HIPAA PRIVACY MANUAL

for

Pediatric Medicine of Wallingford

Disclaimer:

The information provided in this document does not constitute, and is no substitute for, legal or other professional advice. Users should consult their own legal and other professional advisors for individualized guidance regarding the application of the law to their particular questions or situations, and in connection with other compliance-related concerns.

****

Note about HIPAA Compliance:

These materials ("HIPAA Privacy Manual") are designed to meet the requirements of the HIPAA Privacy Rule and HIPAA Breach Notification Rule. Practice must also comply with the HIPAA Security Rule, which generally has not been altered by the January 25, 2013 HITECH update to HIPAA.

HIPAA PRIVACY MANUAL
Table of Contents

List of Policies

List of Appendices

- Appendix E: Complaint Process and Breach Response Plan, with Instructions for Breach Notification
- Appendix F: Requests for a Restriction on Disclosures to a Health Plan
- Appendix G: Patient Directed Release of Records Directly to Patient or to a Designated Person
- Appendix H: Special Rules for Subpoenas, Litigation, and Law Enforcement Disclosures
- Appendix I: HIPAA Workforce Training Log
- Appendix J: Privacy Officer Requirements
- Appendix K: Privacy Contact Information
- Appendix L: HIPAA Privacy Rule
- Appendix M: FAQs, Resources, and Other HIPAA Reference Materials
- Appendix N: OCR Publication: “When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved in Your Care”
- Appendix O: PowerPoint Training Presentation: “HITECH Changes to HIPAA 2013”
- Appendix P: HIPAA Audit Tools

Policy:	**General Policy Issues – Privacy of Patient Information**	
Purpose:	**To outline Practice's general position on implementation or compliance with HIPAA and other privacy laws.**	
Related Materials:	**Appendix E:**	**Complaint Process and Breach Response Plan, with Instructions for Breach Notification**
	Appendix I:	**HIPAA Workforce Training Log**
	Appendix J:	**Privacy Officer Requirements**
	Appendix K:	**Privacy Contact Information**
	Appendix L:	**HIPAA Privacy Rule**
	Appendix M:	**FAQs, Resources, and Other HIPAA Reference Materials**
	Appendix P:	**HIPAA Audit Tools**

Pediatric Medicine of Wallingford (which will be referred to throughout these policies as "Practice") will implement the required elements of the HIPAA Privacy Rule (beginning on April 14, 2003) and will use various policies, procedures and documentation as required by HIPAA. These policies shall be maintained in a notebook/manual, along with appendices, to assist in compliance.

> These policies use the term "patient" to refer to the individual who is the subject of a health record (HIPAA uses the term "individual" instead of patient). For an office-based pediatric practice, in many instances, the person who is able to authorize release of, or demand access to, a patient's record is a parent or guardian.

The Practice's HIPAA policies relating to Privacy were revised consistent with the HIPAA Rules updates published January 25, 2013, effective September 23, 2013. Consistent with those updates, the policies of the Practice will reference "HIPAA Rules" as including the HIPAA Privacy, Security, Breach Notification, and Enforcement rules.

Continuing compliance with HIPAA will be achieved through ongoing assessment, oversight and informational training, as coordinated through the Privacy Officer.

Pledge to Comply with HIPAA Privacy, Internal Controls:

Practice respects the rights of individuals, including employees, to make complaints, ask questions, or inquire as to the Practice's compliance with HIPAA and other privacy laws. Practice will address all complaints received from patients, clients, employees or third parties in an expeditious and meaningful manner. No adverse action or retaliation shall be taken against any such individual or employee based on any legitimate complaint, question, or inquiry.

- Note: the Breach Rule, as outlined in the HIPAA Rules, shall be observed. A Breach Response Plan and instructions for investigating and processing possible breaches, and reviewing any complaints, is found at **Appendix E**.

Workforce and Training:

Practice will identify those members of its workforce that require access to protected health information to perform their duties, specify the protected health information to which they require access, and make reasonable efforts to limit their access accordingly. The minimum necessary standard will be observed.

All workforce members, including new employees, will be trained in HIPAA rules. Training will occur on a periodic basis to ensure continued compliance. Retraining will address significant changes that occur affecting HIPAA or privacy practices of Practice. **Appendix I** may be used to document workforce HIPAA training.

Practice will train all workforce members to inform the Privacy Officer (or a supervisor) of any issues, concerns, possible breaches, or HIPAA-related questions or comments that they may have.

Enforcement and Sanctions:

Employees who fail to follow HIPAA requirements and/or Practice's policies with respect to privacy rules, shall be sanctioned appropriately. Such sanctions may range from oral reprimand to termination. Any intentional breach of patient confidentiality not permitted by law shall be severely punished, likely resulting in dismissal.

- All such HIPAA-related sanctions shall be documented, in writing, by Practice as personnel matters.

Note: See **Appendix E** (Complaint Process and Breach Response Plan, with Instructions for Breach Notification) for specific instructions on when employees are "whistleblowers" or acting within legal authority.

Remediation:

To the extent practicable, Practice will mitigate the harmful effects of any known use or disclosure, by itself or its business associates, that is in violation of the Privacy Rule and/or the Practice's policies and procedures. Additionally, **Appendix E** contains a Breach Response Plan, including instructions for breach notification, should a breach occur.

Privacy Officer:

The Privacy Officer shall implement necessary procedures or protocols to ensure that HIPAA compliance is maintained, including implementation and ongoing compliance with the rights set forth in Practice's published Notice of Privacy Practices. Such procedures and protocols may range from informal work processes to formal implementation policies. The Privacy Officer shall work with the governing body of Practice to implement major decisions. **Appendix J** provides a job description for the Privacy Officer.

There shall, at all times, be an appointed Privacy Officer, whose name shall be logged consistent with the Documentation Obligations and Log policy of the Practice.

There will also be a designated Privacy Contact, as outlined in **Appendix K**.

HIPAA Final Rule and Citations:

Although this set of polices is designed to create pathways and HIPAA-compliant operations that incorporate HIPAA Rules, it may be useful from time-to-time to review the actual HIPAA Rules and their corresponding commentary. To assist in locating the rules, there are bracketed citations in this policy set that refer to the HIPAA Rules, a copy of which is found at **Appendix L**. There are also FAQs, resources, and other helpful reference materials found at **Appendix M**.

Policy:	**Acknowledgment of Notice of Privacy Practices**	
Purpose:	**To implement the process for providing the Notice of Privacy Practices to patients, and to describe when an acknowledgment is required and the manner in which an acknowledgment should be obtained from individuals.**	
Related Materials:	**Appendix A:**	**Notice of Privacy Practices**
	Appendix B:	**Acknowledgment of Receipt of Notice of Privacy Practices**

Practice is a health care provider with a direct treatment relationship with its patients. HIPAA, therefore, requires the Practice to provide a Notice of Privacy Practices (NOPP) to each patient, consistent with the HIPAA Privacy Rule. A copy of the NOPP is found at **Appendix A**.

The offering of the NOPP is documented by a patient acknowledgment of receipt of the NOPP. The following applies to the NOPP and acknowledgment process.

Practice must:

- Provide a NOPP to the patient on his/her first visit, following April 14, 2003, or as soon as practicable after an emergency treatment situation (after the emergency has ended);

- Make a good faith effort to obtain a written acknowledgment from the patient that he/she has received a copy of the NOPP or, if unable to obtain an acknowledgment from the individual, document the good faith efforts used in seeking the acknowledgment and the reasons why an acknowledgment was not obtained. **Appendix B** contains the form to be used for documentation;

  - Note: If Practice presents the patient with a NOPP and the patient refuses to sign an acknowledgment, HIPAA allows Practice to document the good faith efforts used in trying to obtain an acknowledgment. **Appendix B** is the form that will be used to document that the NOPP was offered.

- Post the NOPP in a clear and prominent location within the office where it is visible to all patients;

- Post the NOPP on any website that where Practice maintains general information;

- Provide an individual receiving an electronic NOPP with a paper copy upon request;

- Make the NOPP available at a physical service delivery site of Practice;

- Make the NOPP available if and when the NOPP is revised and the patient requests a revised copy.

The HIPAA acknowledgment is not consent for treatment, but rather pertains to the permissible uses and disclosures of patients' information in the course of treatment, payment or health care operations.

See Appendix A, for a copy of the NOPP. See Appendix B, for a copy of the Acknowledgment form.

Policy:	**Authorization for the Use/Disclosure of Protected Health Information Determination - When Required**
Purpose:	**To provide the circumstances under which an individual's authorization is (or is not) required for the use and/or disclosure of protected health information.**
Related Materials:	**Appendix D: Authorization for Release of Medical Records**

Usually, a HIPAA compliant authorization is required for any disclosure of protected health information that a health care provider makes outside of the context of treatment, payment, or health care operations.

- Operational note: An authorization for release of records should not be combined with other forms or permissions. The reason is to ensure that the patient understands what he or she is signing, and to avoid capturing a signature that the patient intended for some other purpose.

- Patients may request restriction of uses and disclosures in the context of treatment, payment or health care operations. Such restrictions might include:

  - A patient who has requested that the Practice not disclose a particular treatment or visit to a person who is otherwise involved in the patient's care or payment of the patient's care.

- Practice will consider any such requests, but is not required to honor them, except as outlined in the "Requests for Restrictions on Disclosures to Health Plans" policy.

Patients have a right to access their own records, without signing an authorization, and a right to instruct that their records be disclosed to third parties, as outlined in the policy: "Access to Records and Protected Health Information."

- Note: Practice is responsible for verifying the identity of any person requesting access to – or claiming authority to access – records. Verification of identity should be based on a reasonable review of the circumstances (e.g., comparing signatures on file, asking to see a State investigator's identification).

Outside of treatment, payment or health care operations, Practice should not disclose protected health information ("PHI") without an authorization unless one of the following exceptions applies:

- To conduct limited discussions, involving health information, with the patient while family and close friends are present, if the patient agrees and has been given an opportunity to object. If the patient is not present, or is unable to consent because of incapacity or an emergency situation, the provider may make such a disclosure if, in his/her professional judgment, it is in the best interests of the patient [164.510];

- To disclose PHI to the extent it is required by law (including disclosure to a local, state, or federal agency in compliance with a reporting duty) [164.512];

- To disclose PHI to a health oversight agency for activities authorized by law [164.512] -- this includes requests from the Department of Public Health and the Medical Examining Board;

- To disclose PHI pursuant to a court order, or in limited circumstances, in response to a subpoena [164.512] - See **Appendix H** for instructions on response to subpoenas, litigation, and law enforcement requests;

- To disclose PHI to law enforcement officials, particularly where the disclosure is necessary to report a crime [164.512] - See **Appendix H** for instructions on response to subpoenas, litigation, and law enforcement requests;

- To disclose PHI to a coroner or medical examiner for the purpose of identifying the decedent or determining the cause of death [164.512];

- To disclose PHI to an organ procurement organization for the purposes of organ or tissue donation [164.512];

- To disclose PHI in an emergency treatment situation [164.512];

- To disclose PHI for specialized governmental functions (including disclosure to federal officials for national security and intelligence purposes, and disclosure to armed forces personnel for purposes of a military mission) [164.512];

- To disclose PHI for purposes of complying with laws pertaining to workers' compensation [164.512];

- To disclose childhood immunization information to a school official when the Practice receives consent from the parent (or the patient if the child is the decision-maker), and the Practice documents receiving the consent. This consent may be verbal or through a written authorization, at the Practice's discretion [164.512];

- To disclose to a public or private entity (such as the Red Cross) to assist with disaster relief efforts [164.510(b)(4)];

- To disclose information that is not PHI under the HIPAA rules.

    - Note: records of deceased patients are still protected by HIPAA until fifty (50) years after death. (State privacy laws might still affect such older records.) The Practice is not required to keep records for longer than its normal retention period.

The following disclosures also do not require an authorization, but usually would not apply to the office-based pediatric practice. They are offered for reference in furtherance of a full understanding the HIPAA Privacy Rule:

- To disclose psychotherapy notes to the extent that only the creator of the notes will access them for treatment purposes [164.508];

- Hospital- or facility-based (for reference): To release patient information for use in a facility's directory. The information must be limited to patient name, patient location, and general condition. The patient must be given an opportunity to restrict or prohibit disclosure [164.510].

See Appendix D for a copy of the form of Authorization to be used by Practice for release of records.

- Note: while it is preferable to use the form in **Appendix D**, a patient can direct the disclosure of his/her record by providing an authorization that contains all of the essential HIPAA elements (in plain language), which are the following:

  - Name of entity/entities to being authorized to release
  - Signed & dated by the patient or their authorized representative
  - Purpose of release
  - To whom being released
  - Brief description of what is being disclosed
  - Expiration date or expiration event
  - Required statements: Right to revoke statement, re-disclosure warning, cannot condition care on signing

  An authorization with all of these elements will be considered a valid HIPAA Authorization.

Any outside authorization received will be reviewed to ensure that these essential elements are included before records may be disclosed. If the outside authorization is not complete, the patient/requestor will be given Practice's Authorization (**Appendix D**) for completion.

Implementation Notes:

These implementation notes include both HIPAA and Connecticut-specific rules for responding to record requests.

- Practice has 30 days to provide the records from the time of receipt of a valid request.

- Note: The response time may be shorter if directed by a court order or other official demand, such as from a licensing board.

- Practice must allow for live inspection of the record if the patient or representative has authorized it. Practice has 30 days, from the time of the receipt of the request, to arrange for inspection the records.

- The maximum charge for copies of the record is $.65 per page of records provided. There are no mandatory fees for records provided in connection with a social security disability application or proceeding. The patient and/or the patient's lawyer should not be charged for such records. Practice, however, may submit an invoice to the social security office, at its discretion, outlining the copying fees.

Policy:	**Minimum Necessary Standard (including discussion of incidental disclosures)**
Purpose:	**To require adherence to the minimum necessary standard and identify the difference between incidental and improper disclosures.**

Every HIPAA covered entity (and business associate) must follow the minimum necessary rule for payment and health care operations, which means that Practice must make a reasonable effort to limit use and disclosure of, and responses to requests relating to, protected health information, to the minimum necessary to accomplish the intended purpose. Practice shall inform each workforce member as to his or her role, and the corresponding amount of PHI he or she will be permitted to access to perform his or her job.

- Important note: The minimum necessary standard **does not** apply: to activities related to treatment; in response to a valid authorization; or to the extent another rule or law requires the use or disclosure. It is most commonly applied to payment activities (for example, coding and patient invoicing), and Practice's other day-to-day business activities (for example, reviewing quality measures using patient data).

The following are examples of a ***failure*** to follow the minimum necessary standard, and each would be a potential HIPAA violation:

Example: Allowing an employee unimpeded access to patient files, where such access is not necessary for the employee to perform his/her job.

Example: Displaying patient name along with any other personal information, or reference to the patient's medical condition, where reasonable safeguards have not been used to try to protect the information.

- Note: A patient's name on a sign-in in sheet, or calling out a patient's name in the waiting room, is permitted (but should not include other information along with the name, such as medical condition, address, insurance, or phone number).

Example: Charts left unattended at a central desk where visitors and patients sometimes walk without escort.

Example: Physicians chatting about a patient, naming the patient, or discussing other details about the patient's care, in the hallway (or elevator, or parking lot), specifically in an area where patients, vendors and others could easily overhear them.

Distinguish the above examples from the following, which ***would be permitted*** under the rules:

Example: A provider instructs a staff member to bill a patient for a particular procedure and is overheard by someone in the waiting room, but the provider made a reasonable effort not to be overheard and reasonably limited the information that was shared with the staff member.

Example: Sign-in sheets and calling out names in the waiting room. The information disclosed must be appropriately limited, i.e., the sign-in sheet does not display medical information that is unnecessary for the purpose of signing in (e.g., the patient's condition).

Example: Charts placed near an exam room, but not in open view. Provider and staff ensure that the area is supervised, escort non-employees in the area, or place the patient chart with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by.

Example: Patient walks by light board while physician is examining an X-ray. If an X-ray is accidentally viewed by the patient, but reasonable safeguards are usually in place to avoid such an occurrence, then the disclosure is incidental and not a violation of the HIPAA Privacy Rule.

Policy:	**Access to Records and Protected Health Information & Patient Access to Electronic Copies**	
Purpose:	**To explain when a patient, and his or her representative, has a right to access the patient's medical records.**	
Related Materials:	**Appendix G:**	**Patient Directed Release of Records Directly to Patient or to a Designated Person**

The general rule is that a patient has a right to access his or her own medical records, including all records (both medical chart records and billing records) kept in the designated record set for that patient by the Practice. This includes a right to access medical records created by other providers outside of the Practice that are kept in the patient's file. The patient also has a right to receive "confidential communications," including copies of records, in the format requested, and at any address the patient provides.

Note: This policy applies only to requests for records made by the patient or the patient's legal representative. For requests made by third parties, Practice will consult the Authorization for the Use/Disclosure of Protected Health Information Determination - When Required policy.

- In addition to the patient, any person who has been designated by the patient, in writing, as the patient's legal representative, has the same right of access as if that person were the patient. Examples of legal representatives include: a person who provides Practice with a valid power of attorney for medical decision-making for a patient unable to make his or her own decisions, or a conservator appointed by a probate court. For additional information on legal representatives, see Practice's "Personal Representatives" policy.

Additionally, if Practice does not possess the requested records, but knows which provider possesses them (such as a hospital or other physician's office), Practice must direct the patient to the other provider. Practice is not obligated to seek out other providers, but merely to point the patient in the right direction. The Practice will direct the patient to the other provider because the Practice is likely to have a much greater understanding about medical recordkeeping than the patient. For example, a patient may have surgery at the hospital and, during the post-operative period, a physician from the Practice rounds on the patient at the hospital. The patient recalls seeing the Practice's physician, and makes a record request that asks for all of the records of the patient's care at the hospital. Practice should redirect the patient to the hospital to seek the hospital records directly, while also providing the office records that are responsive to the request.

Denial of Access:

Note that there are exceptions to this general right of access that could result in denial of access to portions of the record. If access is denied, Practice will provide a written denial to the patient, and will include the name, title and phone number of a person to contact at the Practice to

discuss the denial or register a complaint. The denial notice must be sent within 30 days of the request for records.

Any denial of access only extends to the specific records where there is an exception allowing the denial. If access is denied, other records that are responsive to the request for access must still be provided.

The reasons why record access may be denied are outlined below.

- Safety Issues (where a patient's access may be denied, but the Practice must review the denial if the patient asks for a review) including:

    - If a licensed provider determines that giving the access is likely to endanger the life or safety of the patient or others.

    - If the information involved contains information about someone other than the patient and the provider believes that the access is likely to cause harm to that person because of the disclosure.

    - If the disclosure is to the patient's representative and a licensed provider believes access by the representative is likely to cause substantial harm to the patient or others.

      Example: The patient told the physician that he fears the representative may become violent toward him. While the physician is attempting to contact the proper authorities to ensure the patient's safety, the representative requests immediate access to the record. If the physician believes that it is dangerous to disclose under those circumstances, access can be denied.

    These situations are likely to occur infrequently, if at all. For these three safety situations, a patient may ask for an internal review of such denial. If such review occurs, Practice will consult OCR guidance materials before conducting the review.

- Forensic and/or Legal System Related Exceptions (where the patient does not have a right of access and the patient cannot appeal or demand a review of a decision to deny access), including:

    - If the records were prepared exclusively for a court or agency-related matter. Generally, in these circumstances, the individual involved is not a patient of Practice, but Practice may have acted as a consultant or independent medical expert at a hearing or other similar court or agency proceeding.

    - If the patient is an inmate in a correctional system, and the prison administrator has provided reasons to deny access to the records.

- Records that are protected by the federal Privacy Act, under Title 5 of the United States Code, Section 552a.

- Specific types of records, and /or providers, for which the patient does not have a right of access - and the patient cannot appeal or demand a review of a decision to deny access:

    - HIPAA defined "psychotherapy notes." (Note: Practice probably does not have these records in its files, unless it provides psychotherapy counseling. This is a special designation for certain, but not all, mental health records that usually stay in the therapist's own file.)

    - CLIA lab rules restrict a patient's direct access to lab results. This does not affect Practice's process of sharing lab results with a patient; it only restricts the lab's ability to send results directly to the patient without a physician's instruction.

    - Records prepared in the course of a clinical research project.

    - If the information was provided by a non-health care provider with the promise that it would not be re-disclosed to the patient. This is a rare event – but can occur if a spouse or friend shares information about the patient on the express promise that the patient cannot know the source of the information. The Practice's physicians and practitioners will use their professional judgment, and follow ethical obligations to their patients, before making any promise that might trigger the possibility of restricted patient access.

<u>Patient Access to Electronic Copy of Records</u>

To the extent that Practice has electronic digital medical records (usually in its EMR or EHR system), it is required to provide the patient with a copy in electronic format.

If a patient requests an electronic copy of his/her record, the Practice is required to provide the individual with an electronic copy in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Practice and the individual.

- Notes on processing requests for electronic records:

    - If the Practice can produce the copy in the format the patient wants, it must do so, even if Practice would prefer to use a different method.

    - A web-based portal may be used if a machine readable copy can be accessed.

    - Practice is not required to accept portable media (e.g., disc, flash drive, etc.) supplied by the patient if Practice has made a risk assessment and determined that using such media would be an unacceptable security risk.

- Practice may offer a copy on its own external media and ask the patient to pay for the cost of the media, but the patient is not required to pay for the media. (If the patient is not willing to pay for the media, Practice is not required to use this method of providing an electronic copy, but will need to find another method). Practice could also absorb the cost of the media.

- If the method of providing the electronic copy is through e-mail, the e-mail should be encrypted – but, if unencrypted, then Practice may send the electronic copy by e-mail only if the following criteria are met:

    - Practice advises the patient that there is risk in transmitting unencrypted e-mail, and that a third party might intercept or see the records, including PHI;

    - the patient, after being warned, still prefers that the electronic copy be sent by e-mail; and

    - Practice documents the warning and patient agreement (for example, in the Documentation Log).

- Practice may discuss the scope, format, and other aspects of the patient's record request as necessary to facilitate the timely provision of access. Note: Timely is within 30 days of the request.

Direct Request from Patient for Access by a Third Party. (This type of disclosure is different than when a third party requests a copy, which normally requires a valid Authorization form.)

- Practice is required to provide a copy (paper or electronic) to a designated person (other than the patient) when the patient makes a direct request. When doing so, the request by the patient must:

    - be in writing;

    - be signed by the patient (or authorized person such as parent);

    - clearly identify the designated person; and

    - clearly identify where to send the copy.

    These elements are included in the Patient Directed Release of Records Directly to the Patient or Designated Person form, found at **Appendix G**.

- Note about the "Patient Directed Release of Records Directly to the Patient or Designated Person" form:

The Practice could use its authorization form as a template for documenting the release to the patient, or the patient's legal representative, and remain compliant, but an authorization is not required for a patient's own access, and the Practice's authorization form may be too elaborate in some circumstances. For example, a patient is not required to give a purpose for requesting his or her own access, even though that information is required for an authorization to release protected health information or medical records to others.

Because it is the policy of Practice to obtain written documentation (in some format) of all requested releases, including to the patient, Practice may document the request using the "Patient Directed Release of Records Directly to the Patient or Designated Person" form found at **Appendix G**.

Implementation Notes:

- Practice has 30 days to provide the records to the patient or representative from receipt of the request.

- Practice must allow for live inspection of the record if the patient or representative requests it.

- Practice should document that the patient, and/or the patient's legal representative, accessed the file with the "Patient Directed Release of Records Directly to the Patient or Designated Person" form.

- The maximum charge for copies of the record is $.65 per page of records provided. Failure or unwillingness to pay the fee cannot be the basis for denying access. The maximum charge must also take into consideration the discussion on copy fees as oulined in the following boxed text:

Maximum Charges for Copy Fees

This applies to requests made directly by the patient.

Connecticut law sets the maximum for copy fees at $.65 per page, plus first class postage (plus any fees needed to copy films or tissue blocks). There is no distinction in Connecticut law between paper and electronic copies.

HIPAA sets the maximum allowable copy fee at "cost-based" charges, which is limited to the following:

- Labor** for copying the protected health information requested by the individual, whether in paper or electronic form;
- Supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media;
- Postage, when the individual has requested the copy be mailed; and
- Preparing an explanation or summary of the protected health information, if agreed to by the individual. This applies when a patient requests a summary instead of the record, and Practice agrees to provide it.

Both rules must be taken into consideration when record copy charges are calculated. As such, the amount will never exceed the Connecticut $.65 per page (plus postage, films and block copies), and could be lower if the costs allowed by HIPAA are less.

** HHS has clarified that "labor" for the allowable cost-based fee can include: skilled technical staff time spent to create and copy the electronic file, such as compiling, extracting, scanning and burning protected health information to media, and distributing the media. But fees related to retrieving records from storage are not permitted under either Connecticut law or the HIPAA Rules.

Policy:	**Communications with Family, Friends, or Others Involved in Patient's Care or with Payment**	
Purpose:	**To explain when family, friends, or others can be exposed to patient information in the course of care or with regard to payment issues.**	
Related Materials:	**Appendix N:**	**OCR Publication: "When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved in Your Care"**

As long as a patient does not object, Practice is permitted to share or discuss patient health information with a patient's family, friends, or others directly involved in the patient's care, or involved in payment for care. This only extends to information that the family, friend, or other person involved needs to know relating to care and treatment, or payment for services rendered. This is not a substitute for requiring an authorization, but is meant to cover real-life situations such as:

- Needing to explain to an adult child of the patient the medication schedule, post-procedure, when the patient is still coming out of anesthesia.
- Discussing patient care options or test results with the patient in front of a close friend of the patient when the patient obviously wants that person in the room.
- Answering questions from a spouse in a follow up exam with the patient present (and not objecting).
- Discussing with a patient's spouse what insurance pre-authorization is needed where the patient has indicated the spouse handles his or her insurance issues.

The ability to continue communications with persons who are "friends and family" does not apply, and communication should be stopped, if the patient (or parent) objects or expressly indicates, at any point, that the communication with the person should not occur.

Practice may wish to keep a list of persons that the patient has designated as appropriate persons with whom Practice may share information and PHI about the patient.

After a Patient Has Died

While, generally, deceased patients' records are not accessible to anyone but the legally appointed or responsible person(s) (which could include the parent of a minor), the Practice is also permitted (but not required) to extend this "friends and family" policy *after* a patient has died to continue communications with persons involved in the care of the patient (while the patient was alive) about matters that were already under discussion relating to treatment/care or payment.

- A Note About Interpreters. A patient's interpreter (e.g., sign language interpreter for deaf and hearing impaired, or a language interpreter for patients with limited English proficiency) does not need authorization to be involved in patient communications. If a patient objects to the interpreter hearing the information, Practice should discuss other

available communication options with the patient. If the interpreter is a service and has a contract with the Practice, and/or provides interpretation services to the Practice, a business associate agreement or addendum should be executed.

Where appropriate, Practice may provide a copy of the HHS-OCR publication entitled "When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved in Your Care" (included as **Appendix N** to this policy manual) to persons with questions about such communications.

Policy:	**Accounting of Disclosures of Protected Health Information Determination and Requirements**
Purpose:	**To identify the disclosures of protected health information that must be included within an accounting, and to describe the information that must be included within the accounting.**

HIPAA requires a covered entity to account for any disclosure of protected health information (PHI) made by the covered entity itself, or by one of its business associates. To achieve compliance with this rule, Practice will follow the following policy and steps:

(1) Has the covered entity or any of its business associates disclosed PHI?

(2) If so, do any of the following exceptions apply, thereby eliminating the accounting requirement? Such exceptions may include [164.528]:

- ❑ disclosure made to carry out treatment, payment or health care operations;
- ❑ disclosure made directly to the individual patient;
- ❑ disclosure made for a facility's directory or to person's involved in the patient's care;
- ❑ disclosure made to correctional institutions or law enforcement about an inmate in custody;
- ❑ disclosure made for national security or intelligence purposes;
- ❑ disclosure to or by a business associate that is for an exempt purpose (e.g., disclosure for treatment, payment or health care operations);
- ❑ disclosure pursuant to an authorization;
- ❑ disclosure pursuant to an authorization for psychotherapy notes;
- ❑ disclosure of a limited data set;[1]
- ❑ incidental disclosure;
- ❑ subsequent disclosure by an entity that receives information from a covered entity or its business associate.

---

[1] A disclosure for research, public health, or health care operations, in which a limited data set is used/disclosed and a data use agreement is obtained from the recipient of the limited data set, is not subject to the HIPAA accounting rule. A limited data set includes no direct identifiers but can contain admission, discharge, and service dates, date of death, age, and 5 digit zip code.

(3) If an exception does not apply, the covered entity must account for the disclosure of PHI. Examples include:

- disclosure made for research purposes pursuant to board approval of a waiver of authorization;[2]
- disclosure made to a public health authority;
- disclosure required by law;
- disclosure to a government entity;
- disclosure to law enforcement;
- disclosure to insurers for claims investigations;
- disclosure made to child or adult protective services when referral is made for abuse or neglect.

(4) The accounting must include [164.528(b)]:

- Disclosures that occurred during the six (6) years prior to the date of the request for an accounting;
- The date of the each disclosure;
- The name of the entity of person receiving the PHI and their address, if known;
- A brief description of the PHI disclosed;
- A brief statement of the purpose of the disclosure, or in lieu of such statement, a copy of the written request for disclosure under 164.502(a)(2)(ii) (required disclosure to Secretary of HHS to investigate or determine covered entity's compliance) or 164.512 (uses and disclosures for which an authorization or opportunity to agree or object is not required).

(5) If the covered entity makes multiple disclosures of PHI to the same person or entity for a single purpose under 164.502(a)(2)(ii) or 164.12, the accounting may include:

- The information required in Section 4 (above) for the first disclosure;

---

[2] If the research disclosure involves 50 or more records, the Covered Entity must only provide a simplified accounting. Rather than an individual accounting, the Covered Entity must disclose a list of all relevant protocols under which the individual's information may have been released, and the researcher's name and contact information.

- The frequency with which the disclosure is made;
- The date of the last disclosure.

Policy:	**Amending Protected Health Information Contained within a Designated Record Set**
Purpose:	**To identify the process involved in accepting and denying an individual's request for an amendment to protected health information.**

HIPAA requires that a health care provider permit a patient to request an amendment to his/her medical record. Practice will respond to every request for amendment consistent with this policy. Note that:

- Practice may require that the patient request be in writing.
- Regardless of whether Practice agrees to the amendment, Practice must provide the patient with written notice of its decision within 60 days of the request.
- Practice is eligible for a 30-day extension if, within the initial 60-day period, it sends a written statement to the patient explaining the reasons for the delay and the date on which its decision will be provided.
- All amendment correspondence and processes should be documented by the Privacy Officer, and the documentation should be retained for a minimum of six (6) years.

To achieve compliance with the amendment rule, Practice will follow the following policy and steps.

Initial Step - Determine if the Rule Applies

- Practice is not required to amend the record:

- If the request is for a portion of the medical record that was not created by a workforce member of the Practice, and the actual originator of that portion is available to address the patient's request. But, if the patient provides a reasonable basis for believing that the originator of the PHI no longer exists, or cannot be located, the requirement to amend still applies to Practice for records it maintains [164.526];

- If the request is directed to records that are not part of Practice's medical record, billing record, or the record set that Practice maintains and uses to make decisions regarding the patient [164.526];

- If the portion that the patient wishes to amend consists of information to which the patient does not have a right of access [164.526];

- If the portion that the patient wishes to amend is accurate and complete [164.526].

The Denial Process

- If Practice denies the request for the amendment, Practice must [164.526]:

- Notify the patient in writing of the basis for the denial;

- Notify the patient of his/her right to submit a statement of disagreement into the medical record and the procedure involved in filing such a statement. If the patient submits a statement of disagreement, Practice has the right to insert a rebuttal statement into the medical record. Practice must provide the patient with a copy of the rebuttal statement;

- Notify the patient that if he/she does not wish to submit a statement of disagreement, he/she may request that a copy of the request and a copy of the denial be included with any future disclosures;

- Notify the patient of his/her right to pursue a complaint process with Practice, and of his/her right to contact the Secretary of Health and Human Services to complain.

<u>If Practice Agrees to Amend</u>

- If Practice agrees to the amendment, Practice must [164.526]:

- Notify the patient (preferably in writing) that the amendment has been accepted;

- Mark the portions to be amended with instructions on where the amendment can be found (the original record should not be destroyed or obliterated);

- Make reasonable efforts to inform business associates (and other individuals known to the health care practitioner or identified by the patient), who have the protected health information, of the amendment.

Policy:	**Marketing**
Purpose:	**To clarify the rules for promoting or marketing products to patients, including when a third party pays for the marketing activity; to explain when patient authorization is required.**

Marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. If Practice receives financial remuneration(**) from a third party for the marketing activity, then the authorization must notify the patient of that relationship.

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

EXCEPTIONS

Marketing, by definition, DOES NOT include – and an authorization is not needed for – communications made as follows:

- The below-listed treatment and health care operations purposes, if Practice does not receive financial remuneration in exchange for making the communication:
  - For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;
  - To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or
  - For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent that these activities do not fall within the definition of treatment.
- Other exceptions (no authorization required):
  - A face-to-face communication made by a covered entity to an individual; or
  - A promotional gift of nominal value provided by the covered entity.
- Separate exception for refill reminder funded by third party (no authorization needed):
  - To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, but any financial remuneration(**) is

received by Practice in exchange for making these communications, must be reasonably related to Practice's cost of making the communication).

Policy:	**Fundraising Disclosure Determination**
Purpose:	**To identify the circumstances under which a covered entity may make a fundraising communication without the authorization of the individual.**

If Practice does not do any fundraising and/or does not use its own patient information for fundraising, this policy does not apply and it is not necessary to include it in the Practice's policies.

This rule generally applies only to not-for-profit facilities or organizations that engage in fundraising for themselves (i.e., on their own behalf).

HIPAA allows a covered entity to use or disclose certain protected health information, including to a business associate or an institutionally related foundation, without an authorization, for fundraising purposes [164.514(f)]. This applies, for example, when a hospital or other non-profit provider engages in a fundraising event or annual appeal for charitable contributions.

In those circumstances, the provider is limited to use or disclosure from its own patient records as follows [164.514(f)]:

- demographic information pertaining to the individual, including name, address, other contact information, age, gender, and date of birth; dates of health care provided to an individual; department of service information; treating physician; outcome information; and health insurance status.

If a provider uses its patient records for fundraising, it must [164.520(b)(1)(iii); 164.514(f)(2)]:

- have a separate statement within its Notice of Privacy Practices documenting the provider's intentions to contact individuals to raise funds;

- have a statement within its fundraising materials alerting individuals as to how they can opt-out of receiving any further fundraising communications (this method must be simple and cause undue burden to the patient); and

- the opt-out process must be clear and conspicuous, and honored by the provider as soon as received.

Providers that fundraise should consult HHS guidance for more information on allowable fundraising requests and how to process opt-out communications.

Policy:	**Research Disclosure Determination and Discussion of De-Identification**
Purpose:	**To identify the processes involved in disclosing protected health information for research purposes; to explain the de-identification process.**

All research activities must meet numerous Federal and State laws, regulations, and rules for human subject research. In addition to those primary research obligations, HIPAA adds certain requirements described below.

Practice will follow all research rules if and when it engages in any such research.

Under HIPAA, a covered entity may use/disclose protected health information (PHI) for research purposes with an individual authorization, or a through a very specific waiver process. A limited data set, or de-identified information, may also be used for certain research.

A waiver is permitted where [164.512(i)]:

- an Institutional Review Board or Privacy Board determines that a waiver of individual authorization is appropriate and satisfies the following criteria:

  (a) the use/disclosure of PHI involves a minimal risk to the privacy of individuals;

  (b) the waiver will not adversely affect the privacy rights and welfare of individuals;

  (c) the research could not be conducted without the waiver;

  (d) the privacy risks to individuals are reasonable in relation to the anticipated benefits to the individual or the knowledge resulting from the research;

  (e) there is an adequate plan to protect identifiers from improper use/disclosure;

  (f) there is an adequate plan to destroy all identifiers once they are no longer necessary to the research; and

  (g) there are adequate written assurances that the PHI will not be reused or disclosed to any other person/entity, except as required by law, for authorized oversight of the research, or for other research that would otherwise be permitted by the HIPAA Rules.

- the PHI is utilized for preparatory research or the development of a protocol, where the PHI will not leave the covered entity and the researcher demonstrates that access is necessary.

Disclosures made pursuant to a waiver are subject to the HIPAA accounting rule and the minimum necessary standard. If, however, the research disclosure involves 50 or more records, the entity must only provide a simplified accounting [164.528 (b)(4)]. Rather than an individual accounting, the simplified accounting requires the entity to disclose a list of all relevant protocols

under which the individual's information may have been released, and the researcher's name and contact information.

Disclosures made pursuant to an individual authorization are not subject to the accounting or the minimum necessary standard. [164.528(a)(1)(iv) and 164.502(b)(2)(iii)]

Unlike the traditional HIPAA authorization, research-related authorizations:

- do not require an expiration date – a notation indicating "end of research project" or "none" will suffice [164.508(c)(1)(v)];

- may be a condition to the provision of research-related treatment [164.508(b)(4)(i)];

- may be combined with any other legal permission for to the same or another research study (including another authorization); but where a compound authorization used and , where research related treatment has been conditioned on providing the authorization, it must clearly differentiate between the conditioned and unconditioned components, and provide the individual an opportunity to opt in to the research activities described in the unconditioned authorization [164.508(b)(3)(i)].

Research disclosures of de-identified information, or a limited data set, do not require an authorization or a waiver of authorization. Both are also exempt from the HIPAA accounting requirements [164.528(a)(1)(viii)].

A disclosure of a limited data set requires [164.514(e)]:

- a data use agreement with the recipient of the limited data set;

- a limited data set including no direct identifiers, but which can contain admission, discharge, and service dates, date of death, age, and 5 digit zip code;

Because de-identified records can be used for research, the de-identification rules are outlined below.

DE-IDENTIFICATION OF PATIENT RECORDS

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information, and is not subject to HIPAA Privacy protections.

De-identified data may be used for research, or other purposes. It is essential that all identifiers listed be removed for actual de-identification.

De-identified Information contains no individually identifiable health information, and specifically does not include any of the following information about a patient, the patient's relatives, the patient's employer, or the patient's household members:

- name
- all geographic subdivisions, including address and zip code
- all dates, except for year (including birth date, admission date, discharge date, and date of death)
- telephone number
- fax number
- e-mail address
- social security number
- medical record number
- health plan beneficiary number
- account number
- certificate/license number
- vehicle identifier and serial number, including license plate number
- device identifiers or serial numbers (e.g., pacemaker or implants IDs)
- web universal resource locator (URL)
- internet protocol address number
- biometric identifier, including finger and voice prints
- full face photographic image and any comparable image
- any other unique identifying number, characteristic, or code

A record is also considered be de-identified if:

- A person, such as a consultant or expert with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
    - applying such principles and methods, 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
    - documents the methods and results of the analysis that justify such determination.

More information about de-identification, including a technical guidance document, can be found on the following OCR website: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.

Policy:	**Business Associate Determination**
Purpose:	**To provide a mechanism for determining if an outside entity is a business associate.**
Related Materials	**Appendix C: Practice's Business Associate Addendum (template)** **Appendix C-1: Cover Letter for Business Associate Addendum (template)**

HIPAA requires covered entities to have contractual arrangements with their vendors if the vendor has access to protected health information in the course of performing services for the covered entity. Practice will assess its relationship with each vendor to determine if protected health information is accessible to a vendor in the scope of work it performs on behalf of Practice. For such identified vendors, a business associate agreement or business associate addendum shall be put in place between Practice and the vendor. **Appendix C** is a copy of the standard business associate terms that may be used, although business associate arrangement terms may vary.

Generally, a person or entity is a business associate of the Practice if they perform, ***on behalf of the Practice***, any function that involves creating, maintaining, transmitting, using or disclosing protected health information.

- Examples of business associates (if they can access Practice PHI) are: claims processors/ administrators (i.e., malpractice insurance personnel, or lawyers hired to defend Practice in a malpractice case); data analysts; data processors or administrators; third party billing companies; individuals/entities performing quality assurance or utilization review functions; individuals/entities performing benefit management or practice management functions; advice or business lawyers; accountants; consultants; actuaries; financial analysts (e.g., experts hired to value Practice); individuals or entities performing accreditation functions; record storage companies (paper storage or electronic including cloud storage); IT consultants who may access the medical information or billing system.

- The following are generally not considered business associates because they should not be using any PHI to do work for the Practice: cleaning companies, the post office or "FedEx" type couriers, internet service providers (who do not provide other services that would require their access to include PHI).

- Workforce (e.g., employees or Practice owners) are not business associates.

- You do not need a business associate relationship with other providers or covered entities if they are not performing a service for the Practice. For example: a physician in one medical group speaking to a physician in another medical group about medication choices for a patient; a hospital and a medical group communicating to schedule a test or surgery; or an insurance company conducting an audit for its billing reconciliation (not on the Practice's behalf).

More Guidance is available at:
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

- Note: HHS regularly provides online guidance materials that are frequently updated. To remain current, Practice should consult the HHS online materials from time-to-time.

❑

Policy:	**Minors**
Purpose:	**To describe the access rights of a minor and identify the circumstances under which he/she has a right to access his/her medical records.**

The parent or legal guardian of a minor (someone 17 years old or younger) generally has the right to access the minor's records by requesting access in writing and submitting the request to the provider. A minor does not have the right to access his/her medical records without parental authorization except in limited circumstances (listed below).

However, there are exceptions when a minor, and only the minor, may access his/her own records, without obtaining parental or legal guardian consent, in the following circumstances, and where such privacy has been promised to the minor by the Practice or treating provider:

- Examination or treatment for sexually transmitted and venereal diseases (for patients 13 years old and up);
- HIV/AIDS testing, counseling, and treatment if the minor objects to parental involvement;
- Abortion counseling and performance;
- If the minor has been emancipated;
- With respect to a child of the minor;
- Drug and alcohol abuse treatment; and
- Outpatient mental health if the "sixth session" rule is met(**).

- To the extent that Practice, through its medical providers, has extended treatment and privacy rights to an adolescent, instead of requiring parental consent, the minor controls access rights. For example, for family planning/birth control for a mature adolescent.

For some records, Practice may need both the minor patient and the parent to sign authorizations or other consents for disclosure or access.

Important note about DCF and child abuse reporting:

HIPAA does not require any authorization or consent to make a mandatory report to DCF in connection with child abuse reporting. Practice should cooperate with all DCF requests for information in connection with child abuse investigations or reporting.

(**)The Sixth-Session Rule

In an outpatient mental health setting, where no drugs are being used as a treatment modality, a psychiatrist, psychologist, licensed social worker or licensed family and marital therapist, may

provide treatment to a minor without parental consent for six sessions. Upon the sixth session, the practitioner must tell the minor patient that, in order to continue treatment, the minor's parents must be notified – unless the practitioner believes such parental notification would be detrimental to the minor's well-being. At the end of every sixth session, the practitioner must make this assessment. If the minor refuses to agree to parental notification, the practitioner may end treatment, but may not inform the minor's parents of the care or any information about the minor. This is commonly referred to as the "sixth-session rule."

The "sixth-session rule" described above applies if all of the following are met:

(1) informing the minor's parent would cause the minor to reject treatment;

(2) treatment is clinically indicated;

(3) failure to provide treatment would be seriously detrimental to the minor's well-being;

(4) the minor knowingly and voluntarily sought treatment; and

(5) the practitioner believes that the minor is mature enough to participate in treatment productively.

The practitioner must document in the minor's record any determinations about parental notification, and obtain a written statement by the minor that:

- he/she is voluntarily seeking treatment, and that he/she has discussed the possibility of involving his/her parents;
- that he/she has determined not to involve his/her parents; and
- that he/she has been given adequate opportunity to ask the practitioner questions about his/her treatment.

The parent of a minor who has not been notified of treatment of the minor under this section is not responsible for payment for services.

Note: It is important to consult both State and Federal laws and rules, as well as considering ethical guidance, to determine whether a minor or a parent controls privacy and access rights. For example, there are laws other than HIPAA, such as substance abuse treatment privacy protections, that must be observed.

Policy:	**Requests for Restrictions on Disclosures to Health Plans**
Purpose:	**To implement patient-requested restrictions that meet the requirements of 45 CFR 164.522(a)(1)(vi) (restrictions on disclosures to a health plan concerning treatment for which an individual has paid out of pocket in full).**
Related Materials	**Appendix F: Requests for a Restriction on Disclosures to a Health Plan**

In accordance with HIPAA regulations and HHS commentary and guidance, Practice shall restrict disclosure of protected health information (PHI) about an individual to a health plan if:

- the disclosure is for the purpose of carrying out payment or health care operations; and
- the protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid the covered entity in full.

Scope of the Restriction

- The restriction applies:
  - only to disclosures to a health plan (or to a health plan's business associate); and
  - to the protected health information that pertains solely to the item or service about which the patient has requested a restriction; and
  - only if the patient (or someone, on behalf of the patient, who is not the health plan or acting on behalf of the health plan) has paid in full for the item or service.
- For "bundled services" that cannot be separated, Practice will counsel the patient that he/she may pay in full for all services in the bundled service, but Practice is not required to honor a restriction for bundled services that cannot be unbundled.
- Restrictions should not be granted for disclosures that are required by law.
  - Note: HHS guidance indicates that Medicare rules allow the restriction, but Connecticut's Medicaid program appears not to follow this rule at this time.
- Disclosures that are part of a claim, or debt collection activity, against the patient are not affected.
- A patient may utilize a flexible spending account (FSA) or health savings account (HSA) to make payment in full when exercising the right to restrict disclosures to a health plan, but a patient is not permitted to restrict disclosures to the FSA or HSA if such disclosures are required for payment.

- The restriction applies to submission of claims for payment for the items and services delivered (on the date of the request), and also to disclosures for business operations, which include but are not limited to future audit requests by a health plan.

- Practice shall "flag" restricted PHI in a manner that will ensure that the PHI is not disclosed to a health plan.

    - Note: It is not appropriate to segregate the PHI in a separate file just because of a restriction.

- In circumstances where the patient asks for a restriction on disclosures concerning a health plan that is an HMO, and Practice is an in-network provider for the HMO, the patient's request will require additional review to determine whether accepting payment from a patient above the patient's cost-sharing amount is prohibited and the disclosure is required by State law. If this is the case, the patient may be counseled that he or she will have to use an out-of-network provider for the health care item or service in order to restrict the disclosure.

Timing and Type of Patient's Payment

- Timing: Practice is not required to honor a restriction that was not timely requested, and Practice may decline to honor requests made after billing has been submitted to a health plan.

- Type of Payment: Practice Policy (unless Practice has elected the alternative option in the below text box):

    - Payment must be made in full by cash or credit card at the time of the request.

    - The person paying need not be the patient.

    - Checks will not be accepted (because the full payment cannot be verified at the time of service).

Alternative Option for Type of Payment
(If the Practice wishes to accept checks, this policy should be used)

- *Payment must be made in full at the time of the request.*
- *The person paying need not be the patient.*
- *If a check is provided for payment, but the check does not clear (e.g., payment is dishonored by the bank or other payor), then Practice will make reasonable efforts to communicate with the patient to obtain an alternative for payment.*
- *A claim for the item or service shall not be submitted to a health plan unless and until Practice is unable to obtain another source of payment after reasonable efforts. (In such circumstances, the matter does not need to be processed through collections before submitting the claim to a health plan.)*

Precertification

Where precertification is required for a health plan to pay for an item or service, Practice may require that the patient settle payments for the treatment or care prior to providing the item or service, and prior to implementing a restriction.

Follow-up or Other Visits

The restriction applies only to the items and services identified by the patient, and paid in full. If the patient seeks follow-up or related care that would typically trigger submission of a new claim to a health plan, it is the patient's responsibility to inform Practice that the patient also wishes to restrict the PHI pertaining to the follow-up care or related treatment.

Similarly, Practice is not required to continue to honor a prior restriction if the restricted PHI is necessary to support a subsequent claim as medically necessary or appropriate, and the patient chooses (after discussion with Practice) not to exercise his/her right to restrict the follow-up item or service.

Patient Education and Staff Training

- The patient shall be informed (either through discussion or written communication, as appropriate) that Practice is not required to notify any other providers about the restriction, ***and that the patient is responsible for requesting the restriction***:
    - at other health care settings (e.g., pharmacy, other hospitals, private physician office, community health center); and
    - at subsequent visits to Practice.
- Practice shall have appropriately trained staff available to: communicate with the patient about his/her right to restrict disclosures to a health plan with an out-of-pocket payment, and about the general application of such a restriction; and to implement the rule on a day-to-day basis.

Policy:	**Documentation Obligations and Log**
Purpose:	**To implement the process for keeping required documentation for HIPAA compliance.**

Practice will maintain the following documentation for a minimum of six (6) years from either (a) creation or (b) when it was last in effect, whichever is longer:

- any materials listed or required to be created, obtained or kept in any policy or procedure of Practice relating to HIPAA or as required by the HIPAA Rules; and
- documentation of all actions, activities and assessments relating to Practice's HIPAA implementation and continued compliance.

Practice may keep these materials in multiple places, and in hard copy or electronic format, but generally these materials should not be kept in a patient's chart, and should be easily identified and locatable.

Practice may choose to keep materials in a "log" or designated file area.

If the materials include PHI (such as a patient notification letter), the materials need to be protected in similar fashion to how medical records would be protected (i.e., secured and with access only by authorized persons).

At a minimum, the following must be documented and maintained:

- All policies and procedures (includes older versions if effective in last six years).
- Names of Privacy Official, Privacy Contact, and Security Officials of the Practice.
- Notice of Privacy Practices.
- All forms, including acknowledgments and authorizations.
- All patient communications regarding accounting and amendments, including the names of persons responsible for processing same for each case.
- All patient communications regarding access, including any denied access, and including the names of persons responsible for processing and reviewing any denial of access.
- Proof of all HIPAA training of workforce.
- All complaints and responses to such complaints.
- All breach investigations, responses, and notifications.

- Workforce sanctions (for employee non-compliance with HIPAA Rules, policies or procedures).
- Receipt of satisfactory assurances in judicial or administrative proceedings.
- Research authorizations and waivers.
- Business associate relationships (e.g., business associate agreements or addenda).
- Restriction requests and responses (including requests for restrictions on disclosure to a health plan).
- Government officials' requests or communications relating to HIPAA materials or PHI.

Policy:	**Prohibition on Sale of Protected Health Information**
Purpose:	**To outline the rule that prohibits sale of protected health information.**

Subject to the exceptions and definitions discussed below, Practice is not permitted to sell protected health information.

Generally, this means that Practice may not receive anything of value (including in-kind goods or services, cash, rebates) in exchange for disclosing PHI.

The method of exchange or sale is not relevant. For the purposes of this rule, "sale" is to be interpreted broadly and would include not only traditional sales contracts and purchase orders, but also, for example, access, license, and lease agreements.

Exceptions to the Prohibition on the sale of PHI

- The following are exceptions to the prohibition rule:
  - For public health purposes pursuant to § 164.512(b) or § 164.514(e).
  - For research purposes pursuant to § 164.512(i) or § 164.514(e), where the only remuneration received by the covered entity or business associate is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes.
  - For treatment and payment purposes pursuant to § 164.506(a).
  - For the sale, transfer, merger, or consolidation of all or part of the covered entity and for related due diligence as described in paragraph (6)(iv) of the definition of health care operations and pursuant to § 164.506(a).
  - To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and 164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities.
  - To an individual, when requested under § 164.524 (access) or § 164.528 (accounting).
  - Required by law as permitted under § 164.512(a).
  - For any other purpose permitted by and in accordance with the applicable requirements of this subpart, where the only remuneration received by the covered entity or business associate is a reasonable, cost-based fee to cover the cost to prepare

and transmit the protected health information for such purpose or a fee otherwise expressly permitted by other law.

In addition, HHS guidance indicates the following are not considered the sale of PHI, and therefore not prohibited under this rule:

- participation in, including sending information to, a health information exchange (HIE) that is paid for through fees assessed on HIE participants is not a sale of protected health information; rather the remuneration is for the services provided by the HIE and not for the data itself. (Such disclosures may also be exempt from these provisions);

- payments received in the form of grants, or contracts or other arrangements to perform programs or activities, such as a research study, because any provision of protected health information to the payer is a byproduct of the service being provided.

The guidance references the following examples.

- The payment by a research sponsor to a covered entity to conduct a research study is not considered a sale of protected health information even if research results that may include protected health information are disclosed to the sponsor in the course of the study.

- The receipt of a grant or funding from a government agency to conduct a program is not a sale of protected health information, even if, as a condition of receiving the funding, the covered entity is required to report protected health information to the agency for program oversight or other purposes.

Policy:	**Personal Representatives**
Purpose:	**To explain how personal representatives are to be treated with respect to use and disclosure of protected health information.**

Under the HIPAA Rules, a personal representative of a patient is to be treated in the same manner as the patient concerning protected health information. Practice will interact with personal representatives consistent with all policies of the Practice concerning protected health information, including the following policies: "Authorization for the Use/Disclosure of Protected Health Information Determination – When Required" and "Access to Records and Protected Health Information & Patient Access to Electronic Copies."

Practice is permitted to share protected health information with friends, family and other authorized representatives of the patient in at least two circumstances:

(1) When the patient does not object, and such protected health information is shared under the circumstances described in Practice's policy "Communications with Family, Friends, or Others Involved in Patient's Care or with Payment"; and

(2) When Practice has been provided with appropriate documentation that the representative has the legal authority to act on behalf of the patient. Such representatives and documentation may include:

- The parent or legal guardian of a minor child;
- Any person who has been designated by the patient, in writing, as the patient's legal representative such as an attorney in fact, or a health care representative;
- A conservator appointed by the probate court;
- A person providing a valid power of attorney;
- A person who is an executor or administrator of the patient's estate if the patient is deceased.

- Note: Where the personal representative is not authorized to make health care decisions generally, the personal representative may have access only to protected health information that may be relevant to making decisions within the personal representative's authority.

<u>Exception</u>

HIPAA rules do not require Practice to treat a personal representative as the patient if, in the exercise of professional judgment, Practice believes doing so would not be in the best interest of the patient because of a reasonable belief that the patient has been or may be subject to domestic

violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the patient.

Policy:	**Optional – Psychotherapy Notes and Psychotherapy Note Authorizations**
Purpose:	**To explain the scope of psychotherapy notes; provide the circumstances when a separate authorization for psychotherapy notes is required for the use and/or disclosure of protected health information.**

Psychotherapy notes, as defined by HIPAA, do not include all mental health records, but instead are a very limited subset of records that a mental health care provider *might* have that are not intended to be part of the regular patient record, and about which the patient has fewer access rights (see discussion of denial of access in the "Access to Records and Protected Health Information & Patient Access to Electronic Copies" policy). If Practice is not providing primary mental health counseling therapy to a patient, it is highly unlikely that Practice has psychotherapy notes for that patient.

Psychotherapy notes means:

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

If Practice has psychotherapy notes, Practice must keep them physically separate from the rest of the patient's record and only release them if the patient provides a separate authorization for release of psychotherapy notes.

A separate authorization for release of psychotherapy notes should be substantially similar to the form below:

AUTHORIZATION FOR RELEASE OF PSYCHOTHERAPY NOTES

Provider Name:	
Patient/Client Name:	

I, _____, hereby authorize the above-named provider to release a copy of all psychotherapy notes to:

[state to whom the information is being released]

The information to be used/disclosed consists of:

Note: This description must be specific and meaningful.

The information will be used/disclosed for the following purposes:

This authorization is valid unless and until it is revoked, in writing, and properly presented to the records office of the provider listed above.

I understand that if the person or the entity that receives the information is not a health care provider or health plan covered by the federal privacy regulations, the information described above may be redisclosed and no longer protected by those regulations.

I understand that I may refuse to sign this authorization and that my refusal to sign will not affect my ability to obtain treatment or payment or my eligibility for benefits. I may inspect or copy any information used/disclosed under this authorization.

I understand that I may revoke this authorization in writing at any time by submitting a written notice of my revocation, except to the extent that action has been taken in reliance on this authorization.

The authorization expires _____ [insert applicable date or event].

_____ _____

Signature of Patient/Client, or his/her authorized representative, parent or guardian if a minor, please specify relationship to patient/client.

Date

If a representative signs, describe the representative's authority to act on behalf of the patient:

TO THE RECIPIENT OF THESE MATERIALS:

If the released material contains confidential psychiatric communications, as designated in Sections 52-146d through 52-146i of the Connecticut General Statutes, please note the following:

> "The confidentiality of this record is required under Chapter 899 of the Connecticut general statutes. This material shall not be transmitted to anyone without written consent or other authorization as provided in the aforementioned statutes." A copy of the consent form setting forth any limitations shall accompany the disclosure.

This authorization is valid unless and until it is revoked, in writing, and properly presented to the records office of the provider listed above.