Welcome to the Medical College of Wisconsin, Health Insurance Portability and Accountability Act (HIPAA) Security newsletter. We will periodically issue this newsletter to all employees, residents and medical students of the College to provide you with information on the HIPAA Security requirements. One of the primary requirements of HIPAA is continuing education for all employees and other workforce members. We will be using this newsletter to provide you with this education.

HIPAA was signed into law over nine years ago in August 1996. There are many components to this Act that have been passed as regulations over the intervening years. Examples include regulations to ensure the portability of a person’s health insurance when changing jobs, additional dollars allocated to the government for fraud and abuse, and steps to streamline the paperwork involved in the business of healthcare. At the Medical College of Wisconsin, HIPAA most commonly has meant “Patient Privacy.”

The Privacy Regulation has been in effect since April 2003 and concerns “who” can look at “what” health information. The College has many policies and procedures related to privacy that can be found by clicking on the following link, or going to the HIPAA website link provided at the bottom of this newsletter.

HIPAA Privacy Policies and Procedures

Recently the counterpart to Privacy has taken effect – the Security Regulation. Security concerns “how” electronic protected health information (“EPHI”) is secured. Security is important when information is either stored (for example, on a floppy disk) or transmitted (for example, by way of sending an e-mail).

HIPAA Security Policies and Procedures

Over the last several months representatives from several College departments, including system managers, have been involved in helping to draft policies and procedures for storing and transmitting EPHI. These policies may be found by clicking on the following link, or going to the HIPAA website link provided at the bottom of this newsletter.

HIPAA Security Policies and Procedures

Although policies and procedures are an important requirement of the regulation, equally important is communicating to all employees some key things to know about computer security, health information stored or transmitted by a computer, and how this impacts your day-to-day activities.

The purpose of these newsletters is to educate, provide you with resources for obtaining additional information, and give you information that should help you protect one of the greatest assets we have at the College and for which we are all responsible for protecting – the health information of our patients and research participants.

Examples of subjects that we will be covering in the coming months include information on:

1. Use of College Computer Workstations
2. Reporting Security Incidents
3. Creating Passwords
4. Storing Health Information on your Computer
5. Laptops and PDAs
6. E-mail Spam
7. E-mail Hoaxes
8. Spoofing and Phishing
9. Viruses
10. Spyware

In addition we will be providing computer security tips and updated links to additional HIPAA information. Stayed tuned over the next few months as we send information out on the above topics, and more.

COMPUTER SECURITY TIP:
ON WINDOWS 2000 AND XP OPERATING SYSTEMS, PRESSING THE “CTRL-ALT-DELETE” KEYS AT THE SAME TIME AND SELECTING “LOCK COMPUTER” ALLOWS YOU TO IMMEDIATELY SECURE YOUR COMPUTER IF YOU ARE LEAVING YOUR DESK.

YOU CAN REFERENCE ADDITIONAL INFORMATION ON COMPUTER SECURITY AT:
The MCW HIPAA website:  http://infoscope.mcw.edu/display/router.asp?docid=8598
The MCW Information Services website:  http://infoscope.mcw.edu/display/router.asp?docid=7798