Med Center Health

HIPAA Privacy & Security Code of Conduct

WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a complex piece of legislation covering three areas.

1. Insurance Portability
2. Fraud Enforcement
3. Administrative Simplification

Protected Health Information (PHI)

HIPAA PROTECTS THE PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION (PHI)

- PHI can be in the following formats: oral, written, typed, or electronic.
- PHI can be for a person who is living, dead, public figure, or private person.
- PHI can be related to physical health and/or mental health.

WHAT IS PROTECTED HEALTH INFORMATION (PHI)?

- Protected Health Information (PHI) is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service, such as diagnosis or treatment.
- **There are 18 Identifiers that HIPAA recognizes as PHI including:**
  - Name, address, telephone numbers, fax numbers, Social Security Number, medical record number, photographic images, biometric identifiers, email addresses, health plan beneficiary numbers, account numbers, certificate/license numbers, birth date, and others.

MINIMUM NECESSARY RULE

- HIPAA requires that we use the **minimum necessary** information needed to do our job.
- Ask yourself, "Do I need to know this information to do my job?"
- Only access the minimum amount of patient information you need to know.

WAYS TO PROTECT PATIENT PRIVACY

- **Close patient room doors when discussing treatments and administering procedures.**
- **Close curtains and speak softly in semi-private rooms and hallway bed areas.**
- Avoid discussing patients in elevators and cafeteria lines.
- Don't leave messages on answering machines about patient conditions or test results.
- Don't leave patient records lying around or forget to log off your computer.
- Don't assume it is okay to discuss a patient with a family member or friend.

CASE SCENARIO #1

James, RN, just received a patient and is completing the admission assessment on his new patient. Sensitive medical information and history are discussed loudly. The patient is in a semi-private room, and the other bed is occupied by another patient. The other patient also has visitors present in the room. James does not attempt to minimize the chance of others overhearing the information. The patient James completed the assessment on later complains to the House Administrator.

- Is this a HIPAA breach?
- What should the nurse have done differently?

ANSWER

- Yes, it is possible that this situation constitutes a HIPAA breach.
- Discussions in semi-private rooms (or hallway bed areas) do not violate HIPAA privacy requirements, and are considered "incidental disclosures," ***if*** reasonable safeguards are implemented to minimize the risk of others overhearing the conversations.
- In this situation, James could have asked the visitors to leave until the assessment was over and spoken in a softer voice during the assessment. Additional precautions could also have been possible such as temporarily relocating the other patient, if feasible, performing the assessment in a private area, etc.
- Each encounter is different; however, providers should always take any and all reasonable safeguards practical for the situation to protect the patient's privacy.

CASE SCENARIO #2

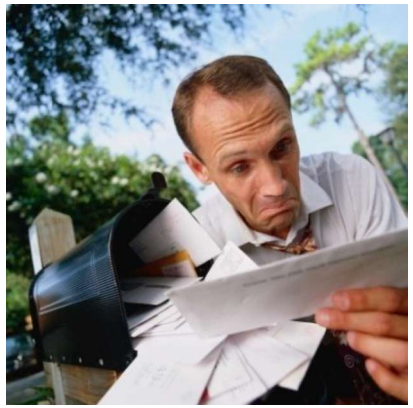
Anna is concerned that a co-worker may be using patient information for a non-work related reason. Anna only has a good-faith suspicion but no hard evidence.

- What should Anna do?

ANSWER

- Anna should use the internal reporting process to make her concerns known.
- Anna will not be disciplined for making a good faith concern known even if she turns out to be wrong.
- Anna does not have to be able to "prove" a concern is true to make a report.
- Anna can ask to remain anonymous.
- Every employee must report compliance or privacy concerns.

POSSIBLE PRIVACY BREACHES



- Accessing patient information out of curiosity.
- Faxing or mailing patient information to the wrong location.
- Leaving patient information on the answering machine of the wrong individual.
- Losing an unencrypted flash drive, laptop, or portable electronic device containing patient information.

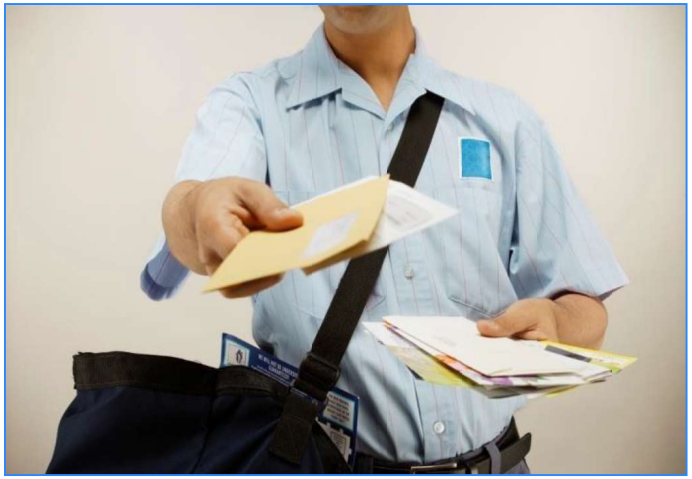
POSSIBLE PRIVACY BREACHES

- Disposing of patient information in the trash.
- Sending the wrong discharge instructions home with a patient.
- Posting patient information on social networking sites, such as Facebook and Twitter.
- Texting patient information to cell phones not secured by Med Center Health.
- Accessing patient information for non-work related reasons.

BREACH NOTIFICATION

- Med Center must notify patients within 60 days if their unsecured patient information was acquired, accessed, used, or disclosed inappropriately.
- The notice must describe what happened and what the organization is doing to investigate the breach, how similar breaches will be prevented in the future, steps individuals can take to protect themselves,
  and contact information.
- **Breach investigations and notification will be handled by the Privacy Officer.**

BREACH NOTIFICATION



- Breaches involving 500 or more patients will require notification of the U.S. Department of Health and Human Services for posting on its website and in the media.
- The Privacy Officer will report the breaches to the government in accordance with our HIPAA Privacy Breach Notification Policy.

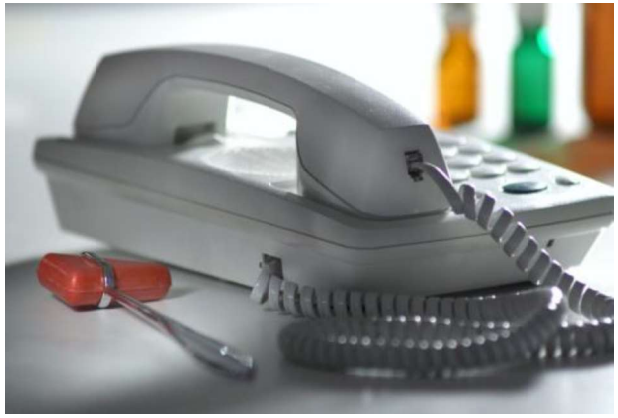
HIPAA PRIVACY & SECURITY REMINDERS

- Protected Health Information (PHI) is only released with written authorization of the patient or as required by law.
- **ALL** patient records, even medical records of employees, must be released in accordance with our Release of Information Policy.
- Abide by the "minimum necessary" rule.
- Remember that patient privacy is the responsibility of **ALL employees**.

INTERNAL REPORTING PROCESS

If you suspect a patient's privacy has been violated, if a patient tells you his/her patient information has been accessed, used or disclosed inappropriately, or you have questions about HIPAA, contact:

- Your supervisor
- Your Compliance/HIPAA Privacy Officer



INTERNAL REPORTING PROCESS

If you wish to report a concern anonymously you may contact the Compliance Hotline at 800-826-6762.

Every employee must report compliance/privacy complaints or issues of any kind, immediately!

COMPLIANCE/LEGAL/ HIPAA PRIVACY

If you have questions or concerns about Compliance or HIPAA privacy, contact:

Joseph M. Newton, JD, CHC, CFE

Director of Corporate Compliance and Privacy

Phone 270.796.6553

Email NewtJM01@MCHealth.net

CORPORATE INFORMATION SECURITY OFFICER

If you have questions or concerns about information security, contact:

Daniel Morrison

Corporate Information Security Office

Phone: 270.796.5580

Email: morrds@mchealth.net

PRIVACY ACKNOWLEDGEMENT

I understand my responsibilities and duties regarding Privacy and Compliance, as well as the disciplinary actions that may apply as a result of my failure to follow the regulations explained verbally and/or in writing. These disciplinary actions consist of, but are not limited to: verbal and written reprimands and possible termination of employment. I understand it is a condition of continued employment to report known or suspected wrongdoing.