HIPAA Security Information

AUDIT TRACKING

This newsletter is one in a series that provides general information on key components of the HIPAA Security Regulation. More detailed information and policies are available on the MCW HIPAA website. In this newsletter we’ll reiterate important information that we provided to you in a previous newsletter regarding Audit Tracking.

HIPAA Privacy concerns who can access health information. HIPAA Security concerns how health information is stored or transmitted. No where is the intersection of Privacy and Security more evident than in Audit Tracking.

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

As an Example…

An MCW employee is curious as to why a co-worker has numerous medical appointments in a short time span. The employee decides to look at the scheduling system to confirm that the co-worker is actually attending doctor appointments. The employee doesn’t think this is a violation of HIPAA because she is not reviewing the co-worker’s medical record or billing information. However, the information available in the scheduling system does meet the definition of EPHI and the employee would have violated the HIPAA regulation because she did not have an appropriate purpose for reviewing the information.

Audit Tracking Capabilities

Medical College of Wisconsin, Froedtert Hospital, Children’s Hospital of Wisconsin and the Veterans Administration Medical Center are required to comply with HIPAA Privacy and Security and conduct audit tracking. Because of this requirement, the IDX, Epic, Affinity, Eclipsys, Chartmaxx and Sunrise systems are able to track who accesses specific patient electronic records, when those records were accessed, and actions taken on those records. The level and detail of information tracked varies by system, however the important point to be aware of is that your activity and use of these systems is tracked.

Additionally, the information contained within the scheduling systems, including both IDX and Cadence, is considered patient information and is confidential. Therefore, it is not acceptable to look up co-workers doctor appointments. Supervisors who require confirmation of any doctor appointments for their staff should work with Human Resources to establish the appropriate procedures which include maintaining the employee’s privacy.

This is another reason to never provide your username and password to anyone. If you do, the activities of the person using your username and password will be attributed to you.

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. Curiosity or “I didn’t know” are never acceptable reasons for looking at health information that you shouldn’t be accessing. Generally, 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.

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

COMPUTER SECURITY TIP:

USERS SHOULDN’T WRITE THEIR PASSWORDS DOWN OR SHARE THEM WITH ANYONE – INCLUDING CO-WORKERS.

YOU CAN REFERENC E ADDITIONAL INFORMATION ON COMPUTER SECURITY AT:

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