Scenarios: Applying Security and Privacy Measures

Scenario 1:

Using Electronic Health Record (EHR) Access Privileges to View a Relative's Medical Record.

Situation: Sandy is a RN at a hospital where her mother has recently been discharged. Sandy works exclusively in the maternity ward while her mother was a patient in the ED. Is it permissible for Sandy to access her mother's medical records?

Response: No. By accessing this information, Sandy would be violating the federal Health Insurance Portability and Accountability Act (HIPAA) regulations. Sally does not need this information to do her job and would be accessing this information for personal reasons.

Scenario 2:

Sharing Unique IDs and Passwords

Situation: Amanda has been tasked with training her new coworker, Mark. Mark has yet to be given his own log in information so Amanda has not been able to show him the applications they use on a daily basis. Would it be okay for Mark to use Amanda's log in information until he receives his own?

Response: No, it is best practice to use exclusively your own log-in information. Do not share your unique log-in information with co-workers. Mark should wait until he receives his own log-in from HR.

Scenario 3:

Disclosing Information to Others Inappropriately

Situation: Pamela works for a cardiology practice. The cardiologists in the practice admit patients to Mount Carmel hospitals. Pamela schedules an admit for her neighbor, Cindy. The following week, Pamela receives multiple messages from her neighbors asking if she knows anything about Cindy's condition. How should Pamela respond?

Response: Pamela must not disclose any information about Cindy obtained as a result of her work in the cardiology practice, not even with Cindy's family or friends. Pamela should politely inform the concerned neighbors that federal laws prohibit the sharing of confidential information about patients without their expressed permission.

Mount Carmel Health Partners

6150 E. Broad St.
Columbus OH 43213
Questions? Email us at HPPE@mchs.com
Reference: OPTUM360 ICD-10-CM 2020

Information Privacy and Security: A Reference Guide

For Employees of Mount Carmel Health Partners and its Affiliates

MOUNT CARMEL
Health Partners

A Member of Trinity Health

Protection of Patient Health Information in Health Systems

- Actively protect the sensitive patient information on devices and work stations
- Log in only with your unique log in and password—Do not give out your log in information
- Sign out or log off of your work station before walking away
- Report any observed password sharing to your supervisor
- Protect the privacy of your computer when viewing protected patient information
- Appropriately dispose of patient information (shred, delete, etc.) when no longer needed.
- Lock file cabinets and office doors where confidential information is stored
- Never leave laptops, tablets, or paper files in unsecure places– public locations, your car etc.
- Be wary of unsolicited emails and avoid clicking links or attachments until you are certain they are from legitimate sources.

Appropriate Use

- Access and use patient information and EMR systems only as needed to do your job.
- Access, use, or disclose patient or other confidential information only for legitimate business purposes, and never for personal or other reasons.
- Access only the minimum necessary amount of confidential information that you need in order to perform your job.
- Do not use information systems to transmit information that is abusive, offensive, disparaging, or a violation of the law.
- Do not attempt to download, copy, or install software residing on any health care network or any other computer.

Additional resources can be found at CMS.gov or HHS.gov

How to Detect "Phishing" Emails

⇒ **Avoid any emails from an unknown personal email account, @gmail or @Hotmail for example, as this is likely phishing.**

⇒ **Be suspicious of emails addressed to "Dear Customer" or another generic greeting.**

⇒ **Phishing emails often include grammatical and spelling errors.**

⇒ **Be suspicious of any email that requires "immediate action" or creates a sense of urgency.**

⇒ **Be careful of links, only click on those you were expecting.**

⇒ **Be suspicious of links. Only click those you were expecting.**