While the HIPAA Security Policies and Procedures specify the responsibilities of all employees and workforce members for safeguarding Electronic Protected Health Information (EPHI), this newsletter provides a summary of general information and educational reminders on some of the key components of the regulation. In this issue we’ll cover General HIPAA Security Information.

All MCW workforce members are responsible for protecting the health information of our patients and research participants. In our environment, MCW workforce members are generally defined as employees, volunteers, trainees, and students. Some general HIPAA Security requirements are listed below.

**Accessing EPHI**

- MCW workforce members cannot be given access to information systems containing EPHI until approved by a supervisor, manager or other person with the authority to grant the access.
- MCW workforce members cannot attempt to gain access to MCW information systems containing EPHI for which they have not been given proper authorization. Don’t try to enter a system if you haven’t been authorized to do so.
- MCW workforce members cannot provide access to MCW information systems containing EPHI to any unauthorized persons. Don’t lend your username and password to a coworker as a “favor” in order for them to “quick look something up.”

**Reporting Security Incidents**

- MCW workforce members should report any observed or suspected security incident as quickly as possible to their Desktop Technician, System Manager or contact Information Services at 456-4357. Examples of incidents you should report include:
  - You’re locked out of your workstation, but you know that you haven’t had any failed attempts.
  - Somebody calls you and asks for your password.
  - Data or information that you routinely work with is missing or corrupted.

- MCW workforce members must immediately report to appropriate management and the Office of Public Safety the loss or theft of any Workstation that had EPHI stored on it (e.g. desktop computer, laptop computer, handheld device, etc…)
- MCW workforce members must immediately report to appropriate management and to the Office of Public Safety the loss or theft of any access key or card used to enter server or computer rooms.
- MCW workforce members can’t prevent another member from reporting a security incident. In addition, MCW has a Compliance Reporting Non-Retaliation and Non-Retribution Policy that ensures that no person will be subject to any adverse action for providing information regarding legitimate policy violations.

**Disciplinary Process**

- MCW Workforce Members must comply with all MCW security policies. Failure to comply with these policies may result in appropriate disciplinary action as specified in Human Resources or other applicable policies and procedures.

**COMPUTER SECURITY TIP:**

CLINICAL MEDICAL RECORD, TRANSCRIPTION AND BILLING SYSTEMS TRACK WHO ACCESSES SPECIFIC ACCOUNTS AND ANY ACTION TAKEN ON THOSE ACCOUNTS. HIPAA SECURITY REQUIRES THIS TRACKING.

**YOU CAN REFERENCED ADDITIONAL INFORMATION ON COMPUTER SECURITY AT:**

The MCW HIPAA website:  [http://infoscope.mcw.edu/display/router.asp?docid=8598](http://infoscope.mcw.edu/display/router.asp?docid=8598)
The MCW Information Services website:  [http://infoscope.mcw.edu/display/router.asp?docid=7798](http://infoscope.mcw.edu/display/router.asp?docid=7798)