This newsletter is one in a series that provides general information on key components of the HIPAA Privacy and Security Regulations. More detailed information and policies are available on the MCW HIPAA website.

In previous HIPAA newsletters, the importance of privacy and confidentiality of health information was extensively covered. Also mentioned in these newsletters was the system tracking capabilities. In this newsletter, we’ll cover details of the system tracking and monitoring currently being performed to identify types of inappropriate access to health information.

The HIPAA Security regulation requires that healthcare organizations electronically track and record “who” is looking at “what” Electronic Protected Health Information (EPHI). This is called Audit Tracking.

Audit Tracking Information
The IDX, Epic, Cadence, Affinity, Eclipsys, Chartmaxx and Sunrise systems track who accesses specific patient electronic records, when those records were accessed, and actions taken on those records. The detail of the tracking can be as specific as the user, the workstation, the module and specific activity, the date, the time of day, and how long a screen was viewed. The appropriateness of individuals’ access and use of health information is assessed according to their job duties.

Monitoring Information Tracked
Access to EPHI is not only tracked but the tracking details are monitored to identify inappropriate access. The following are the most frequent types of monitoring performed:

- Employees looking at spouses’ records. (HIPAA does not allow this without a valid authorization.)
- Employees looking at VIP records. VIPs include the following:
  - Internal Executive Leadership
  - High profile media cases
- Employees looking at MCW co-workers and affiliate employees’ records.

Inappropriate Uses of Health Information
The following are examples of the scenarios of inappropriate access and use of health information that could be identified during the monitoring process.

- An employee checking in the Cadence Scheduling System to see what day their spouse’s appointment is scheduled.
- Employees looking at other employees’ and patients’ demographic information in Epic to get their address for non health care related purposes (e.g. sending flowers). The demographics should not be viewed as a “phone book.” They are considered confidential and should only be used for legitimate purposes.
- Employees looking at records because they are concerned with how a co-worker is doing or are concerned with a particular patient’s level of care, including reviewing the status of their condition when the employee is not involved in the patient’s medical treatment. It does not matter whether you believe the individual would not mind if you look at their record. You cannot view any patient’s electronic medical record for reasons other than those that pertain to treatment, payment, operations, or other reasons permitted by the law and College policies.
- An employee looking at electronic medical record information of employees or patients for medical or scientific curiosity and knowledge, if not involved in the treatment of the patient, or in a supervised learning environment.

Disciplinary Process
College employees must comply with all MCW confidentiality, privacy and 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.

College employees can and have been terminated for disclosing and/or viewing health information inappropriately. Curiosity or “I didn’t know” are never acceptable reasons for looking at health information that you shouldn’t be accessing or disclosing. Remember if you need the information to do your job at the College, you’re probably complying with the rules. If you’re looking at health information because you’re curious, you’re in violation of College policies and the law.

COMPUTER SECURITY TIP:
You are solely held accountable for your account access. No one other than you should know your password! Therefore, you shouldn’t write your password down or share it with anyone – INCLUDING CO-WORKERS.

YOU CAN REFERENCE ADDITIONAL INFORMATION ON HIPAA PRIVACY AND SECURITY AT:
The MCW HIPAA website: [http://infoscope.mcw.edu/display/router.asp?docid=7961](http://infoscope.mcw.edu/display/router.asp?docid=7961)