UMHS Policy 01-04-390

Discipline for Violations of Privacy or Security of Protected Health Information (PHI),
Or Other Sensitive Information for All UMHS Workforce

Rev. 02/11/2013

What Supervisors Should Know

Privacy & Security Responsibilities

- Securing smartphones, tablets, etc. (Password protect and encrypt)
- Electronic Storage (Data at Rest) – Encryption
- Transfer of Data (Data in Transit) – Encryption, Use MiShare
- Removing Sensitive Info Off-site (In any form – paper, laptops, PDAs, flash drives, etc.)
- Telecommuting, Use the VPN (Virtual Private Network)
- Proper Use of E-mail – Must Use Outlook: “@med.umich.edu” email address (The “@umich.edu” address is NOT secure)
- Confusion between PHI, Research & Employment Data
- Understanding what constitutes proper use of electronic systems (Careweb, EWS, etc.)

Information Security Policies/Procedures

- **Portable Device Cautionary Use:** PHI should not be stored on portable electronic devices - laptop computers, USB/thumb drives, etc.; password protect & encrypt smart phones; **and** immediately report to your Supervisor or the Compliance Office if lost or stolen

- **Technical Security:** Data Encryption (all portable devices!), strong passwords, screen savers, auto log off (no shared logins!), anti-virus software, server and desktop management/support, network & firewall support, security of network file space, etc. **If you’re not sure how, ASK!**

- **Physical Security:** Physical access, ID badging, key management, vendor access, student/observer access, after hour’s access, unattended labs, locked doors/cabinets, etc.
Case Studies

Level 1 Violation: Negligent Act (Carelessness)
Sanctions for Privacy & Information Security Violations

Case Study: 1X

While at an outpatient clinic for an appointment, a patient overheard Physician A and Physician B discussing patient’s case while all were in the restroom. Patient told her mother that the two physicians “stated their surprise that the patient did not have any STDs by now.” The patient’s mother reported the incident to Patient Relations, reported to Compliance Office as a privacy violation. OCA investigation and disciplinary action resulted.

Disciplinary/Corrective Action

– Verbal Warning
– Education

Level 2 Violation: Negligent Act (Not following procedure)
Sanctions for Privacy & Information Security Violations

Physician disclosed a patient’s HIV status to patient’s son, despite patient’s request that this information not be released to the son. The patient and patient’s friend, who accompanied patient during the clinic visit, confirmed that the son exited and entered throughout the course of the physician’s consultation with the patient, thus substantiating physician’s claim that the disclosure was inadvertent.

Disciplinary/Corrective Action

– Written Warning
– Education

Level 3 Violation: Purposeful Act (Curiosity or Concern)
Sanctions for Privacy & Information Security Violations

Case Study: 3X

An employee sent flowers to the home of a patient/fellow employee, after accessing the address information in co-worker’s medical record.

Case Study: 4X

During the hospital stay of a famous “Patient Doe,” a routine audit of access revealed a two employees accessed the record – out of curiosity – about the severity of an injury, rather than with a clinical need to know.
Disciplinary/Corrective Action

- Peer Review Investigation (Physician)
- Sanctions
  
  - Medical Staff & Physician Assistant: Suspension of clinical privileges, additional privacy training, participation in an educational activity, potential report to the State Board
  - Clinical Program Trainee (Resident): Probation
  - Non-Medical Staff: Disciplinary Lay off, additional privacy training/education corrective action
  - All: Additional Education

Level 4 Violation: Purposeful Act (Blatant Misuse)
Sanctions for Privacy & Information Security Violations

Employee A and wife reconciled after wife’s affair with her lover (a UMHS patient.) Employee A agreed to the wife’s request to look at the ex-lover’s medical record. The wife and her lover later reunited, and the wife reported her husband’s inappropriate access. When confronted, Employee A (a physician) quit immediately, but resignation in lieu of investigation triggers a report to the State Licensure Board.

Disciplinary/Corrective Action

- Medical Staff & Physician Assistant: Initiate Corrective Action per Medical Staff Bylaws
- Clinical Program Trainee (Resident): Initiate Corrective Action per Medical Staff Bylaws and HOA Contract
- Non-Medical Staff: Initiate Discharge Process