Frequently Asked Questions

Disciplinary Action

1. **What are some examples of “personal gain” or “malicious intent” that constitute Level 4 violations?**

Here are some examples:

- Looking up an electronic medical record of a person before entering or upon entering a dating relationship (e.g., for any number of reasons such as confirming that the person is not married, health history, etc.)
- Looking up an electronic medical record of a spouse for use in a divorce proceeding or for other personal use in a personal relationship
- Compiling a mailing list of patient addresses for personal use or to be sold
- Accessing a supervisor’s electronic medical record to confirm a personal hunch that the supervisor is under psychiatric care
- Accessing an electronic medical record of an athlete before placing a bet on an upcoming game/athletic event

2. **Who determines what level of violation has occurred?**

After reviewing the facts of the situation and interviewing the staff member, the UMHS Compliance Office, the Human Resources Business Partner and/or Office of Clinical Affairs (OCA) will make the initial recommendation on level of violation. The Privacy Violation Review Committee will review the case and make a final determination.

3. **Can a staff member dispute the level of violation and/or the disciplinary action taken?**

Any UMHS workforce staff member may follow the procedures open to him/her under the policy and, as applicable, any U-M/UMHS human resources policies, bylaws, contract or collective bargaining agreement that pertains to the individual staff member’s employment.
4. What steps do I take if someone reports a suspected breach of PHI to me?

See the Process document regarding Discipline for Violations. The document outlines the process for reporting and investigating claims. Briefly, the Compliance Office will make the initial determination that a breach occurred and needs to be investigated. Department leadership and HR or OCA will jointly investigate the facts and prepare the case for presentation to the Privacy Violation Review Committee. The Committee will review the case and determine the Level of Violation. Department leadership and HR or OCA will determine the disciplinary action to be taken in accordance with the Policy, appropriate contract.

Compliance

Note: Frequently asked questions about HIPAA Privacy and Information Security, Accessing Electronic Medical Records, Etc. are available on the Compliance Office website. See the following FAQ links:

**HIPAA / Privacy FAQs:** [http://www.med.umich.edu/u/compliance/area/privacy/faq.htm](http://www.med.umich.edu/u/compliance/area/privacy/faq.htm)

**Accessing Electronic Medical Records FAQs:** [http://www.med.umich.edu/u/compliance/electmedrecord.htm](http://www.med.umich.edu/u/compliance/electmedrecord.htm)

5. If an employee or a patient comes to me with a privacy complaint, do I need to notify the Compliance Office?

Yes, and this has always been the requirement under HIPAA. If the complainant believes that UMHS has violated the HIPAA Privacy Rule, notify the Compliance Office immediately. Even if your department feels the complaint is something that can be handled locally, you must notify the Compliance Office at 615-4400. Centralized reporting of privacy complaints is important because:

- we have a legal responsibility under HIPAA to track privacy complaints, and the Compliance Office is required to conduct an assessment of all complaints to determine if notification to the patient is required;
- we need to ensure we handle complaints consistently;
- patients may be talking to several departments about the complaint at the same time.

6. What can happen if the HIPAA regulations are violated?

The Health System may face civil or criminal penalties. These fines were substantially increased in 2009 and are now up to a maximum of $1.5 Million per HIPAA violation per year.
Employees who knowingly misuse protected health information may also be subject to criminal prosecution, criminal fines and/or imprisonment up to ten years. The penalties for those who deliberately misuse protected health information are:

- For knowing misuse of PHI - up to 1 year imprisonment, or $50,000 fine, or both
- For obtaining PHI under false pretenses - up to 5 years imprisonment, or $100,000 fine, or both
- For using PHI for commercial advantage, personal gain, or malicious harm - up to 10 years imprisonment, or $250,000 fine, or both.