HIPAA Protecting Patient Privacy

In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), our office must ensure the confidentiality, integrity and availability of all the protected health information ("PHI") it creates, receives, maintains or transmits. Our office must also protect against any reasonably anticipated hazards to the security and integrity of PHI. The following information and guidelines should provide all employees the information needed to properly handle and maintain PHI.

What is considered protected health information?

PHI is generally any individually identifiable information that is transmitted or maintained by electronic or other media that relates to an individual's past, present or future physical or mental health, treatment, payment for services or healthcare operations. To be PHI, the information must identify the individual or provide a reasonable basis for identifying the individual.

Examples of PHI include:

- A person's name, address, birth date, e-mail address
- Medical records, prescriptions, lab work and test results
- Billing records, referral authorizations, claim information

We must protect all PHI that includes items such as medical records, diagnoses, X-rays, photos and images, prescriptions, lab work and test results, billing records, claim data, referral authorizations and explanation of benefits.

Who is authorized to access confidential PHI?

Information that our office collects or creates that relates to patient health or to patient care can only be used in limited ways without patient authorization. Patient authorization is not required when doctors, nurses and others use information about patients to determine what services they should receive or to review the quality of their care. PHI may also be used without patient authorization to bill patients (or their insurance companies) for the services they received or to fulfill other necessary administrative and support functions.

Disclosure is also permitted without authorization in a number of other situations. These include:

- Healthcare providers are required to report certain communicable diseases to state health agencies, even if the patient doesn't want the information reported.
- Courts have the right to order healthcare providers to release patient information with appropriate court orders.
- Under limited circumstances, healthcare providers may disclose PHI to police (such as reporting certain wounds or injuries, or to comply with a court-ordered warrant or grand jury subpoena).
- When physicians or other people providing patient care suspect child abuse or elder abuse, they must report it to state agencies.
- Healthcare providers report information to coroners and funeral directors in cases where patients die.

These disclosures are further explained in our Notice of Privacy Practices. For many other uses and disclosures of PHI, our office must get a signed authorization from the patient.

What is the "minimum necessary" standard?

The minimum necessary standard in the HIPAA Privacy Rule requires that when a covered entity uses or discloses protected health information or requests protected health information from another covered entity, the covered entity must make reasonable efforts to limit protected health information to that which is reasonably necessary to accomplish the intended purpose of the use, disclosure or request. You are expected to apply the minimum-necessary standard when you access PHI. For example, although physicians and nurses may need to view the entire medical record, a billing clerk would likely only need to see a specific report to determine the billing codes. You are permitted to access and use only the minimum patient information necessary to do your own job.

What rights do patients have to their PHI?

Patients' rights under HIPAA are described in our Notice of Privacy Practices. These rights include:

- **Right to Receive a Paper Copy of the "Notice of Privacy Practices."** This notice informs patients of their HIPAA rights and how to exercise them.
- **Right of Access.** Patients may request to inspect their medical record and may request copies, including electronic records.
- **Right to Request an Amendment.** Patients may file a request for an amendment to their medical record.
- **Right to an Accounting of Disclosures.** Patients have the right to receive an accounting of disclosures which documents those disclosures for which the patient has not signed an authorization.
- **Right to Request Restrictions.** Patients have the right to request restrictions on how we will communicate with the patient or release information.
- **Right to Complain.** Patients have the right to complain if they think their privacy rights have been violated.
- **Right to Receive Notice of a Security Breach.** Patients have the right to be notified if their health information has been breached.

If a patient requests any of the above, please refer them to our Privacy Officer.

What steps must I take to safeguard PHI?

Here are some common ways that employees can protect patient privacy:

- Talk on the phone in closed quarters, and be careful what you disclose aloud.
- Close patient room doors when discussing treatments and administering procedures.
- Avoid discussions about patients in elevators and office hallways.
- Do not leave messages on answering machines regarding patient conditions or test results.
- Avoid paging patients using identifiable information, such as their condition or name of physician.
- Avoid leaving a patient's medical file on your computer screen when you leave your desk. It is best to log off when leaving a workstation. In public areas, point computer monitors so visitors or people walking by cannot view information.

What if I see someone violate HIPAA?

If you become aware of any HIPAA violation, including a security breach, immediately report it to your supervisor or our Privacy Officer.