



HIPAA

(Health Insurance Portability & Accountability Act of 1996)

**Presented by Stephanie Fowler, RHIA,
Director of Health Information Management & Privacy Officer**

2012 Orientation to HIPAA Privacy Rule Compliance

PHI Definition

- ❑ **PHI (Protected Health Information) is identifiable health information that RMC or any covered entity has acquired in the course of serving its patients.**



Examples of PHI

Data elements that make health information identifiable include:

- ^ Patient Name
- ^ Address
- ^ Employer
- ^ Relatives' Names
- ^ Date of Birth
- ^ Telephone Numbers
- ^ Fax Numbers
- ^ E-mail Addresses
- ^ Or any other linked number, code or characteristic
- ^ Social Security #
- ^ Member/Account #
- ^ License #
- ^ Fingerprints
- ^ Photographs

HIPAA Provides for Specific Uses of PHI...

- ❑ PHI may be used & shared without authorization for purposes of:
 - ❖ Treatment – Ongoing Care
 - ❖ Payment – Doctors, hospitals, insurance payers, including Medicare & Medicaid
 - ❖ Operations – Running the business of health care
- ❑ *This is explained in the Notice of Privacy Practice*

Safeguards to Protecting PHI

- ❑ Refrain from discussing PHI aloud in public areas of RMC, such as cafeteria, nursing units, treatment areas, etc.
- ❑ Destroy all documentation containing PHI. Shred-it bins are available on all units. If small recycle receptacles are used at your desk, please empty into shred-it bin at end of shift.



Facts on HIPAA Breach

- What is a breach?
 - The acquisition, access, use or disclosure of protected health information (PHI) in a manner that is not permitted by the Privacy Rule (role based access – only access patients that you are currently treating or are performing a role based task such as coding, billing)
- Covered entities (which includes hospitals, physician practices, etc.) are required to report breaches that result in a privacy violation
- Not all breaches will result in a violation but you should report all of them so that a full investigation can be done

Your Role

- **If you are made aware of, or suspect a misuse or improper disclosure of a patient's information, contact your Privacy Officer immediately**
- Do not notify the patient / family yourself
- Be aware of how you utilize patient's health information in your job and protect the information from unauthorized disclosure
- Review your facility's privacy and security policies
- If a suspected incident is in question, a full risk assessment will be conducted internally to determine if the breach is reportable
- You will not be retaliated against for reporting a suspected incident in good faith
- Failure to report a suspected incident could result in disciplinary action



Social Media

Some examples:

- Facebook
- Twitter
- My Space
- LinkedIn
- Blogging
- Online posting of photos



Social Media

- Healthcare providers have an obligation to protect PHI during **and** following treatment of a patient and this obligation does not expire because a patient discloses their own condition online through a media source.
- HIPAA Security rules require us to protect “electronic” PHI

Social Media

You may think you are safe as long as you don't use a patient's name BUT not true:

- Someone may be able to determine the patient's name by other details stated
- It is not lawful to even provide the fact that someone is a patient (mere existence of the provider/patient relationship is considered to be PHI)
- Reply or discussion on a blog that was initiated by the patient
- Posting a picture of a patient (sad because my favorite patient died today)

Privacy Officer Contact Information

- RMC Privacy Officer –
Stephanie Fowler, RHIA
stephanie.fowler@LPNT.net
770-918-3376
- LifePoint Corporate Privacy
Officer –
Tina Qualls, RHIT
tina.qualls@LPNT.net
615-372-8511

A friendly reminder to



ZIP IT

with patient information.

All information concerning a present or former patient's care, treatment, diagnosis, prognosis and personal affairs is strictly confidential and is to be discussed or disclosed only by authorized personnel on a need-to-know basis.

Whether information concerning the patient is obtained during the course of one's regular duties or accidentally

overheard while performing work, employees must refrain from discussing such information with unauthorized persons, in or out of the hospital, in order to ensure the patient's right to privacy.

Violation of employee/patient confidentiality is grounds for discipline, up to and including termination.

Orientation Training Acknowledgement

- I acknowledge that I have received training provided by Rockdale Medical Center on HIPAA Privacy and Suspected Incidents (breach)
- I further agree that I will report promptly any known or suspected violations to the Privacy Officer or designee

Print Name

Hire Date

Date of Training: _____

Signature: _____

Dept Name

Manager's Name