy Number 20
HIPAA § 164.522(a)

PURPOSE: Establish a Policy for Patient Requests to Restrict Use and Disclosure of PHI

APPROVED: _____ **DATE:** _____, 2019

Policy: Individuals may request restrictions on the use and disclosure of their PHI. Requests for restriction do not have to be granted; if Practice believes the restriction will not limit its ability to provide quality health care treatment, obtain payment, or manage its operations, and if its information systems and procedures will permit it to comply consistently with the requested restrictions. Except as otherwise required by law, Practice will agree to restriction requests related to disclosures of protected health information to a health plan when such disclosures are for the purpose of carrying out payment or health care operations and the PHI pertains only to health care for which the costs have been paid out of pocket in full..

Procedure:

1. Request to Restrict Use or Disclosure of PHI

(a) An individual may request a restriction on the use and disclosure of his or her PHI.

(b) A covered component does not have to agree to requests for restrictions; however, if it does agree, the covered component may not use or disclose the PHI in violation of such restriction, except in emergency situations.

(c) The covered component should discuss with the individual whether the restriction should be communicated to others (i.e., other covered components of Practice or business associates who may be sending the individual communications on behalf of Practice).

2. Terminating a Restriction

(a) A restriction can be terminated if:

(1) The individual requests the restriction in writing or orally (if the termination is requested orally, it should be documented; or

(2) The designated covered component informs the individual that it is terminating the agreement to a restriction, in which case the termination will only apply to PHI created or received after the individual has been notified of the termination.

GLOSSARY OF TERMS

Authorization. The permission granted by a patient, or the patient's Personal Representative, to use Protected Health Information for specified purposes or to disclose Protected Health Information to a third party specified by the individual. An *Authorization Form* is the document that reflects this permission.

Breach. With certain exceptions, the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI.

Business Associate. With certain exceptions, a person or entity that: (1) creates, receives, maintains, or transmits PHI for a function or activity regulated by the Privacy Rule or (2) provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for Practice, or to or for an Organized Health Care Arrangement ("**OHCA**") in which Practice participates, where the provision of the service involves the disclosure of protected health information from Practice or OHCA, or from our Business Associate, to the person. A Business Associate does not include a member of the Covered Entity's Workforce nor a health care provider with respect to disclosures by the Covered Entity to the health care provider concerning the treatment of a patient. A Business Associate includes: a personal health record vendor, Health Information Organization, and an E-prescribing Gateway or other organization that provides data transmission of PHI to a Covered Entity and requires access to such PHI on a routine basis but not organizations that are mere conduits for the transport of PHI and do not access the information other than on a random or infrequent basis. A Business Associate is also a subcontractor that creates, receives, maintains or transmits PHI on behalf of a Business Associate.

Business Associate Agreement. A Covered Entity's written agreement with its Business Associate, setting forth the Business Associate's obligations related to the Covered Entity's PHI.

Correctional Institution. Any penal or correctional facility, jail, reformatory, detention practice, work farm, halfway house, or residential community program practice operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. *Other persons* held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses or others awaiting charges or trial. *Inmate* is a person incarcerated in or otherwise confined to a correctional institution.

Covered Entity. A health care provider who conducts certain financial and administrative transactions electronically for which standards have been adopted under HIPAA, such as electronic billing. Health Plans and Healthcare Clearinghouses are also Covered Entities.

Data Breach. See Practice's Data Breach Notification Policy.

Designated Record Set. A group of records that a Covered Entity uses to make decisions about individuals, and includes a health care provider's medical records. A *record,* for purposes of a Designated Record Set, means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a Covered Entity.

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

Electronic Health Record. An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

Electronic Media. (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic Protected Health Information (e-PHI). Information in an Electronic Media that comes within of the definition of PHI as specified in this section.

Family Member. An individual's: (1) dependent; or (2) any other person who is a first-degree, second-degree, third-degree, or fourth-degree relative of the individual or of a dependent of the individual. Relatives by affinity (such as by marriage or adoption) are treated the same as relatives by consanguinity (that is, relatives who share a common biological ancestor). In determining the degree of the relationship, relatives by less than full consanguinity (such as half- siblings, who share only one parent) are treated the same as relatives by full consanguinity (such as siblings who share both parents). First-degree relatives include parents, spouses, siblings, and children. Second-degree relatives include grandparents, grandchildren, aunts, uncles, nephews, and nieces. Third-degree relatives include great-grandparents, great-grandchildren, great aunts, great uncles, and first cousins. Fourth-degree relatives include great-great grandparents, great- great grandchildren, and children of first cousins.

Health Care. Health care includes, but is not limited to, the following: Preventive, diagnostic, therapeutic, rehabilitative maintenance, or palliative care, and counseling service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse. A public or private entity that either: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations. Certain administrative, financial, legal, and quality improvement activities of a Covered Entity that are necessary to run its business and to support the core functions of treatment. These activities are limited to the activities listed in the definition of "health care operations" at 45 CFR 164.501, such as : conducting quality assessment and improvement activities and case management and care coordination; reviewing the competence or qualifications of health care professionals, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities; conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs; business planning and development; and business management and general administrative activities, including those related to implementing and complying with the Privacy Rule and other HIPAA rules, customer service, resolution of internal grievances, sale or transfer of assets, and creating de-identified health information or a Limited Data Set.

Health Information. Any information, including genetic information, whether oral or recorded in any form or medium, created or received by a provider that relates to the past, present, or future physical or mental health condition of a patient; the provision of healthcare to a patient.

Health Oversight Agency. An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health Plan. An individual or group plan that provides for, or pays the cost of, medical care.

HHS. The U.S. Department of Health & Senior Services (see *Secretary*).

HIPAA. The Health Insurance Portability and Accountability Act of 1996.

HITECH. The Health Information Technology for Economic and Clinical Health Act.

Incidental use or disclosure. A secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of a use or disclosure permitted by the Privacy Rule.

Individual. The person who is the subject of Protected Health Information.

Individually Identifiable Health Information. Information, including demographic data, that

relates to (1) the individual's past, present or future physical or mental health or condition, (2) the provision of health care to the individual, or (3) the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

Institutional Review Board or IRB or Privacy Board. Within the provisions of the institutional review board (IRB) rules (21 CFR, Part 56) are requirements that the IRB ensure that there are adequate provisions to protect the privacy of research subjects and to maintain the confidentiality of research data.

Law Enforcement Official. An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) investigate or conduct an official inquiry into a potential violation of law; or (2) prosecute or otherwise conduct a criminal, civil or administrative proceeding arising from an alleged violation of law.

Limited Data Set. PHI that excludes the following direct identifiers of the individual or of relatives, employers or household members of the individual:

1. Names;
2. Postal address information, other than town or city, State, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full face photographic images and any comparable images.

Marketing. Communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

Minimum Necessary. The principle that a Covered Entity, when using or disclosing PHI, or when requesting PHI from another Covered Entity, must make reasonable efforts to limit such PHI, to the extent practicable, to the *Limited Data Set* or, if needed by the Covered Entity, to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. The Secretary of HHS will issue guidance on what constitutes "minimum necessary."

OCR. The Office for Civil Rights of the U.S. Department of Health & Human Services. OCR is the federal agency charged with enforcing the Privacy Rule and receives complaints regarding same. The OCR address for filing complaints related to Practice is the Southwest Region – (Arkansas, Louisiana, New Mexico, Oklahoma, Texas):
Office for Civil Rights
1301 Young Street, Suite 1169
Dallas, TX 75202
Customer Response Center: (800) 368-1019
Fax: (202) 619-3818
TDD: (800) 537-7697
Email: ocrmail@hhs.gov

Organized Health Care Arrangement (OHCA). An Organized Health Care Arrangement is: (1) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or (2) an organized system of health care in which more than one Covered Entity participates, and in which the participating Covered Entities: (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following: (A) utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf; (B) quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf.

Personal Representative. Under the Privacy Rule, a person authorized under State or other applicable law to act on behalf of the individual in making health care related decisions is the individual's personal representative. Except in certain limited situations specified in the Privacy Rule, a Covered Entity is required to treat an individual's Personal Representative as the individual with respect to uses and disclosures of the individual's PHI, as well as with respect to the individual's rights under the Privacy Rule.

PHI - *Protected Health Information*. Protected Health Information is individually identifiable health information that is: (i) transmitted by electronic media; (ii) maintained in any electronic medium; or (iii) transmitted or maintained in any other form or medium, but does not include certain education records covered by the Family Educational Rights and Privacy Act or employment records held by a Covered Entity in its role as an employer. A Covered Entity need only comply with the requirements of the Privacy Rule with respect to the PHI of a deceased individual for a period of 50 years following the death of the individual.

Privacy Act. The Privacy Act of 1974 (5 U.S.C., section 552A).

Privacy Contact. The person or persons designated by Practice to answer questions and provide information to patients and others about our Notice of Privacy Practices and our policies and procedures, if this role is not filled by the Privacy Officer.
Privacy Rule. The Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164.

Privacy Officer. The person designated by Practice to oversee the development and implementation of Practice's privacy policies and procedures and, where not delegated to a Privacy Contact(s), the person who receives complaints about our privacy practices and answers questions about our Notice of Privacy Practices.

Protected Health Information (PHI). *Individually Identifiable Health Information* [defined above] that is held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Public Health Authority. An agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency. Examples of a public health authority include State and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention (CDC), and the Occupational Safety and Health Administration (OSHA).

Required by Law. A mandate contained in law that compels a Covered Entity to make a use or disclosure of PHI and that is enforceable in a court of law, e.g., court orders, court-ordered warrants, subpoenas, and summons; or a civil investigative demand;.

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

Sale of PHI. With certain exceptions set forth at 45 CFR §164.502(a)(5)(ii)(B)(2), a disclosure of PHI by a Covered Entity or Business Associate, if applicable, where the Covered Entity or Business Associate directly or indirectly receives remuneration from or on behalf of the recipient of the PHI in exchange for the PHI.

Secretary. The Secretary of the U.S. Department of Health & Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Security Manual. The HIPAA Security Policy & Procedure Manual of Practice, implemented on _____, 2019.

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

Treatment. 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, from one health care provider to another, for health care.

Use. With respect to Individually Identifiable Health Information, is the sharing, employment, application, utilization, examination or analysis of such information within an entity that

maintains such information.

Workforce. Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such Covered Entity or Business Associate, whether or not they are paid by the Covered Entity or Business Associate.

FORMS

REQUEST FOR CONFIDENTIAL COMMUNICATIONS FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996, I have the right to make reasonable requests to receive confidential communications of my protected health information from The Kingsley Clinic PLLC ("**Practice**") by alternative means or at alternative locations. I understand that it is my responsibility to update the Practice of any change in the information provided below. Unless I specifically indicate otherwise below, I also understand that the requested communication, if accepted, will be the primary method of communication by the Practice. By completing and signing this form, I am requesting Practice send confidential communications as follows:

☐ Alternative manner (*Please Describe*):

_____

☐ Alternative location (*Please Specify*)

_____

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

DISCLOSURE AUTHORIZATION FORM

Protected health information is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services ("**PHI**"). As required by the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**"), The Kingsley Clinic PLLC ("**Practice**") has provided a Notice of Privacy Practices describing how it may use and disclose PHI. It is important to understand that any uses or disclosures outside those circumstances described in the notice will be made **only with your written authorization**. This means there may be circumstances where we will not disclose information to a person unless you have specifically authorized them to receive such information. Therefore, this authorization must be completed to identify those individuals who will be permitted to receive information about your medical care.

AUTHORIZATION

I authorize Practice to disclose my protected health information to those listed below (*specify name, relationship and contact information if applicable*):

_____

_____

_____

The information that can be disclosed to the above named individuals includes:

☐ All PHI

☐ Only information relating to (*specify such as appointments, etc.*):_____

_____

☐ Only information pertaining to the time period from:_____ to _____

☐ Other (*specify*):_____

This authorization will be in full force and effect for until the death of the patient unless otherwise indicated below.

☐ Expiration Date:_____

The PHI is being disclosed for the following purpose (*write "at my request" if there is no specific purpose or you do not wish to specify the purpose*):

_____

I understand that I have the right to revoke this authorization, in writing, at any time by

sending such written notification to Practice's Privacy Officer. I understand that a revocation is not effective to the extent that Practice has relied on the use or disclosure of the PHI or if my authorization was obtained as a condition of obtaining insurance coverage and the insurer has a legal right to contest a claim.

I understand that, except as otherwise provided in this authorization, Practice may use or disclose my PHI in accordance with Practice's Notice of Privacy Practices.

I understand that PHI disclosed by this authorization may be subject to re-disclosure by the recipient and may no longer be protected by the Health Insurance Portability and Accountability Act or other applicable laws or regulations.

I understand that Practice will not condition my treatment on whether I provide authorization for the requested use or disclosure except: (1) if my treatment is related to research, or (2) health care services are provided to me solely for the purpose of creating PHI for disclosure to a third party.

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

REQUEST FOR RESTRICTION FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996, I have the right to request restrictions on uses and disclosures of my protected health information for treatment, payment or healthcare operations, or disclosures to Family Members, other relatives, close personal friends, or any other person identified by me. I also understand that The Kingsley Clinic PLLC ("**Practice**") is not legally required to agree to a requested restriction unless the request is made to restrict disclosure to my insurer for purposes of payment or health care operations (and is not for purposes of treatment), and the information I am asking to restrict pertains solely to a healthcare item or service for which I have paid out of pocket in full.

By completing and signing this form, I am requesting the restriction of the use and disclosure of some or all of the protected health information in my medical record(s) as follows:

_____

_____

_____

_____

_____

_____

I understand that I will be notified of a decision regarding this request within 15 days and if the restriction is allowed, it will be maintained as part of my medical record for as long as the Practice holds the record. If approved, the Practice will not use or disclose any protected health information in violation of this restriction, except in emergency situations or to public health, government or law enforcement officials with the proper documentation.

I understand that I have the right to cancel this restriction in writing at any time. In addition, I understand that I may be informed if the restriction is ever terminated; provided, however, that any such termination is only effective as to protected health information created or received after I have been informed of such termination.

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

PRINTED NAME

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

APPROVAL OF REQUEST FOR RESTRICTION FORM

Re: Request for Restriction

Dear _____:

We are writing in follow-up to the requested restrictions on the uses and disclosures of _____ protected health information submitted to us on _____.

After our review, we have approved the restrictions requested as follows: [LIST AND SUMMARIZE THE RESTRICTIONS FROM THE REQUEST THAT HAVE BEEN APPROVED IN ORDER TO CONFIRM THE INFORMATION IS ACCURATE]

The above restrictions will be maintained as part of the medical record for as long as we hold the record. We will not use or disclose protected health information in violation of the above restrictions, except in emergency situations (if the protected health information is needed to provide the emergency treatment) or to public health, government or law enforcement officials with the proper documentation.

Our agreement to the restrictions will only be terminated if you agree to or request termination orally or in writing, or we inform you that the agreement is terminated. However, if we terminate the agreement it will only be effective as to protected health information created or received after you have been informed.

If you have any questions or concerns, please do not hesitate to contact us.

Sincerely,

_____

[**INSERT NAME**], Privacy Officer

_____

[**INSERT EMAIL ADDRESS**]

DENIAL OF REQUEST FOR RESTRICTION FORM

Re: Request for Restriction

Dear _____:

We are writing in follow-up to the requested restrictions on the uses and disclosures of __ _____'s protected health information submitted to us on _____.

After our review, we are denying the request as provided in §164.522 of the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996. Our basis for denial is as follows: **[LIST THE RESTRICTIONS FROM THE REQUEST THAT HAVE BEEN DENIED AND SUMMARIZE REASON FOR DENIAL]**

If you have any questions regarding this denial, please do not hesitate to contact us.

Sincerely,

_____

[INSERT NAME], Privacy Officer

_____

[INSERT EMAIL ADDRESS]

RECORDS REQUEST FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996 I have the right to obtain a copy of my protected health information or choose to get a summary of my protected health information in lieu of a copy. I understand that Practice is allowed to charge me for copying my medical record. I understand that, unless otherwise provided by law, the cost of the copy may not exceed $25 for the first twenty pages and fifty cents ($0.50) per page for every copy thereafter. If the information is in electronic format and the request is for an electronic copy to be transmitted electronically, the cost of the copy may not exceed $25 for 500 pages or less and $50 for more than 500 pages. A reasonable fee of up to $15 may be charged for executing an affidavit upon request. I understand that my request will not be fulfilled until I have paid the full amount due. Practice may not charge a fee for my medical records if the request is related to a benefits or assistance claim based on a disability.

By completing and signing this form, the protected health information I am seeking is:

☐ Entire medical record
☐ Only information relating to:_____
☐ Only information occurring from:_____ to _____
☐ Other (specify):_____

For the protected health information described above, I request:

☐ Regular copy
☐ Summary

I request Practice provide me the information in the following form:

☐ Paper copy
☐ Electronic copy (*Specify Form*):_____

If approved, I will:

☐ Pickup
☐ Pay for delivery to (*Specify Delivery Method and Delivery Information*):

_____

_____

If approved, Practice may contact me at the following telephone number:

_____

If denied, Practice may send the written denial to the following address:

_____

_____

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

ACCESS TO RECORDS REQUEST FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996, I have the right to read and examine my protected health information. I understand that I will be provided a place to review the information away from others and may have one additional person of my choosing accompany me, but a member of Practice will remain present during the review to ensure that the information remains intact and unaltered.

By completing and signing this form, the protected health information I am seeking is:

☐ Entire medical record
☐ Only information relating to:_____
☐ Only information occurring from:_____ to _____
☐ Other (specify):_____

My available dates and times within the next 5 business days to inspect the information described above:

_____

_____

If approved, Practice may contact me at the following telephone number for scheduling:

_____

_____

If denied, Practice may send the written denial to the following address:

_____

_____

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

DENIAL OF RECORDS REQUEST FORM

Re: Records Request

Dear _____:

We are writing in follow-up to the requested access to or copy of protected health information for _____ submitted to us on _____.

After our review, we are denying the request as provided in §164.524(d) of the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996. Our basis for denial is as follows: **[DESCRIBE REASON FOR DENIAL]**

***[USE IF APPLICABLE]** You do have the right to request a review of this denial by a licensed health care professional designated by us who did not participate in the original decision regarding this denial whose determination will be final and binding. Please initial and sign below and return this form to us for our records.

_____ I am requesting a review of this denial of access to or copy of protected health information.

_____
PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE)

***[USE IF APPLICABLE]** You do not have the right to request a review of this denial.

You may file a written complaint with us at the address above, attention - Privacy Officer, or to the Department of Health and Human Services, Office for Civil Rights at: Office for Civil Rights, Southwest Region by mail at 1301 Young Street, Suite 1169, Dallas, Texas 75202, by telephone at (800) 368-1019 or (800) 537-7697 (TDD), or by facsimile at (202) 619-3818. You may also file a written complaint with the Texas Medical Board, Mail Code 261, P.O. Box 2019, Austin, Texas 78768-2019.

If you have any questions regarding this denial, please do not hesitate to contact us.

Sincerely,

_____
[INSERT NAME], Privacy Officer

_____
[INSERT EMAIL ADDRESS]

REQUEST TO AMEND RECORDS FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996 I have the right to request The Kingsley Clinic PLLC ("**Practice**") to amend or correct my protected health information to the extent legal and ethically permissible. I also understand that I will be notified of Practice's decision regarding the requested amendment within 60 days, as allowed by law. By completing and signing this form, I am requesting my protected health information be amended as follows (*attached separate sheet if necessary*):

_____

_____

_____

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

REQUEST FOR ACCOUNTING FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
REQUESTED BY:	**RELATIONSHIP:**	
PHONE:	**PHONE 2:**	

I understand that under the Health Insurance Portability and Accountability Act of 1996 I have a right to receive an accounting of the disclosures of protected health by The Kingsley Clinic PLLC ("**Practice**") in the last six years. I also understand that the right to an accounting does not include disclosures made: (i) to carry out treatment and health care operations; (ii) to me; (iii) pursuant to an authorization provided by me; (iv) to a Family Member, other relative, close personal friend, or any other person identified by me related to their involvement with my care for my health care services or to notify or assist in the notification of my location or general condition to such person; (v) for national security or intelligence purposes; (vi) to correctional institutions or law enforcement officials; or (vii) as part of a limited data set. By completing and signing this form, I am requesting an accounting and I understand that I will be notified regarding this request within 60 days by telephone at the number above.

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

BUSINESS ASSOCIATE AGREEMENT

The undersigned business associate executing this Agreement as set forth on the signature page ("**Business Associate**") and The Kingsley Clinic PLLC, a Texas professional limited liability company ("**Covered Entity**") enter into this Business Associate Agreement ("**Agreement**") to be effective as of the date set forth on the signature page ("**Effective Date**") (Business Associate and Covered Entity, each a "**Party**," collectively, the "**Parties**"). Capitalized terms used, but not otherwise defined in this Agreement, have the same meaning as those terms in the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Part 160 and Part 164 ("**HIPAA Rules**").

Recitals

A. Business Associate and Covered Entity are engaged in a business relationship where Covered Entity purchases, and Business Associate sells or provides, certain services to Covered Entity ("**Business Arrangement**").

B. In performance of its obligations under the Business Arrangement, Business Associate creates, receives, maintains, or transmits, or otherwise uses or discloses Protected Health Information.

C. As required by the HIPAA Rules, the Parties desire to enter into this Agreement regarding the use and disclosure of Protected Health Information which will be in accordance with the HIPAA Rules and in addition, the Texas Health and Safety Code Chapters 181 and 182 and Texas Business and Commerce Code Section 521, both as amended by HB 300 (82nd Legislature) effective September 1, 2012, including any implementing regulations (collectively, "**Texas Law**").

Based upon the above recitals and the mutual covenants in this Agreement, the Parties agree as follows:

Article 1

Use, Disclosure & Obligations

1.01. **Permitted Uses and Disclosures.** Except as otherwise provided in this Agreement:

(a) Business Associate may use or disclose Protected Health Information as necessary to perform the services required by the Business Arrangement or as required by law;

(b) Business Associate agrees to make uses and disclosures and requests for Protected Health Information in accordance with the "minimum necessary" principle described in the HIPAA Rules (i.e. only Protected Health Information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request may be used or disclosed);

(c) Business Associate may use and disclose Protected Health Information to de-identify the information in accordance with 45 C.F.R. 164.514(a)-(c), but only if (1) the precise

use is disclosed to Covered Entity and permitted by Covered Entity in its sole discretion, and (2) the de-identification is in compliance with 45 C.F.R. § 164.502(d), and any such de-identified health information meets the standards and implementation specifications for de-identification under 45 C.F.R. 164.514, or such regulations as they may be amended from time to time. Notwithstanding anything to the contrary, Business Associate will not attempt to re-identify any information in violation of Texas law regardless of whether such action is on behalf of or permitted by the Covered Entity;

(d) Business Associate may use Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate provided that such use is permitted under the HIPAA Rules, Texas Law, and other federal and state laws;

(e) Business Associate may disclose Protected Health Information for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom Protected Health Information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of Protected Health Information has been breached;

(f) Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. 164.504(e)(2)(i)(B);

(g) Except as permitted by subsections (d)-(f) above, Business Associate may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity; and

(h) Business Associate may not sell Protected Health Information nor use Protected Health Information for marketing purposes in such a manner as to violate Texas Law.

1.02. **Responsibilities of Business Associate.** With regard to the use or disclosure of Protected Health Information, Business Associate agrees to:

(a) Not use or disclose Protected Health Information other than as permitted or required by the Business Arrangement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information, to prevent the use or disclosure of Protected Health Information other than as provided for by the Business Arrangement;

(c) Report to Covered Entity any use or disclosure of Protected Health Information not permitted by the Business Arrangement of which it becomes aware or any Security Incident of which it becomes aware, without unreasonable delay but in no event more than 48 hours after it becomes aware;

(d) Report to Covered Entity any Breaches of Unsecured Protected Health Information, including the identity of the affected individual(s) and all other relevant information required by 45 C.F.R. 164.410 and Texas Law, without unreasonable delay but in no event more than 5 business days after it becomes aware of such Breach;

(e) In accordance with 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that all Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of Business Associate agree in writing to the same restrictions, conditions, and requirements that apply to Business Associate with respect to such information;

(f) Make available to Covered Entity within 5 business days after receipt of request by Covered Entity, Protected Health Information in a Designated Record Set in order to meet the requirements under 45 C.F.R. 164.524. To the extent that Business Associate receives a written request for such access directly from an individual, Business Associate will promptly notify Covered Entity and reasonably cooperate with Covered Entity in meeting the requirements under 45 C.F.R. §164.524 with respect to such individual;

(g) Make any amendment(s) within 15 business days after receipt of direction by Covered Entity to Protected Health Information in a Designated Record Set that Covered Entity directs pursuant to 45 C.F.R. 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 C.F.R. 164.526. To the extent Business Associate receives a written request for such amendment(s) directly from an individual, Business Associate will promptly notify Covered Entity and reasonably cooperate with Covered Entity in meeting the requirements under 45 C.F.R. §164.526 with respect to such individual;

(h) Maintain and document the information necessary to provide an accounting of disclosures as required under 45 C.F.R. § 164.528;

(i) Make available to Covered Entity within 15 business days after receipt of request by Covered Entity such information described in subsection (h) above to permit Covered Entity to satisfy its obligations under 45 C.F.R. § 164.528. To the extent Business Associate receives a written request for such accounting directly from an individual, Business Associate will promptly notify Covered Entity and reasonably cooperate with Covered Entity in meeting the requirements under 45 C.F.R. §164.528 with respect to such individual;

(j) To the extent Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 C.F.R. Part 164, comply, with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s);

(k) Make internal practices, books, and records available to Covered Entity or to the Secretary of the Department of Health and Human Services or their designee ("**Secretary**"), for purposes of determining compliance with the HIPAA Rules. Business Associate will promptly notify Covered Entity of communications with the Secretary regarding Protected Health Information provided by or created by Covered Entity and will provide Covered Entity with copies of any information Business Associate has made available under this provision. Notwithstanding

the foregoing, no attorney-client, accountant-client, or other legal privilege will be deemed waived by Business Associate or Covered Entity by virtue of this Agreement;

(l) Provide the necessary training to its members of its workforce required by the HIPAA rules, Texas Law, other applicable federal and state laws, and this Agreement relating to the use, disclosure, and protection of Protected Health Information;

(m) Review and understand the HIPAA rules, Texas Law, other applicable federal and state laws, and this Agreement as they apply to Business Associate and comply with applicable requirements and any amendments affecting the obligations of Business Associate; and

(n) Comply with the requirements and obligations of which Business Associate receives notification pursuant to Section 1.03.

1.03. **Responsibilities of Covered Entity.** Covered Entity will:

(a) Notify Business Associate of any limitation(s) in its notice of privacy practices that Covered Entity produces in accordance with 45 C.F.R. 164.520 to the extent that such limitation may affect Business Associate's permitted or required uses or disclosures of Protected Health Information, as well as any changes to such notice;

(b) Notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose their Protected Health Information, if such changes affect Business Associate's permitted or required uses or disclosures.

(c) Notify Business Associate of any restriction on the use or disclosure of Protected Health Information that Covered Entity has agreed to or is required to abide by in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's permitted or required uses or disclosures of Protected Health Information;

(d) Notify Business Associate, in writing, of any amendment(s) to the Protected Health Information in the possession of Business Associate and inform the Business Associate of the time, form, and manner in which such amendment(s) will be made; and

(e) Inform Business Associate of any opt-outs exercised by any individual from marketing or fundraising activities of the Covered Entity when the Business Arrangement pertains to marketing or fundraising.

Article 2

Term and Termination

2.01. **Term.** The term of this Agreement will be effective as of the Effective Date and will terminate upon termination of the Business Arrangement or earlier if terminated in accordance with Section 2.02 below.

2.02. **Termination for Cause.** Covered Entity may terminate this Agreement upon notice to Business Associate if Covered Entity determines that Business Associate has breached a material term of this Agreement and Business Associate fails to cure the breach within 10 days of receipt of notice describing the breach. If Covered Entity determines the breach is not curable as determined by Covered Entity in its sole discretion, Covered Entity may terminate this Agreement immediately upon notice without any opportunity to cure.

2.03. **Effect of Termination.**

(a) Except as permitted by subsection (b) below, upon termination of this Agreement for any reason, Business Associate will, as specified by Covered Entity, return or destroy all Protected Health Information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that Business Associate still maintains in any form. If instructed to destroy, Business Associate agrees that all paper, film or other hard copy media will be shredded or destroyed such that it may not be reconstructed, and electronic Protected Health Information will be purged or destroyed in accordance with National Institute for Standards and Technology Guidelines for media sanitization. However, in the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate will provide in writing to Covered Entity notification of the conditions that make return or destruction infeasible. Upon mutual written agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate will extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

(b) In the event Business Associate uses or discloses Protected Health Information for its own management and administration or to carry out its legal responsibilities as permitted by Section 1.01(d) and (e) above and Business Associate needs to retain Protected Health Information for such purposes after termination of this Agreement, Business Associate will:

(1) Retain only that Protected Health Information which is necessary to continue Business Associate's proper management and administration or to carry out its legal responsibilities;

(2) As specified by Covered Entity, return or destroy the remaining Protected Health Information that Business Associate still maintains in any form;

(3) Continue to use appropriate safeguards and comply with Subpart C of 45 C.F.R. Part 164 with respect to electronic Protected Health Information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section 2.03, for as long as Business Associate retains the Protected Health Information;

(4) Not use or disclose the Protected Health Information retained other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out in Section 1.01(d) and (e) which applied prior to termination; and

(5) As specified by Covered Entity, return or destroy the Protected Health Information retained when it is no longer needed for Business Associate's proper management and administration or to carry out its legal responsibilities.

(c) The obligations under this Section 2.03 will survive termination of this Agreement.

Article 3

Additional Provisions

3.01. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA rules, and other applicable federal and state laws. Amendments of this Agreement will not be binding unless such amendment is in writing and signed by a duly authorized representative of each Party.

3.02. **Governing Law.** This Agreement will be governed by Texas law (without reference to its rules as to conflicts of law).

3.03. **Waiver of Trial by Jury.** THE PARTIES WAIVE TRIAL BY JURY IN ANY JUDICIAL PROCEEDING INVOLVING ANY DISPUTE ARISING OUT OF OR RELATING TO THIS AGREEMENT.

3.04. **Waiver.** The failure of either Party to insist in one or more instances upon performance of any terms of this Agreement will not be construed as a waiver of future performance required by the term. No term of this Agreement may be waived except by written consent of the waiving Party. All remedies, rights, undertakings, and obligations contained in this Agreement will be cumulative and none of them will be in limitation of any other remedy, right, undertaking, or obligation of a Party.

3.05. **Entire Agreement.** This Agreement and the terms of the Business Arrangement constitute the complete and exclusive statement of the agreement of the Parties with respect to the subject matter of this Agreement and supersedes all prior proposals, understandings, and agreements, whether oral or written, between the Parties with respect to the subject matter of this Agreement.

3.06. **Severability.** The provisions of this Agreement are severable. The invalidity, in whole or in part, of any provision of this Agreement will not affect the enforceability of any other provisions. If one or more provisions of this Agreement are declared unenforceable, the remaining provisions will be enforceable and will be construed in the broadest possible manner to effectuate the purposes of this Agreement.

3.07. **Rules of Construction.**

(a) **Interpretation.** Neither Party will be deemed the drafter of this Agreement despite the possibility that one Party or its representatives may have prepared the initial draft or played a greater role in the preparation of subsequent drafts. In construing this Agreement, no provision will be construed in favor of one Party on the ground that such provision was drafted by the other Party. If any claim is made by a Party relating to any conflict, omission, or ambiguity in the provisions of this Agreement, no presumption, burden of proof, or persuasion will be implied because this Agreement was prepared by or at the request of either Party or its counsel.

(b) **Captions.** The headings and captions of this Agreement are inserted for reference convenience and do not define, limit or describe the scope or intent of this Agreement or any particular section, paragraph, or provision of this Agreement.

(c) **Include Not Limiting.** Unless otherwise provided, the words "include(s)," "included," or "including" do not limit the preceding words or terms.

(d) **Pronouns.** Pronouns in this Agreement refer to the masculine, feminine, neuter, singular or plural as the context will require.

3.08. **Counterparts.** This Agreement may be executed in any number of counterparts. This Agreement may be executed by facsimile signature or any electronic signature complying with the U.S. federal ESIGN Act of 2000 (e.g., www.docusign.com)..

3.09. **Notices.** All notices required or permitted under this Agreement will be in writing (including electronic form) and will be delivered to the address set forth by each Party in this Agreement, or to such other party and/or address as any of the Parties may designate in a written notice served upon the other Party. Each notice will be given and will be effective: (a) if delivered by hand, when so delivered; (b) if delivered by nationally recognized overnight courier service or sent by United States Express Mail, upon confirmation of delivery; (c) if delivered by certified or registered mail, on the third following day after deposit with the United States Postal Service; (d) if delivered by facsimile, upon confirmation of successful transmission; or (e) if delivered by email, upon confirmation of receipt by the other Party in writing by return email.

3.10. **Interpretation.** Any ambiguity in this Agreement will be resolved to permit compliance with the HIPAA Rules. In the event there is a conflict between any provision or obligation under this Agreement, the HIPAA Rules, or Texas Law, the Parties agree that the most stringent requirement regarding protection of Protected Health Information will apply.

3.11. **No Third Party Beneficiary.** Nothing in this Agreement is intended, nor will be deemed, to confer any benefits on any third party.

3.12. **Effect of Agreement.** Except as amended by this Agreement, the terms and provisions of the Business Arrangement will remain in full force and effect.

3.13. **Legal Costs and Expenses.** In the event that any suit or legal proceeding is instituted concerning or arising out of the Agreement, the substantially prevailing party will be entitled to all of such Party's costs, including, without limitation, the court costs and reasonable attorneys' fees incurred in each and every such action, suit or proceeding, including any and all appeals.

(Signature Page Follows)

The Parties have executed this Agreement duly authorized to be effective as of the Effective Date.

COVERED ENTITY

The Kingsley Clinic PLLC

By:_____
James Kingsley, M.D., Manager

_____
Effective Date

BUSINESS ASSOCIATE

[Signature block for entities]

_____
(Print Name of Entity)

By:_____
(Signature)

_____
Printed Name, Title

[Signature block for individual]

_____
(Signature)

_____
(Print Name of Individual)

COMPLAINT FORM

PATIENT NAME:		
DATE OF BIRTH:	**SSN:**	
ADDRESS:		
CITY:	**STATE:**	**ZIP:**
PHONE:	**PHONE 2:**	
PREFERRED CONTACT: ☐ **PHONE** ☐ **PHONE 2** ☐ **OTHER:** _____		
SUMMARY (*PROVIDE SUFFICIENT INFORMATION, INCLUDING NAMES AND DATES, TO ALLOW FOR A THOROUGH INVESTIGATION OF YOUR COMPLAINT*)**:**		
DESIRED RESOLUTION *(DESCRIBE HOW YOU WOULD LIKE YOUR COMPLAINT ADDRESSED. PLEASE NOTE THAT WE DO NOT GUARANTEE THAT YOUR COMPLAINT WILL BE ADDRESSED ACCORDINGLY AS WE RESERVE SOLE DISCRETION AS TO THE RESOLUTION BASED ON THE CONCLUSION OF OUR INVESTIGATION)***:**		

_____ _____

PATIENT SIGNATURE (OR PERSONAL REPRESENTATIVE) **DATE**

_____

PRINTED NAME

_____

PERSONAL REPRESENTATIVE'S AUTHORITY (IF APPLICABLE)

FOR OFFICE USE ONLY
WE WILL MAKE A GOOD FAITH EFFORT TO OBTAIN A WRITTEN COMPLAINT FROM THE INDIVIDUAL. IF AN INDIVIDUAL IS UNWILLING OR UNABLE TO COMPLETE AND SIGN THIS FORM, THE GOOD FAITH EFFORTS TO OBTAIN SUCH FORM AND REASON WHY THE FORM WAS NOT OBTAINED MUST BE DOCUMENTED.
REASON:
FORM COMPLETED BY: