PROTECTING OUR PATIENTS’ PRIVACY

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 this newsletter we’ll cover the importance of viewing, using or forwarding health information only for appropriate and legitimate purposes.

It’s Important
Health information of our patients and research participants is one of the most valued assets the College has. We are entrusted to view, use or forward this information only for appropriate and legitimate purposes. The HIPAA Privacy & Security regulations were enacted to hold organizations and individuals accountable for the protection of this information. Generally, if you need the information to do your job at the College, you’re probably complying with the rules. Curiosity or “I didn’t know” are never acceptable reasons for looking at health information that you shouldn’t be accessing or disclosing.

While every patient is entitled to privacy and confidentiality of their health information, VIPs, high profile individuals and College employees deserve the utmost respect and privacy of their confidential health information.

Examples
The following are examples of when accessing and disclosing health information is NOT appropriate.

- You decide to look at the scheduling system to confirm that a co-worker is actually attending doctor appointments and to determine what illness the co-worker has.

- Your sister wants to send flowers to a friend that she knows is having surgery. You search for the friend’s name in the registration database.

- A high profile medical case that is performed at the hospital is being talked about in the news. You are not involved in the patient’s care but review the medical record “just to look.”

- Your supervisor is going to be on medical leave for a few weeks. You decide to look at their medical record to determine their medical issues.

- You tell your neighbor that someone she knows came to the clinic that day.

User ID and Password
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. For instance, although it may be more convenient, allowing a new employee to use your account because they haven’t received training and haven’t yet been assigned a user id and password is not compliant with HIPAA.

Most importantly, once you log-on to the system you should NEVER let anyone else use the same session. Any actions performed will be tracked to your user id and you will be responsible for any information accessed inappropriately.

Tracking Information
The IDX, Epic, 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.

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. 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.

Importance of Electronic Medical Records (EMRs)
EMRs allow patient information to be accessible and usable at the point of care, wherever and whenever it is needed, and provide the foundation for improving efficiency and quality of patient treatment. Additionally, EMRs have the potential to improve communications and collaboration between healthcare providers. As patient medical records become more integrated and accessible, the College’s ability to protect the security of that information and the privacy of patients becomes increasingly important.

**COMPUTER SECURITY TIP:**
A Web site uses secure technology when the Web address begins with https and a tiny locked padlock appears at the bottom right of the screen.

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)