Employee Security Responsibilities

Confidentiality of Patient Information and Your Roles

INSIDE:

1. What is Patient Information?
2. Access to Patient Information is Determined by the Need to Know
3. How to get Access to Applications, Systems and Networks
4. IDs and Passwords
5. General Security Issues
6. Computer Security Incidents
7. Security Incident Escalation Procedures
8. Contacts to Get Answers to Your Security Questions

You are responsible for ensuring that UMHHC Patient Information is kept confidential.

What is Patient Information?
- Medical record, including data recorded on paper, microfilm, or computer database
- Multimedia representations
- Administrative data
- Business or financial records

Access to Patient Information is Determined by the Need to Know

The Need to Know:
Necessary to fulfill the mission or charge of the UMHHC and its clinical staff, employees, trainees, students, volunteers, or vendors to provide quality patient care, education, and research

Examples of the Need to Know:
- Rendering care to specific patients
- Billing and collecting for services
- Financial analysis
- Provision of educational materials, given at the direction of treating physician

Examples of Inappropriate Use:
- Disseminating knowledge of who is at hospital
- Using personal patient information to make employment decision
- Accessing employee medical information to check up on employee
- Using the information technology resources in ways that interfere with use by other users

Examples of Appropriate Use:
- Include as intended use: schoolwork, communicating with family and friends, and information gathering not related to school assignments but for self-awareness
- Using only the ‘Uniqname and UMHS System-ID’s assigned to you by the University of Michigan

Release of Patient Information Outside of UMHHC:
- Restricted to those with a legal right to know

How to get Access to Applications, Systems and Networks
- Your manager (or other authorized signer) will submit a Remedy ticket to obtain access to the applications, systems and networks required for you to perform your job.

- Using games on the servers
- Using e-mail to harass or threaten other users
- Sending chain messages, message sent to 1 or more persons that ask the person(s) to contact several other people and has some promise of reward for doing so or threat of punishment for not doing so
- Sending illegal material such as pornographic or obscene messages, images, recordings, etc.
- Accessing another user’s electronic mailbox or reading someone else’s e-mail without his/her permission
- Handing out passwords to non-UMHS staff

Last Update: June 2004
The Keys to Patient Data

Passwords:

♦ Your manager will explain the password requirements for each application or operating system required for you to perform your job.

Bad Password Examples:

♦ Dictionary words (house, mother, etc)
♦ Foreign words
♦ Simple transformations (justin7, 7eleven)
♦ Repeated words (kittykitty)
♦ Names of people
♦ Keyboard sequences (qwerty, ghjkl)
♦ Phone numbers
♦ Words with vowels removed

Good Password Strategy:

♦ Use a line from a song or verse
  ♦ Verse: "I pledge allegiance to the flag of the United States of America"
  ♦ Password: ipattfotusoa
♦ Add Numbers
  ♦ "Mary had a little lamb"
  ♦ m1h3a5i7l

For more information refer to the Understanding Passwords Guide.

General Security Issues

Hospital Security:

♦ Wear your ID at all times when on hospital property.
♦ If you see someone without a badge in a secure area, ask to help him or her.

♦ If you are unsure about any visitor’s purpose in your area, contact security.
♦ Follow the proper rules for visitors and vendors coming into secure areas.
♦ Don’t talk about patients or patient information in the hallways, elevators, etc.
♦ Don’t talk about patients or patient info when away from the hospital.

Office Security:

♦ Log off from your PC when you leave your desk.
♦ If your PC has password protected screen savers, use them.
♦ Don’t print patient data to the printer and leave it at the printer.
♦ Lock up printed patient information when you are not using it or when you are away from your desk.
♦ Shred reports that contain patient information.

Computer Security Incidents

A computer security incident is any event that does impact or potentially could impact UMHHC’s ability to deliver on its mission.

Security Incident Escalation Procedures

All incidents must be reported to the Help Desk (6-8000) immediately. A Remedy ticket will be created and will be categorized as Major, Intermediate, or Minor. The Help desk is trained on how to handle each type of impact category.

Major Impact Category:

♦ Server break-in
♦ Virus attack

Intermediate Impact Category:

♦ Email spoofing, and spamming
♦ Misuse of User-ID
♦ Inappropriate use of computer resources

Minor Impact Category:

♦ Customer suspended
♦ Access report request

Contacts to Get Answers to Your Security Questions

Help Desk: 936-8000
Networking Manager: Chuck Singer, Phone: 936-5926
Operational Services Manager: Dean Carter, Phone: 763-9070
Director OTS: Joe Kryza, Phone: 936-3877
Chief Information Officer: Jocelyn DeWitt, Phone: 764-4262

Reminder:

Security and confidentiality of patient information and UMHHC assets is the responsibility of all employees, contractors, temps, and interns. Remember that patient care information is the property of the patient. UMHHC is the steward or caretaker of the information and the owner of the medium of storage.