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 cover some important information for you regarding workstation Log-in and Logoff processes you need to be aware of.

**Log–In**

MCW and its workforce members are required by HIPAA to monitor log-in attempts for Information Systems containing Electronic Protected Health Information (EPHI) and to follow-up on discrepancies if appropriate. Many of the steps to help secure log-in attempts are maintained by your system administrator, however you have a role to play as well.

Access to all MCW Information Systems containing EPHI must be via a secure log-in process (e.g. via a Unique Username and Password). Examples of how the log-in processes of these systems are set up follow:

1. The number of unsuccessful log-in attempts allowed is limited to 5 or fewer.

2. Passwords are not displayed while being input by the user.

3. Systems only validate log-in information when all data has been input. If an error arises, the system will not indicate which part of the data is correct or incorrect. For example, systems will not indicate whether you entered an incorrect username, or an incorrect password – only that you entered incorrect information.

Once the user has successfully logged-in to many systems at the College including network access as provided by MCW Information Services, IDX, or Epic Systems, the date and time of either the last interactive log-in or attempted log-in will appear. The user is responsible for reviewing this information and verifying that they were the individual who last signed in. If there is a discrepancy between the date and time on the screen compared to the date and time the user believes they last logged-in, the user should notify their Desktop Technician, System Manager or contact Information Services at 456-4357.

**Logoff**

MCW workforce members must terminate electronic sessions by logging out of Information Systems that contain or access EPHI unless the Information System is secured by a locking method as described below.

1. MCW workstations must contain locking software (e.g. screen saver locking software) that is activated after 20 minutes of inactivity on the workstation, or less time if the workstation is in a high risk area (e.g. front desk/registration workstations, or workstations close to the public’s access).

2. As an extra security precaution the user can lock their workstation at any time. 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 or area.

3. High risk MCW applications (e.g. IDX) that contain or can access EPHI will automatically terminate after 20 minutes or less of inactivity.

4. Special precautions must be taken with “portable workstations” such as laptops and Personal Digital Assistants (PDAs). Locking software is required on all portable workstations and must activate after 20 minutes of inactivity.

**COMPUTER SECURITY TIP:**

The best defense against spam is not to respond to unsolicited email spam, but simply delete these messages.

**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