

## **General Rules for Uses & Disclosures of PHI**

### **Policy:**

The policy of this office is to protect the privacy of individual protected health information (PHI). Therefore, we will limit the amount of accessible information disclosed to the minimum amount needed to perform a specific type of work or to complete a function.

### **Definitions:**

- Protected Health Information (PHI) is defined as health information that is individually identifiable and created or received by a health care organization.
- PHI can be written (e.g. patient sign in sheet, insurance card) or oral (e.g. appointment reminder left on answering machine).
- PHI can be recorded on paper (e.g. financial record, fax sheets, test results), computer (e.g. data appearing on computer screen), or other media (e.g. data stored or communicated on the internet, extranet, or an intranet, or saved on discs).
- PHI is information that reveals the state of a person's health condition (e.g. information revealed to a physician's office, insurance information requests, treatment codes obtained for payment).
- PHI is information that identifies the individual patient (e.g. all demographics).
- PHI is information that gives a reasonable basis for determining a person's identity (e.g. combination of certain demographic information).

### **Procedure:**

- Prior to providing individual health care information, we need to determine the reasons why the information would be needed:
  - Patient request
  - Needed for billing information, healthcare treatment, or operation
  - Healthcare provider who has an indirect relationship with individual; (e.g. laboratory or pharmacy)
  - For care to an inmate of a correctional facility.
  - Representative of an accrediting body.
  - Information provided per each request for healthcare information shall be limited to :
    - Complete legal name, address and telephone number
    - Date of birth
    - Social security number
    - Past medical history information
    - Documentation of completed diagnostic tests, laboratory values, results of procedures and surgical procedures
  - Documentation of healthcare information requested by parties not directly involved in the provision of patient care is to be maintained and retained for a period of six (6) years.

- Follow the “minimum necessary” guidelines. Provides validated requesting parties with the minimum amount of information necessary to perform the required task.

## **Uses and Disclosures Under Restricted Agreement and During Emergency Situations**

### **Policy:**

- The policy of this office contends that patients have the right to have his/her individual healthcare information treated as confidential and private except as needed for treatment, insurance payment or for healthcare operations.
- A patient has the right to restrict access to his/her private medical information.
- A patient can request that his/her private medical information not be provided to family members.
- A patient can verbally request that access to his/her private medical information be restricted.
- This must be documented in the patient’s medical record.
- This office can terminate the agreement to restrict a patient’s private medical information if the information is needed to provide emergency care or treatment. Any information obtained to help provide emergency care cannot be used beyond the provision of emergency care.
- This office will maintain a record of agreed restrictions. This record shall be retained for six (6) years from the date it was created or the date it was last in effect, whichever is later.

### **Definitions:**

Emergency Treatment Situations are defined as one in which the patient has acute and severe symptoms (like acute pain), or is unconscious and the absence of immediate medical treatment places the health of the patient in jeopardy.

Restricted Agreements are agreements that restrict the release of information to designated parties as per patient’s request.

### **Procedure:**

- This information will be given to the patient in writing (Privacy Notice).
- Inform the patient of who will have access to his/her personal medical information; inform the patient that they have the right to restrict access to his/her personal medical information.
- After patient has been provided with a Privacy Notice and advised of their rights have the patient acknowledge in writing that they are aware of their privacy rights.
- Should the patient request his/her health information be restricted, the patient must complete and sign the Restriction Agreement.

- If a patient should subsequently to their first visit call in and request restriction to their medical information, we must have the patient come in to sign the Restriction Agreement.
- The completed Restriction Agreement is to be maintained in the patient's medical record and noted in any applicable computer systems.
- In the case of emergency treatment, this office can terminate the Restriction Agreement, after informing the patient of the termination of the agreement. Once the patient is notified, this office must maintain the confidentiality of the information in the original agreement prior to the termination of the agreement. Information accumulated after the notification to terminate the agreement would not be covered or restricted by the terms of the previous agreement. Document the form of notification to the patient in the medical record.
- Should we decide to terminate a Restriction Agreement with a patient without the patient's agreement, we will need to include a Statement of Emergency Disclosure in the patient's medical record. Any information prior to the termination will need to be maintained as confidential and private. Medical information after the date and of the notice of agreement termination would not be held as confidential and private
- In case of emergencies, we can:
  - Use and disclose PHI to treat the patient
  - Disclose PHI to family members or others involved with the patient's care, if those disclosures appear to be in the patient's best interests. The PHI disclosed for these purposes are limited to the patient's location, condition, or death.
- Disclose PHI to law enforcement personnel, only if the disclosure appears necessary to alert law enforcement of the commission and nature of a crime; location of such a crime or the victims; and identity, description and location of the perpetrator of a crime.
- We may disclose patient PHI to law enforcement under the following conditions:
  - Patient is incapacitated and can't consent to the disclosure of his/her PHI
  - Law enforcement officers assert that the PHI is needed to determine if someone other than the victim committed a crime.
  - If waiting until the victim consents to the disclosure of his/her PHI would hamper efforts to investigate the crime or catch a criminal
  - The disclosure appears to be in the best interests of the patient
  - If we believe a patient is a victim of domestic violence or abuse and neglect; we must give the law enforcement personnel the patient's PHI
- If a patient in our treatment is suspected of committing a crime, we can give law enforcement personnel the patient's demographics, physical description, blood type and Rh factor, type of injury, date and type of treatment. Other information can only be disclosed by order of the court, unless patient has suffered a gun shot or stab wound, in which case, by state law, we are required to disclose this information to law enforcement.

## **Authorizations Not Required For Uses and Disclosures**

### **Policy:**

The policy of this office is to provide protected health information to public health authorities or law enforcement agencies without the written consent or authorization of the patient.

### **Procedure:**

- Protected health information may be disclosed to public health authorities in order to:
  - Report a birth or death
  - Report child abuse, child neglect, or domestic violence
  - Report certain types of wounds (gunshot, stabbing)
  - Prevent or control a disease, injury or disability
  - Report a communicable disease
  - Report adverse effects of food or dietary supplements
  - Report defects or problems with a biologic product
  - Report defective products to enable product recall, repairs or replacements
  - Follow up with the use of products to comply with the requirements of the Food and Drug Administration
  - Investigate a work-related illness injury
  - Respond to a court order, subpoena, discovery
  - Conduct civil, criminal or administrative investigations, audits or licensure
  - Provide appropriate information to a coroner or medical examiner
  - Provide appropriate information to organ procurement agencies
  - An adult patient can refuse to have the abuse, neglect or domestic violence reported to public officials or law enforcement agencies.

- The office can supersede the patient's decision to not report the abuse, neglect or domestic violence if that person is suspected of being the responsible party of the abuse, neglect or domestic violence.
- The office may provide protected health information to law enforcement agencies for the purpose of identifying, locating a suspect of being the responsible party of the abuse, neglect or domestic violence.
- The office may provide protected health information to law enforcement agencies for the purpose of identifying, locating a suspect, fugitive, material witness or missing person. This information is allowed to be provided:
  - Name and address, date and place of birth, social security number
  - Blood type and Rh factor, type of injury
  - Date and time of treatment or date and time of death
  - Description of physical characteristics such as height, weight, gender, race, hair and eye color, beard, moustache, tattoos and scars.
  - DNA data, DNA analysis, dental records, sampling, typing or analysis of body tissues or fluids may not be disclosed

### **Patient Authorization Required for Marketing Purposes**

#### **Policy:**

The policy of this office is to not use or disclose protected health information for marketing without patient authorization

#### **Procedure:**

- Obtain patient authorization to release PHI for the purposes of marketing.
- Patient authorization is not required in the following circumstances:
  - Marketing is performed directly with the patient, face-to-face meeting,
  - Relates to health-related products or services in the form of a newsletter or similar communication and is distributed to a large cross-section of patients and provides instructions on how the patient may opt out of future communications
  - If the office targets patients based on their health status or condition the office must:
    - Document that the product or service is advantageous to the patient's health.
    - Inform the patient why she or he has been targeted.
    - Inform the patient how the product or service is associated to the health of the patient.
    - Discontinue distributing future marketing materials to patients who have informed the office that they do not want to receive marketing information.

## **Business Associates**

### **Policy:**

The policy of this office is to prevent the inappropriate disclosure of confidential PHI unless an agreement exists defining the function of the business associate and the uses of the PHI.

### **Procedure:**

A business associate is a person acting on behalf of another covered entity, who may have access to confidential patient healthcare information during the normal course of business or during the provision of services. Business associates may provide consulting, management, administrative, legal, actuarial, accounting, data aggregation, administrative, accreditation, or financial services.

Business Associate contracts must:

- Establish who will have access to PHI and the required uses of the PHI.
- Establish that PHI will not be used for any purpose other than that set forth in the contract or as required by Texas state law.

- Establish how PHI will be safeguarded from inappropriate use by the business associate (e.g. destruction of record, encryption of electronic data exchange).
- Establish that the business associate is responsible for contacting this office within two (2) day of its discovery of any use or disclosure of PHI not provided for in the contract.
- Establish how this office will be contacted if confidential PHI is disclosed.
- Establish how subcontractors of the business associate will safeguard against PHI provided to them.
- Establish how the business associate will amend confidential PHI upon request by the patient.
- Establish that information be made available to enable this office to provide an accounting of disclosures of PHI except for the purposes of treatment, payment or healthcare operations.
- Establish that the records, books and internal practices of the Business Associate be made available for inspection to determine if PHI is being used for the agreed upon terms of the contract.
- Establish how PHI will be returned or destroyed upon conclusion of the Business Associate contract.
- Establish how PHI will be returned at the termination of the contract. If all information cannot be returned upon termination of the contract, the Business Associate must explain how the information will be protected.
- Establish that Business Associate contract may be terminated if the Business Associate violates any terms of the contract.
- The Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of ePHI (electronic Protected Health Information) that it creates, receives, maintains or transmits as required by the Security Rule.

## **Right to Access**

### **Policy:**

The policy of this office is to provide patients with their healthcare information upon request. The healthcare information designated record set is defined as medical records and billing records. The patient may be denied access to healthcare information as it relates to:

- Psychotherapy notes
- Incident reports
- Inmate records

Research studies if the patient did not consent to having access to his/her healthcare information while the research is in progress. Access to the healthcare information will continue upon completion of the research.

### **Procedure:**

- When the patient requests to read or wants a copy of their PHI:

*Valley Surgical Center of Minimally Invasive Surgery  
Policy & Procedure Manual*

*Updated 8.2009*

- Ask the patient to put the request in writing
- Determine if patient has any reason for the request to be denied.
- Will the patient's life or physical safety be jeopardized if he/she or his/her legal representative has access to his/her healthcare information?
- Will another person's life or physical safety be jeopardized if the patient or legal representative has access to his/her healthcare information?
- Does the information reference another person and if so, could this information cause harm to the person?
- The patient has the right to request denial to be re-evaluated by another employee or staff member who did not participate in the original decision to deny access.
- The patient if the request has been accepted or denied.
- If the request is denied, provide the patient with a written response explaining the reason for denying the request. The name of the Privacy Officer must be included in the response.
- If the request is accepted, provide the patient with the requested healthcare information. The information is to be provided to the patient within 30 days of the request. If the requested information is not on the -office premises (off-site storage), provide the patient with the information within 60 days of the request.
- If the information cannot be provided within 60 days, an extension of 30 additional days can occur after informing the patient in writing of the delay. This statement must include the date in which the requested information will be available for the patient. Only one extension per request for healthcare information can be made.
- The office can provide the patient with a summary of the requested healthcare information if the patient agrees in advance and agrees to pay the appropriate fees established by Texas state law for this information.
- Document the information requested by the patient, what information was provided to the patient, the date the information was provided and the name of the employee who processed the request for information. This information is to be kept for six (6) years.

## **Right to Request an Amendment to Medical Records**

### **Policy:**

The policy of this office to amend a patient's medical record upon patient request.

### **Procedure:**

- The patient may request to review their healthcare information and request changes be made to information in the record.

- The request for the amendment must be put in writing by the patient and include the reasons why the patient wants the changes made to the information.
- The request must be handled within 60 days of the request for changes. If the office cannot fulfill the request within 60 days. The time period can be extended once for an additional 30 days. The office must write the patient a letter explaining the reasons for the 30-day extension and the estimated date of completion.
- The office has the right to deny the request for an amendment if:
  - The request for the amendment is for records that were not created by the office (e.g. from a different physician's office)
  - The request for the amendment is for information the patient wants changes has nothing to do with the current visit.
  - The request for the amendment is for records that are currently accurate and complete.
  - If the office denies the patient's request to make changes the office will:
    - Write a letter to the patient explaining the reason(s) for the denial.
    - Explain the steps the patient can take to argue with the decision (e.g. meet with the Privacy Officer, meet with the physician)
    - Explain that if the patient does not protest the decision, the patient may request the office provide the patient's request for changes and the denial with any future releases of the disputed healthcare information.
    - The patient has the right to file a formal complaint with the Privacy Officer. If this occurs, the office will follow the steps below in the case of a denial:
      - Allow the patient to provide a written statement with the reason for the proposed changes and why the patient disagrees with the office denial.
      - Furnish the patient with a written letter stating the reasons the office disagrees with the patient's statement.
      - Attach the patient's request for changes, the office's denial of the request, the patient's statement of disagreement and the office's written rebuttal to the document(s) in question.
      - Include a copy of the patient's request for changes and a copy of the denial to make these changes with any releases of the information if the patient has not submitted a written statement of disagreement.
      - If the office agrees with the request for changes, the following steps will be taken:
        - Amend the changes to the record.
        - Notify the patient that the changes were accepted and the changes have occurred.
        - Obtain a list of any other individuals who need to be informed of the changes.
        - Make a reasonable effort to contact those individuals who need to have the changed information. Document who has been contacted and who was unable to be contacted.
        - Contact any necessary business associates and request that they amend their record in accordance with the patient's request.
        - Document names of the employees responsible for processing the request for amendments.

- Documentation will be maintained for a period of six (6) years.

**Accounting of Disclosures of PHI**

*Valley Surgical Center of Minimally Invasive Surgery  
Policy & Procedure Manual*

*Updated 8.2009*

**Policy:**

The policy of this office is to provide a patient with a list of disclosures for PHI, which has been release within the last six (6) years. The effective date is April 14, 2003.

The office does not have to comply with this policy if the information was:

- Disclosed for the provision of patient care, payment for services or healthcare operations.
- Disclosed according to written authorization provided by the patient.
- Disclosed to the patient.
- Disclosed to employees responsible for patient's care.
- Disclosed fro the purpose of national security or intelligence.
- Discloses to correctional facilities or law enforcement officials.
- Disclosed prior to the date of compliance (April 14, 2003)

The office may exclude a patient's right for a listing of disclosers to a health oversight agency or law enforcement official if the agency or official provides the office with a written statement with the reasons why the patient is likely to impede the agency's or official's activities and the time period for the suspension.

If this request is given verbally, the office must document the statement given, the name of the person making the statement and temporarily suspend the patient's right to the list of releases The s suspension can list no longer than 30 days unless the ambulatory surgical center receives a written request for the suspension.

**Procedure:**

- The request for disclosures must be in writing
- The office must provide a written account of the times the PHI has been released. This written account must include:
  - The date the PHI was released.
  - The name of the individual, business, organization or company and address that received the information.
  - A description of the protected health information released.
  - A statement of the reason for the disclosure of the information or a copy of the written request for the information.
- If the same individual made multiple requests, the office must provide the dates of all the disclosures, a statement of the reasons for each disclosure or copy of the written request for the information
- The office must respond to the request within 60 days of receiving the request.
- The office will:
  - Provide the patient with a list of disclosures of PHI.
  - Inform the patient of the reasons why the list will not be prepared within 60 days (if this is the case). The patient must be informed of the date in which the list of disclosures will be available (no longer than an additional 30 days).
- The office must provide the patient with the first request for a list in any 12-nmonth period at no charge. The patient may be charged a seasonable, cost-based fee for each future request within the 12-month period. The office must inform the patient in advance of the fee and allow the patient to decline their request.

- The office will document the patient's request for a list of disclosures. A copy of the disclosures list will be maintained for six years and will include the name of the person fulfilling the request.

### **Right to Privacy Notice**

#### **Policy:**

The policy of this office is to inform patients of their privacy rights and the uses and disclosures of their PHI.

#### **Procedure:**

- The privacy notice will be posted in the main lobby and the website (if applicable).
- Each patient is provided a copy of the privacy notice upon his/her first visit.
- Each patient should sign the Acknowledgment of Receipt of the privacy statement.
- A copy of the privacy notice is provided to anyone upon request.
- The office will retain a copy, and any revisions, of the Privacy Notice for six (6) years.

## HIPAA Privacy & FAQs for Providers

See the FAQs listed below for information on maintaining medical charts, sharing information, leaving messages for patients, and using sign-in sheets.

These FAQs are abbreviated excerpts from the Office for Civil Rights' Frequently Asked Questions located at <http://www.hhs.gov/ocr/hipaa>.

**1. Does the HIPAA Privacy Rule permit doctors, nurses, and other health care providers to share patient health information for treatment purposes without the patient's authorization?**

**Yes.** The Privacy Rule allows those doctors, nurses, hospitals, laboratory technicians, and other health care providers to share protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise. This includes sharing the information to consult with other providers to treat a different patient, or to refer the patient. See 45 CFR 164.506.

**2. Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?**

**Yes.** The HIPAA Privacy Rule specifically permits doctors to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the doctor may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The doctor may also share relevant information with the family and these other persons if he or she can reasonably infer, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient's mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient's payment options with her adult daughter.
- A doctor may instruct a patient's roommate about proper medicine dosage when she comes to pick up her friend from the hospital.

- A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

**3. May a hospital or other covered entity notify a patient's family member or other person that the patient is at their facility?**

**Yes.** The HIPAA Privacy Rule permits covered entities to notify, or assist in the notification of, family members, personal representatives, or other persons responsible for the care of the patient, of the patient's location, general condition, or death. Where the patient is present, or is otherwise available prior to the disclosure, and has capacity to make health care decisions, the covered entity may notify family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also use or disclose this information to notify the family and these other persons if it can reasonably infer from the circumstances, based on professional judgment, that the patient does not object. Under these circumstances, for example:

- A doctor may call a patient's wife to tell her that her husband was in a car accident and is being treated in the emergency room for minor injuries.
- A doctor may contact a pregnant patient's husband to let him know that his wife arrived at the hospital in labor and is about to give birth.
- A nurse may contact the patient's friend to let him know that his roommate broke his leg falling down the stairs, has had surgery, and is in recovery.

**4. Are physicians' and doctors' offices prohibited from maintaining patient medical charts at bedside or outside of exam rooms, or from engaging in other customary practices where the potential exists for patient information to be incidentally disclosed to others?**

**No.** The HIPAA Privacy Rule does not prohibit doctors from engaging in common and important health care practices; nor does it specify the specific measures that must be applied to protect an individual's privacy while engaging in these practices. For example, the Privacy Rule does not prohibit covered entities from engaging in the following practices, where reasonable precautions have been taken to protect an individual's privacy:

- Maintaining patient charts at bedside or outside of exam rooms, displaying patient names on the outside of patient charts, or displaying patient care signs (e.g., "high fall risk" or "diabetic diet") at patient bedside or at the doors of hospital rooms.

Possible safeguards may include: reasonably limiting access to these areas, ensuring that the area is supervised, escorting non-employees in the area, or placing patient charts in their holders with identifying information facing the wall or otherwise covered, rather than having health information about the patient visible to anyone who walks by.

- Announcing patient names and other information over a facility's public announcement system.

Possible safeguards may include: limiting the information disclosed over the system, such as referring the patients to a reception desk where they can receive further instructions in a more confidential manner.

- Use of X-ray lightboards or in-patient logs, such as whiteboards, at a nursing station.

Possible safeguards may include: if the X-ray lightboard is in an area generally not accessible by the public, or if the nursing station whiteboard is not readily visible to the public, or any other safeguard which reasonably limits incidental disclosures to the general public.

**5. May a health care provider disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS)?**

**Yes.** The HIPAA Privacy Rule permits a provider to disclose protected health information to a health plan for the quality-related health care operations of the health plan, provided that the health plan has or had a relationship with the individual who is the subject of the information, and the protected health information requested pertains to the relationship. See 45 CFR 164.506(c)(4). Thus, a provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, so long as the period for which information is needed overlaps with the period for which the individual is or was enrolled in the health plan.

**6. May physicians' offices or pharmacists leave messages for patients at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready? May providers continue to mail appointment or prescription refill reminders to patients' homes?**

**Yes.** The HIPAA Privacy Rule permits health care providers to communicate with patients regarding their health care. This includes communicating with patients at their homes, whether through the mail or by phone or in some other manner. In addition, the Rule does not prohibit covered entities from leaving messages for patients on their answering machines. However, to reasonably safeguard the individual's privacy,

covered entities should take care to limit the amount of information disclosed on the answering machine. For example, a covered entity might want to consider leaving only its name and number and other information necessary to confirm an appointment, or ask the individual to call back.

**7. How should appointment reminders be handled for patients who request confidential communications?**

In situations where a patient has requested that the covered entity communicate with him in a confidential manner, such as by alternative means or at an alternative location, the covered entity must accommodate that request, if reasonable. For example, the Department considers a request to receive mailings from the covered entity in a closed envelope rather than by postcard to be a reasonable request that should be accommodated. Similarly, a request to receive mail from the covered entity at a post office box rather than at home, or to receive calls at the office rather than at home are also considered to be reasonable requests, absent extenuating circumstances. See 45 CFR 164.522(b).

**8. May physicians' offices use patient sign-in sheets or call out the names of their patients in their waiting rooms?**

**Yes.** Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

**9. Can a patient have a friend or family member pick up a prescription for her?**

**Yes.** A pharmacist may use professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person, other than the patient, to pick up a prescription. See 45 CFR 164.510(b). For example, the fact that a relative or friend arrives at a pharmacy and asks to pick up a specific prescription for an individual effectively verifies that he or she is involved in the individual's care, and the HIPAA Privacy Rule allows the pharmacist to give the filled prescription to the relative or friend. The individual does not need to provide the pharmacist with the names of such persons in advance.

For additional information on these FAQs and other frequently asked questions visit the Office for Civil Rights' Web site at <http://www.hhs.gov/ocr/hipaa/>.