PATIENT PRIVACY

The Privacy Rule was created in order to build a uniform standard for health care providers in establishing regulations for releasing a patient's **"personal health information"** or **PHI**. The Privacy Rule centers on when healthcare providers can release PHI without patient consent, and when patient authorization is required. It also details how much patient information should be disclosed and under what circumstances.

Before we go into the actual Privacy laws it is important that you understand a central term in the Privacy Regulations. This term is "**TPO**", which stands for **treatment, payment, or healthcare operations**. Whether or not a disclosure of a patient's PHI is for purposes of treatment, payment, or healthcare operations will determine if patient authorization is needed. If a disclosure of patient PHI is made to a third-party for purposes of treatment, payment, or healthcare operations, no patient authorization is required. Examples of this type of disclosure would be those made to your billing service or those made to a specialist who is treating your patient. If the disclosure is for some other "non-routine" purpose, then patient authorization is required. An example of this type of disclosure might be for marketing or research purposes.

Our practice has developed our "Patient Privacy Policy" which details under what circumstances we will routinely release patient information without a patient's prior consent (i.e. T.P.O.), and under what circumstances we will be required to obtain a patient's authorization. Please review the copy of our practice's Privacy Policy located in the "Forms & Documents" section of this manual and become familiar with it. *A copy of our Patient Privacy Policy must be provided to each of our patients during their next visit, and should also be posted in our lobby.*

ACKNOWLEDGEMENT OF RECEIPT OF OUR NOTICE OF PRIVACY PRACTICES

We are required to make a ***good faith effort*** to obtain an individual's written acknowledgement of receipt of our notice of privacy practices. The purpose of this acknowledgement process is to alert patients to the importance of our privacy notice and provide them the opportunity to discuss privacy issues with us.

This acknowledgement should be obtained at the time of the first service delivery, which would generally be when the patient arrives in your office for an appointment.

While the rule requires the acknowledgement to be in writing, it does not prescribe the other details such as the form that the acknowledgement must take or the process for obtaining the acknowledgement. For example, all of the following methods specifically satisfy the definition of written acknowledgement:

- A signature on either a separate page or on a signature list,
- A patient placing his or her initials on a cover sheet of the notice to be retained by the provider,
- An electronic acknowledgement where the patient transmits the receipt of acknowledgement, which may not necessarily his or her signature (this is an important point and as such a quotation from the final rule is included: "Generally, the privacy rule allows for electronic documents to qualify as written documents for purposes of meeting the rules requirements. This also applies with respect to the notice acknowledgement. For notice delivered electronically, the department intends a return receipt or other transmission from the individual to suffice as the notice acknowledgement. For notice delivered on paper in a face-to-face encounter with the provider, although it is unclear to the Department how exactly the provider may do so, the rule does not preclude providers from obtaining the individual's written acknowledgments electronically. The Department cautions, however, that the notice acknowledgement process is intended to alert individuals to the importance of the notice and provide them the opportunity to discuss privacy issues with their providers. To ensure that individuals are aware of the importance of the notice, the rule requires that the individual's acknowledgement the in writing. Thus the department

would not consider a receptionists notation in a computer system to be an individual's written acknowledgment.")

If an individual refuses to sign or otherwise fails to provide an acknowledgment, we are required to document our good-faith efforts to obtain the acknowledgement and the reason why the acknowledgement was not obtained. **Failure to obtain an individual's acknowledgement, assuming we otherwise documented our good faith effort, is not a violation of the rule.** For example, there is no rule violation if an individual refuses to sign the acknowledgement after they were requested to do so or if an individual is mailed the notice of privacy policy and chooses not to mail back his or her receipt of acknowledgement.

By law of our office must retain acknowledgement receipts for six years from the date received. The rule does not dictate the form in which the acknowledgments are to be saved. Although not required, other covered entities (including us), may if they choose, require patients to provide written consent for the use and disclosure of protected health information. However we are not required to determine the restrictions on another covered entity's consent form before disclosing information to that entity for TPO purposes.

AUTHORIZATIONS

An authorization is a more customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. Please see copy of our Patient Authorization Form to release PHI in the "Documents & Forms" section of this manual. It covers only the uses and disclosures and only the PHI stipulated in the authorization; it has an expiration date; and, in some cases, it also states the purpose for which the information may be used or disclosed.

All covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a patient mailing list, to disclose information to an employer for employment decisions, or to disclose information for eligibility for life insurance. A provider may have to obtain separate authorizations from the same patient for different uses or disclosures.

The privacy rule requires us to obtain authorization to use or disclose PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes or for payment or for health care operations purposes, except as specified in the privacy rule.

An authorization is also required if another entity requests disclosure of PHI for TPO purposes. For example, a health plan seeking payment for a particular service from a second health plan, such as in coordination of benefits or secondary payer situations, may need PHI from a physician who rendered the health-care services. In this case the provider typically has been paid, and the transaction is between the plans. Since our disclosure is for the TPO purposes of the plan, our authority to disclose PHI for TPO would not allow disclosure. Rather, the plan would have to obtain the patient's authorization when requesting such a disclosure.

ACCOUNTING FOR DISCLOSURES

When our office makes "non - routine" disclosures of PHI for purposes other then TPO, we need to document those disclosures and patients have the right to obtain an accounting of them. Our documentation of such disclosures should include the following elements:

- **D** – Date of Disclosure
- **W** - Who the recipient is
- **W** – What was disclosed
- **P** – Purpose of the disclosure

PATIENTS ACCESS TO THEIR RECORDS

Under HIPAA, patients have the right to access their own medical records. We need to respond to their request within 30 days. Please see our "Patient Request to View / Amend Record" form in the "Forms & Documents" section of this manual.

There are three options for granting patient's access to their medical record:

1. Allow patient to view original copy with a representative from the practice (patients should never be left alone with the original record).
2. Provide a summary of the record, if the patient agrees to it.
3. Provide a copy of the medical record, and a reasonable fee can be charged.

Patients also have the right to request changes or amendments to their medical record. Physicians do not have to agree to these requests to amend the record, especially if it would make the record inaccurate.

MINIMUM NECESSARY PROVISION

HHS has declared that health care workers must take reasonable steps to limit the use or disclosure of, and requests for Personal health information (PHI) to the minimum necessary to accomplish the intended purpose. However, they are also very clear that restricting PHI to the minimum necessary should never out way quality of patient care. ***A great deal of discretion is provided to the physician on the amount of information provided to a third-party when patient treatment and quality of care is involved.***

Whenever we deal with PHI always review and/or disclose the least information necessary to deliver the highest quality care. We must determine our own standards for minimum necessary use and disclosure of patient information. The privacy rule requires us to make reasonable efforts to limit use, disclosure of, and request for protected health information to the minimum necessary to accomplish the intended purpose. We have flexibility in assessing what protected health information is reasonably necessary for a particular purpose, given the characteristics of our business and work force. This is a reasonableness standard that calls for good judgment in adhering to generally acknowledged practice standards, while trying to limit any unnecessary sharing of medical information.

Exceptions to the Minimum Necessary Provision:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an authorization requested by the individual.
- Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.'
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
- Uses or disclosures that are required by other law (i.e Federal or State Law)

The privacy rule does not prohibit the use of sign-in sheets, but it is generally recommended that the reason for the patients visit not be included on the sign-in sheet.

Keep in mind that nothing in the Privacy Rule prevents you from discussing its concerns with the person making the request, and negotiating an information exchange that meets the needs of both parties. If you have real concern about a request, contact our Compliance Officer. The most difficult situations are when a non-routine disclosure is needed. As a general rule, these special situations should be discussed with our HIPAA

Compliance Officer. In these cases we want to be especially vigilant that we determine and limit disclosure to only the minimum amount of PHI necessary to accomplish the purpose of the non-routine disclosure.

We must evaluate our practice and enhance protections as needed to prevent unnecessary or inappropriate access to PHI. If you have any suggestions as to how we can better limit access to and disclosure of our patient information please bring this information to our HIPAA Compliance Officer. The minimum necessary standard is intended to reflect and be consistent with, not override, professional judgment and standards. **Please keep in mind that we want to appropriately limit access to personal health information without sacrificing the quality of health care that we offer.**

COMMON MINIMUM NECESSARY QUESTIONS

MEDICAL RESIDENTS, MEDICAL STUDENTS, NURSING STUDENTS AND OTHER MEDICAL TRAINEES

The minimum necessary requirements do not prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training. The definition of "health care operations" in the rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers."

THIRD PARTIES

The minimum necessary concept does not need to be applied to disclosures to third parties that are authorized by an individual, unless the authorization was requested by a covered entity for its own purposes. **The Privacy Rule exempts from the minimum necessary requirements most uses or disclosures that are authorized by an individual**. This includes authorizations covered entities may receive directly from third parties, such as life, disability, or casualty insurers pursuant to the patient's application for or claim under an insurance policy.

DISCLOSURES TO FEDERAL AND STATE AGENCIES

We are not required to make a minimum necessary determination to disclose to federal or state agencies, such as the Social Security Administration (SSA) or its affiliated state agencies or for individuals' applications for federal or state benefits. These disclosures must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements.

DISCLOSURE OF AN ENTIRE MEDICAL RECORD

HHS has said that the Privacy Rule does not prohibit use, disclosure, or requests of an entire medical record. As with all of our policies the balance is to keep the patients health care utmost in your mind while at the same time divulging the minimum information about the patient that is necessary for their best care. HSS has also said that a covered entity may use, disclose, or request an entire medical record without a case-by-case justification. If the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes.

STAFF ACCESS & MINIMUM NECESSARY

It is important that you are aware of those persons or classes of person in our workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. We must, whenever possible, restrict access to all or part of a patient's medical record if it is not necessary for an employee to complete their job duties. **The Rule says that the basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the covered entity.**

In this light, HHS has said that we should take into account our ability to configure our record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. **HHS have said that it may not be reasonable for a small, solo practitioner with largely paper-based records system,**

to limit access to certain employees. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the rule. This is what is meant by reasonable efforts.

MISC.

Regarding patient medical charts at bedside, empty prescription vials, X-ray light boards HHS has indicated that specific workplace practices need to remain as they have been developed over the years in order to maintain proper patient care and reasonable workflow. **The minimum necessary standards do not prohibit us from maintaining patient medical charts at bedside, nor do they require that we shred empty prescription vials, or require that X-ray light boards be isolated.**

ORAL COMMUNICATIONS

As mentioned earlier in this manual, HHS has stated that **the Privacy Rule applies to individually identifiable health information in all forms, electronic, written, oral, and any other**. Coverage of oral (spoken) information ensures that information retains protections when discussed or read aloud from a computer screen or a written document.

Basic Rules for Oral Communications about Patient Health Records

- We are required to reasonably safeguard Personal health information (PHI), including oral information, from any intentional or unintentional use or disclosure that is in violation of the Privacy rule. The rules of oral communication basically are the same as those of written communication. You should always use the minimum necessary information for best health care.
- In particular, with oral communications, we require that our employees be discrete when talking to or about patients. Be aware of who is in the area, who could listen in. Because we discuss health care issues all day, it may be easy to assume a patient is not private about this information. Always assume the patient wants the minimum number of ears to hear the minimum necessary information about their health care. Again, the minimum necessary standard does not apply to disclosures, including oral disclosures, among providers for treatment purposes.
- "Reasonably safeguard" means that you must make reasonable efforts to prevent uses and disclosures not permitted by the rule. However, HHS does not expect reasonable safeguards to guarantee the privacy of PHI from any and all potential risks. HHS has said that in determining whether a covered entity has provided reasonable safeguards, the Department will take into account all the circumstances, including the potential effects on patient care and the financial and administrative burden of any safeguards. Remember, balance privacy with patient care.
- It is important that all our employees interacting with patients speak quietly when discussing a patient's condition with family members in a waiting room or other public area, and avoid speaking about patients in public hallways and elevators. Protection of patient confidentiality is an important part of our practice.
- If the patient or others has difficulty hearing or exhibits other communication problems, take them to a private area when discussing health information. There is nothing more embarrassing to a patient than to be walking out of a crowded waiting room and have the nurse talking about their treatment or medications. It is not only embarrassing, now it is illegal.

Talking to other Providers and Patients

The Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. The rule only requires covered entities to implement reasonable (there's that word again) safeguards that reflect 'their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients.

- HHS has also said that they also understand that overheard communications are unavoidable. For example, in a busy emergency room, it may be necessary for providers to speak loudly in order to ensure appropriate treatment. The Privacy Rule is not intended to prevent this appropriate behavior.

Calling out Patient names

Calling out a patient’s name in a waiting room is allowed.

Private Rooms and Soundproof Walls

The Privacy Rule does not require hospitals and physicians' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard. As you work around the office, you should make yourself aware of the level of voice that is needed to maintain privacy in different areas of the office.

Once again reasonable safeguards are appropriate. The rule does not require that all risk be eliminated to satisfy this standard.

Patient access to oral information

HHS has said that covered entities do not need to provide patients access to oral information. **The Privacy Rule requires covered entities to provide individuals with access to PHI about themselves that is contained in their "designated record sets."** The term "record" in the term "designated record set" does not include oral information; rather, it connotes information that has been recorded in some manner.

We do not have to document ALL oral communications

If the oral communications you are giving are relevant to any disclosures signed by the patient or if they have anything to do with following The Privacy Rule, or if they can be used in patient care, we recommend that you document this in the patient's records. Once again we strive to provide the best patient care without wasting time documenting events or actions that will not help the patient.

BUSINESS ASSOCIATES

HHS' definition of a Business Associate

- **A business associate is a person or entity who provides certain functions, activities, or services for or to a covered entity, involving the use and/or disclosure of PHI.**
- A business associate is not a member of the health care provider, health plan, or other covered . entity's workforce.
- A health care provider, health plan, or other covered entity can also be a business associate to another covered entity.
- The rule includes exceptions. The business associate requirements do not apply to covered entities who disclose PHI to providers for treatment purposes - for example, information exchanges between a hospital and physicians with admitting privileges at the hospital.

In allowing providers and plans to give Personal health information (PHI) to "business associates," the Privacy Rule conditions such disclosures on the provider or plan obtaining, typically by contract, satisfactory assurances that the business associate will:

1. Use the information only for the purposes for which they were engaged by the covered entity.
2. Safeguard the information from misuse.
3. Help the covered entity comply with the covered entity's duties to provide individuals with access to health information about them and a history of certain disclosures (e.g., if the business associate maintains the only copy of information, it must promise to cooperate with the covered entity to provide individuals access to information upon request).

HHS has stressed that PHI may be disclosed to a business associate only to help the providers and plans carry out their health care functions - not for independent use by the business associate. If you have any questions about whether a particular business associate of ours is properly contracted under the HIPAA rules, please contact the Compliance Officer. We have a "Business Associates PHI Privacy Agreement" that should be used in situations where required.

Business Associates have more narrow provisions of Rule

Our contract with business associates covers a set of contractual obligations far narrower than the provisions of the rule, to protect information generally and help us comply with our obligations under the rule. The Privacy Rule does not "pass through" its requirements to business associates or otherwise cause business associates to comply with the terms of the rule. For example, HHS has said that we do not need to ask their business associates to agree to appoint privacy officer, or develop policies and procedures for use and disclosure of PHI.

Our Liability for business associates violations of the Privacy Rule

HHS has said that a health care provider, health plan, or other covered entity is not liable for privacy violations of a business associate. We are not required to actively monitor or oversee the means by which the business associate carries out safeguards or the extent to which the business associate abides by the requirements of the contract. Because businesses by law are specifically covered by the Rule, business associate's violation of the terms of the contract does not, in and of itself, constitute a violation of the rule by our practice. Under our contract, business associates must advise us when violations have occurred. If we become aware of a pattern or practice of a business associate that constitutes a material breach or violation of that business associate's obligations under our contract, we are required by HHS to take "reasonable steps" to cure the breach or to end the violation.

PARENTS & MINORS

The Privacy Rule provides individuals with certain rights with respect to their personal health information, including the right to obtain access to and to request amendment of health information about themselves. These rights rest with that individual, or with the "personal representative" of that individual. In general, a person's right to control Personal health information (PHI) is based on that person's right (under state or other applicable law, e.g., tribal or military law) to control the health care itself.

The concepts below will give you excellent guidance regarding confidential relationships and parents or guardians. If you find yourself in a situation where you are not sure as to the PHI you should divulge to a parent, guardian or child, please check with our Compliance Officer.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a "personal representative" of his or her minor child under the Privacy Rule and has the right to obtain access to health information about his or her minor child. This would also be true in the case of a guardian or other person acting in *loco parentis* of a minor.

There are exceptions in which a parent might not be the "personal representative" with respect to certain health information about a minor child. In the following situations, the Privacy Rule defers to determinations under other law that the parent does not control the minor's health care decisions and, thus, does not control the PHI related to that care.

- When state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health care service, the parent is not the minor's personal representative under the Privacy Rule. For example, when a state law provides an adolescent the right to consent to mental health treatment without the consent of his or her parent, and the adolescent obtains such treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment. The minor may choose to involve a parent in these health care decisions without giving up his or her right to control the related health information. Of course, the minor may always have the parent continue to be his or her personal representative even in these situations.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services. For example, courts may grant authority to make health care decisions for the minor to an adult other than the parent, to the minor, or' the court may make the decision(s) itself. In order to not undermine these court decisions, the parent is not the personal representative under the Privacy Rule in these circumstances.

In the following situations, the Privacy Rule reflects current professional practice in determining that the parent is not the minor's personal representative with respect to the relevant PHI:

- When a parent agrees to a confidential relationship between the minor and the physician, the parent does not have access to the health information related to that conversation or relationship. For example, if a physician asks the parent of a 16-year old if the physician can talk with the child confidentially about a medical condition and the parent agrees, the parent would not control the PHI that was discussed during that confidential conference.

- When a physician (or other covered entity) reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the physician may choose not to treat the parent as the personal representative of the child.

State Laws

In addition to the provisions (described above) tying the right to control information to the right to control treatment, **the Privacy Rule also states that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent** (§ 160.202). This is true whether the state law authorizes or prohibits such disclosure.

Parental Consent

The Privacy Rule addresses access to health information, not the underlying treatment. The Rule does not address consent to treatment, nor does it preempt or change state or other laws that address consent to treatment.

Emergency medical care without a parent's consent

Even though a parent does not provide consent to treatment in an emergency medical situation, under the Privacy Rule, the parent would still be the child's personal representative. This would not be so only when the minor provided consent (and no other consent is required) or the treating physician suspects abuse or neglect or reasonably believes that releasing the information to the parent will endanger the child.

PATIENT BILLING & PAYMENTS

In order to understand the Privacy Rule as it pertains to patient payments, we first must give the HHS definition of payment. ***"Payment" is a defined term that encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and for a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care***. In addition to the general definition, the Privacy Rule provides examples of common payment activities which include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims;
- Risk adjustments;
- Billing and collection activities;
- Reviewing health care services for medical necessity, coverage, justification of charges, and the like; * Utilization review activities; and
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity).

HHS has said that as provided for by the Privacy Rule, our practice may use and disclose Personal health information (PHI) for payment purposes.

Consumer Credit Reporting Agencies

The Privacy Rule's definition of "payment" includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following PHI about the individual: name and address; date of birth; social security number; payment history; and account number.

Debt Collection Agencies

The Privacy Rule permits our practice to use the services of debt collection agencies. Debt collection is recognized as a payment activity within the "payment" definition. Disclosures to collection agencies under a business associate agreement are governed by other provisions of the rule, and the minimum necessary requirements.

Location information services of collection agencies and the Fair Debt Collection Practices Act

As described above, "Payment" is broadly defined as activities by health plans or health care providers to obtain premiums or obtain or provide reimbursements for the provision of health care. The activities specified are by way of example and are not intended to be an exclusive listing. Billing, claims management, collection activities, and related data processing are expressly included in the definition of "payment".

HHS has stated that obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable. Therefore, would constitute a payment activity. We would still have to comply with any limitations placed on location information services by the Fair Debt Collection Practices Act.