# DILEY RIDGE MEDICAL CENTER

## HIPAA & Privacy Overview

## *HIPAA Regulations*

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by Congress in 1996. The HIPAA Privacy Rules became effective in April 2003 and the HIPAA Security Rules became effective in 2005.

Major amendments to the original privacy and security rules were enacted into law in February of 2009 as part of the American Recovery and Reinvestment Act of 2009. The specific revisions are referred to as the Health Information Technology for Economic and Clinical Health Act or the HITECH Act. Some of the first provisions of the HITECH act to be enforced are those that strengthen the civil and criminal enforcement of the HIPAA rules and under certain circumstances, notification of patients if privacy rights have been violated. As the HITECH laws are implemented, Diley Ridge will strive to keep physicians informed of the implications of the law.

Diley Ridge Medical Center and Medical staff jointly use and disclose patient's health information during the provision of services that we provide. Since we are both covered entities under HIPAA, we both have the same obligations and duties to protect information. Regardless of HIPAA, we both have a duty to:

- Protect and safeguard information;
- Educate patients on their rights regarding their information;
- Protect the patient's rights;
- Ensure their information is used and disclosed appropriately; and
- Ensure that appropriate administrative requirements are fulfilled.

## *The Privacy Officer*

Under HIPAA, each organization is required to select someone to serve as the Privacy Officer. This person is responsible for developing and maintaining privacy related policies and procedures, providing training and overseeing the privacy functions in Diley Ridge. Our Privacy Officer is Christie Santa-Emma who can be reached at 614-546-3284 or at csanta-emma@mchs.com

.

## *Benefits*

**Benefits to the Patient**

Patients receive several benefits under the privacy rules of the Administrative Simplification requirements. Some of these benefits include:

- An understanding of how their protected health information (PHI) may be used by the Diley Ridge and/or the Medical Staff.
- The ability to approve who may use or disclose their PHI.
- A right to access and amend PHI.

**Benefits for Diley Ridge Medical Center and the Medical Staff**

- Enhance patient confidence and develop a positive public image in the community as a result of efforts taken to protect patient information in compliance with the privacy and security standards.

- Minimize the potential for civil and/or criminal penalties and fines.

## *Failure to Comply*

Compliance with HIPAA and the Administrative Simplification requirements is very important. A facility or provider that does not follow the rules may:

- Be responsible for civil penalties and fines that can quickly add up to thousands of dollars.
- Be accused of criminal violations that can result in even larger penalties and fines, along with possible jail time.
- Be excluded from participation in the Medicare program.

## *Privacy Rules*

Starting on April 14, 2003, the privacy rules set the minimum standards that all providers must follow to protect patients' health information. The key term that you will hear when discussing the privacy rules is Protected Health Information:

**Protected Health Information (PHI):** Information in any format related to any healthcare provided to a person. This includes demographic information that can be used to identify the patient. Information that can be used in some manner to identify the person (e.g. social security number) is also considered PHI.

## *Patient Rights*

**Notice of Privacy Practices**

Patients have the right to receive a Notice of Privacy Practices (NPP) which describes patient rights under the privacy rule as well as how the covered entity (health care provider, payer/health plan, health care clearing house) will use and disclose their information. The document must be given to the patient at the first encounter to the covered entity.

The covered entity must make every effort to have the patient sign a written acknowledgement that the NPP was offered. The notice must provide the name or title and phone number of a contact person in the event the patient wishes to file a complaint. The NPP must be easy to read and understandable. It also must be prominently posted in the facility.

## *Patient Rights*

Patients have several basic rights regarding their protected health information or PHI such as:

- The right to a **Notice of the Privacy Practices** of Diley Ridge and the Medical Staff (discussed in the previous section)
- The right to **Request Additional Privacy Protections** and **Confidential Communications**. Patients may request that additional steps be taken to protect their PHI. Patients can also request that PHI be provided in a different, confidential manner (e.g. mailing PHI to a different address or

sending information to an e-mail address instead of the patient's home address, etc.).

- The right to obtain **Access to their PHI**. With certain exceptions, patients have a right to review and copy their PHI.
- The right to **request an Amendment to their PHI**. Patients can request that Diley Ridge make changes or updates to their PHI if needed. Certain rules and exceptions apply here too.
- The right to an **Accounting of the Uses and Disclosures of their PHI**. This includes how certain PHI has been disclosed for certain reasons, for a period of up to 6 years, as well as who has received those disclosures
- The right to **agree or object** to specific disclosures of their PHI, for example, from a facility directory, for disaster relief purposes, or to family or friends involved in their care.
- To **file a complaint** with Diley Ridge or directly to the Department of Health and Human Services. Diley Ridge must promptly investigate and respond to complaints

## *Privacy Policies and Procedures*

As part of the privacy practices, is required to have written policies and procedures relating to PHI and information practices. Below is a general listing of some of the types of policies and procedures:

- Confidentiality policy
- Records retention policy
- Employee training policy
- Employee termination policy
- Release of information policies

## *Safeguards and Sanctions*

Diley Ridge must develop the necessary administrative, technical and physical safeguards for PHI. Diley Ridge must also reasonably protect PHI from intentional or accidental use or disclosure, or other possible violation of the rules. Diley Ridge Medical center, in coordination with the Medical Staff must identify what happened and those responsible for the improper disclosure. Disciplinary actions must be taken as appropriate. These actions, or sanctions, should consider the severity and intent of the violation. They should also consider if there is a pattern or practice of improper use or disclosure of PHI. Disciplinary actions could range from a warning to termination.

Beginning in September of 2009, the new HITECH requirements require that under certain conditions, patients are notified of a breach in their PHI. At Diley Ridge the Privacy Officer will work to determine if the violation meets the breach notification requirements. Additionally, depending on the nature and the magnitude of the breach, the United States Department of Human Services and Media outlets may need to be notified.

## *Incidental and Oral Communications*

The Privacy Standards apply to PHI that is oral, written, stored in computer files, and stored in paper medical records.

Many patient complaints lodged with the Office of Civil Rights (OCR) – the Department of Health and Human Services entity that oversees HIPAA Privacy and Security – involve the inappropriate disclosure of oral PHI.

HIPAA does allow for incidental disclosures, **BUT PHYSICIANS MUST TAKE REASONABLE SAFEGUARDS**, to prevent others from overhearing or seeing protected health information.

Do not discuss results of surgery in a surgery waiting area. Take the family to a less public location.

**Always request the patient's permission prior to sharing any PHI in front of other individuals present in the room. This includes immediate family members. Another option is to request that all leave the room while you update the patient. This takes the burden off the patient to ask visitors to leave.**

The goal of the privacy rule is not to prevent needed discussions related to patients, but to make sure that when discussions need to take place, Diley Ridge and the Medical Staff are doing what is reasonable to protect a patient's PHI. If a facility/provider does not take reasonable steps to protect patient privacy, it could be found in violation of the privacy rule.

It really means using your best judgment, for example:

- Discussions in busy hallways and elevators mean that anyone around can overhear the conversation
- Use overhead paging, only when absolutely necessary
- Patient information that is visible on computer screens should be kept confidential. Unless impossible to accomplish, screens should be located to avoid access or viewing by unauthorized users. Log off applications when you have completed your business.
- When phoning patients, messages should be kept to a minimum when the patient cannot be reached directly. Leave only your name and number, not diagnostic information, or the reason you are calling.
- Place patient information in a secured location when not in use. Secure information that you carry on your person. Use the appropriate document destruction bins to dispose of information that has PHI on it.

## *Reporting Concerns and Violations*

The Privacy regulations are complex, and you may have questions from time to time. To seek answers to questions or concerns, including possible violations of the law, or policies and procedures it is recommended that:

1. Call the Privacy Officer directly at 614-546-3284.

## *De-identification and Re-identification*

At times, Diley Ridge Medical Center or members of the Medical Staff may want or need to de-identify health information. For example, a pharmacy is doing a study to determine how many patients with a specific condition have been admitted to a local hospital. The results of the study will help the pharmacy budget their inventory for a very expensive drug that is used to treat that condition. By obtaining de-identified health information, the pharmacy will be able to maintain the necessary supply of the drug and the hospital will be able to help make sure patients receive the treatment they need.

HIPAA lists specific information that must be removed for PHI to be considered de-identified. We can remove code or encrypt the information to create de-identified information. In any of these processes, we must be reasonably sure that the remaining information cannot identify the person, either by itself or in combination with information from another individual or organization.

- Obtain a data use agreement that:
- Specifies the permitted uses and disclosures of the information;
- Identifies who can use the information;
- Includes an agreement that the recipient of the information will not re-identify the information or contact the individual; and,
- Provides that the recipient of the information has appropriate safeguards in place to prevent use or disclosure of the information other than for the intended purpose, or otherwise allowed under the privacy rule.

Use or disclosure of limited data set PHI for purposes other than those specifically identified in the privacy rules would be considered a violation.

## *Summary*

Providers are already protecting information. With a few exceptions, HIPAA did not create new principles, or new ideas. It attempted to have a set of standards for all providers, across all practice settings. It also provides each of us an opportunity to improve the ways that we utilize and disclose information.

If you have additional questions or concerns please contact the Privacy Officer, Christie Santa-Emma, for Diley Ridge Medical Center at 614-546-3284.