Newly Revised Policy:
UMHS Policy 01-04-390,
Disciplinary Actions for Privacy & Information Security Violations

February 2013
Privacy & Security Enforcement
HITECH Act

• Mandatory Notice of “Breach”, subject to tight time frames
  • To Individuals & U.S. HHS/OCR – All cases of “Breach”; To Media
• Enhanced State and Federal Enforcement:
  • 4 Tiers of Civil Monetary Penalties (per HIPAA violation per year): Up to $1,500,000
  • Criminal fines: $250,000/up to 10 years.
• Criminal penalties expanded to individuals
• State attorney general can file civil action
• Disciplinary action policy and enforcement required
  • Other possible reporting (e.g., State Licensure Board, National Practitioner Data Bank, etc.)
Background / Overview

• The policy was revised and approved by ECCA and the Compliance Committee in 4th Quarter 2012

• This policy combines existing Human Resources Disciplinary Guidelines with UMHS Policy 04-06-067 - Privacy Violations, Sanctions for Medical Staff Members, PAs and Clinical Program Trainees
  – The Medical Staff policy has a six year track record and is considered a fair, consistent standard process compliant with external regulations and has been adopted by other Academic Medical Centers.

• The revised policy constitutes a single policy that applies to all faculty and staff - Codifies existing HR and OCA disciplinary processes to assure consistency across the health system
Multi-Disciplinary Involvement:

• Nursing
  – Margay Britton, Laura Cherven, Marna Flaherty-Robb, Karen McConnell, Barb Wetula,
• Human Resources
  – Rich Holcomb, Margaret Hough, Kevin Newman, Stephanie Schroeder,
• Office of the General Counsel
  – David Masson
• Compliance
  – Jeanne Strickland, Lauren Shellenberger
• Office of Clinical Affairs
  – Heather Wurster
Key Policy Objectives

• Summarize consequences of privacy and information security violations
• Summarize Levels of Discipline (Levels 1 through 4)
• Identify situations that warrant assignment of a particular Level of Discipline
• Identify aggravating and mitigating circumstances and when they may or may not be applicable
• Consideration of all facts and circumstances available at time the decision is made
• Identify type(s) of disciplinary action that must be taken based on the Level of Discipline

Take-Home Message: No Supervisor/Manager solely makes decision – ALWAYS utilize HR
Investigation Process and Progressive Disciplinary Action

- Investigation of incident Documentation of investigation
- Determine level of violation
- Determine disciplinary action (appropriate within the level of violation) – consider aggravating & mitigating factors and program impact
Disciplinary Variables

- Nature of the misconduct, severity of the transgression
- Employee’s past record of disciplinary actions taken and insight
- Oral or written warning, or reprimand does NOT need to precede a Suspension/DLO
- Oral or written warning, reprimand, or Suspension/DLO does NOT need to precede a discharge
Tools and Guides

• Process Handout
• FAQ
• Discipline Grid
• Supervisor’s Tips
• Policy
• http://www.med.umich.edu/umhshr/supervisor/privacy%20violation%20policy.html
Level 1 Violation

Negligent Act - Carelessness

Workforce member unintentionally or carelessly renders PHI in any format susceptible to being overheard, accessed, used or disclosed to unauthorized individuals.

Examples:
• Failure to sign off a workstation.
• Leaving PHI in a non-secure area.
• Dictating or discussing PHI in a public area (e.g., cafeteria, elevator).
• Improper disposal
• Repeated occurrence of one or more of the above examples which was previously followed by verbal coaching.
Level 1 – Corrective Action/Discipline

- Verbal coaching
- Verbal warning with documentation
- Documentation maintained in appropriate departmental file
- HIPAA Training via MLearning
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
Workforce member acts without consideration of privacy or information security procedure or policy.

Examples:

- Failure to take reasonable precautions to prevent incidental disclosure of highly sensitive PHI (e.g., HIV status.)
- Failure to follow the minimum necessary standard (e.g., releasing more information than applicable to a work-related injury to a workers compensation carrier)
- *Additional Level 1 violation(s)*, regardless of type, which was followed by disciplinary action (prior misconduct resulting in discipline.)
Level 2 – Corrective Action/Discipline

- Written warning
- Documentation maintained in appropriate departmental file
- HIPAA Training via MLearning
Level 2 Violation: Negligent Act (Not following procedure)

Sanctions for Privacy & Information Security Violations

Case Study: 2X

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 - Deliberate act out of curiosity or concern

Workforce member intentionally accesses, reviews, or uses or discloses confidential information or systems without documented authorization to do so, due to curiosity or concern, but unrelated to personal gain or malicious intent.

Examples:

• Sharing ID/password with another coworker or using another person's ID/password.

• Accessing and reviewing the medical record of a patient without written authorization solely out of curiosity or concern, but with no malicious intent and/or not for personal gain.

• Additional Level 1 and/or Level 2 violation(s), regardless of type, which was followed by disciplinary action (prior misconduct resulting in discipline.)
Level 3 – Corrective Action/Discipline

• Suspension / Probation / Disciplinary Lay Off (DLO) in accordance with any applicable Bylaws, Collective Bargaining Agreement, etc.

• HIPAA Training via Mlearning (except in the case of discharge)
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 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 / Gross Negligence
Workforce member accesses, reviews, or discloses confidential information or fails to comply with information security safeguards that result in loss of availability, integrity, and confidentiality of systems and/or damage to the health system’s reputation, or uses the data for personal gain or with malicious intent.

Examples:
- Accessing or allowing access to patient record without legitimate reason for personal gain or malicious intent.
- Tampering with or unauthorized destruction or disposal of PHI.
- Additional Level 3 violation(s), regardless of type, which was followed by disciplinary action (prior misconduct resulting in discipline.)
Level 4 – Corrective Action/Discipline

- Discharge/Termination/Corrective Action in accordance with applicable Bylaws, Collective Bargaining Agreements, with reporting to appropriate agencies, as applicable (e.g., licensure board, national practitioner databank, etc.)
Level 4 Violation: Purposeful Act (Blatant Misuse)
Sanctions for Privacy & Information Security Violations

Case Study: 5X

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
Aggravating/Mitigating Factors

• Consider aggravating or mitigating factors to determine the appropriate disciplinary action within the disciplinary action range of the applicable level violation.

• Exception: Mitigating factors are not relevant in determining the disciplinary action when it is determined that a workforce member has accessed, used and/or disclosed a patient’s electronic medical record with malicious intent and/or for personal gain.
• Target Effective Date: March 15, 2013
• Education Rollout between now and March 15, 2013, spear-headed by Human Resources with involvement from Nursing, OCA, and Compliance
Extenuating Circumstances?  Perhaps...

• Investigations can reveal:
  – Illness causing judgment errors
  – Power of Attorney rescinded, so permission to access can become permission denied
  – Etc.
• Each case is fact-specific, unique

HR and/or OCA investigates each case forwarded by Compliance or other sources to determine the validity of the alleged violation, type of violation, and associated consequences, if applicable.

Take-Home Message: No Supervisor/Manager solely makes decision – ALWAYS utilize HR
References

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:
http://www.med.umich.edu/i/policies/umh/01-04-390.htm

Human Resources Website Information:
http://www.med.umich.edu/umhshr/supervisor/privacy%20violation%20policy.html

UMHS Compliance Office – HIPAA FAQs:
http://www.med.umich.edu/u/compliance/area/privacy/faq.htm

Direct privacy-related questions to:
HIPAA-Questions@med.umich.edu or call Compliance Office 615-4400
Next Steps/Roll out

**HR Business Unit Managers, Consultants and Generalists** – These groups have been educated on the Policy, but training will continue through March 2013, including reviewing and discussing cases that arise and the pertinent issues, to ensure as thorough an understanding of the Levels of Violations and Disciplinary Action as possible.

**Leadership Groups** - Presentations will be made to various groups in February and March. During those presentations, we will ask that each Director, Manager, Chair, etc. share the information (via HR Documents including Disciplinary Grid, Power Point Presentation, FAQs, and Process document) with their respective leadership groups in order to push the information down into the organization. (Within HR, appropriate HR professional will help coordinate and participate in those presentations so as to establish the correct protocol and to be the primary educator on the policy. This will likely be more intensive for those business units with direct patient care responsibilities.)

**Global User messages** - During February and March 2013. HR and PRMC working on the messages. This will help to educate all UMHS staff and make them aware that things have gone to a higher level of scrutiny relative to HIPAA violations.
Questions?