UNIVERSITY OF MIAMI MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE UNIVERSITY OF MIAMI

Issue 4, Sept. 2007

HIPAA HAPPENINGS

The Newsletter of the Office of HIPAA Privacy and Security (OHPS)

Message from Director

In July, the Office of HIPAA Privacy and Security launched its new website. It was designed with you—our users in mind. We are very appreciative of the positive feedback and wonderful suggestions that have been made. We continue to tweak the site and add new and helpful information to assist you in your efforts.

We encourage you to use our website as a resource for your HIPAA needs. If you need assistance or have any suggestions, please email us.

Thank you for your continued efforts in support of HIPAA compliance.

Respecting Patient Privacy, Building Patient Trust!

Sharon A. Budman, M.S. Ed., CIPP
Director/Ombudsman, Office of HIPAA Privacy and Security

What's Inside?

- **Message from the Director**
- **Business Associates**
- **Important Tips on Access Codes**
- **Employee Access to Medical Records**
- **Right to Revoke**
- **Disability Authorization**
- **Random Audits**
- **Frequently Asked Question of the Month**

Important Tips on Access Codes

- Never share your username and passwords with anyone as you are responsible for all entries and actions made with your username.
- Never log in for others.
- Never log in and leave the computer unattended.
- Never use anyone else's username and password.
- Do not write down your password and leave it under the mouse or keyboard where others can access it.

DID YOU KNOW?

All employees are required to take the Core HIPAA Courses — Privacy & Security Awareness through ULearn.

PHI FLOWS

The Office of HIPAA Privacy and Security is reviewing and updating our PHI Flows and questionnaires. This is required by the Federal HIPAA Privacy Regulation. Please assist us and complete your questionnaire when received.

Business Associates

A business associate is an outside party that receives protected health information from the University or from another business associate of the University, in connection with accounting, accreditation, actuarial, administrative, consulting, data aggregation, management, financial or legal services to or for the University; or uses or discloses protected health information in connection with the performance of a function or activity on behalf of the University. They are not part of the University's workforce. A Business Associate contract is required before the University can share it's Protected Health Information with any outside party/vendor. Please visit our website to complete the business associate form so that we may confirm the need for a Business Associate contract and begin the process if necessary.

Employee Access to Medical Records

As employees, we are charged with a task to perform and must do so within the realm of our positions. However, when we, as employees, are patients at the medical center, we must follow the same policies as all of the other patients who are treated here. Therefore, as a patient, we must go through the prescribed process for accessing and obtaining our medical records. An Attachment 19 must be completed and given to either the medical records custodian of the department where the services were rendered or, you may contact the Office of HIPAA Privacy and Security and we will facilitate the request for you.

Employees are not permitted to access their own medical records, in any form, paper or electronic, or those of their co-workers or family members. This is a violation of the University's Minimum Necessary HIPAA Policy.

Right to Revoke

The Privacy Rule gives individuals the right to revoke, at any time, an Authorization they have given. The revocation must be in writing, and is not effective until the covered entity receives it. The Privacy Rule requires the Authorization to clearly state the individual's right to revoke; and the process for revocation must be stated clearly in the Authorization itself. The University's Attachment 46—Authorization for Third Party Disclosure form provides a description of the revocation process. If an individual revokes an authorization, he/she must send a letter in writing to the Privacy Officer requesting the revocation.

Disability Authorizations

Disability authorizations related to disability cases fall outside of the HIPAA regulation and do not require HIPAA compliant authorizations. However, the law requires that we Account for the Disclosure of this information. Therefore, the policy is for the department to complete an Attachment 45, Accounting for Disclosure, and send it along with the original authorization (documentation) to the Office of HIPAA Privacy and Security for scanning into the central repository. We encourage you to keep a copy of these documents in the patient's file. For assistance, call our office.

Random Audits

The Office of HIPAA Privacy and Security conducts random document audits of HIPAA related documents completed by employees throughout the University. These documents are audited for proper completion, inclusion in the central scanning repository, supporting documentation when applicable, and appropriateness of use. The purpose of the document audits is to ensure compliance with the University's HIPAA policies and procedures and determine areas of deficiency that require remediation. The OHPS is responsible for the implementation of, and compliance with, the federally mandated HIPAA Privacy and Security regulations for the University of Miami Miller School of Medicine.

If a patient believes that his/her privacy rights have been violated, please transfer the call to our office 305-243-5000, or provide our contact information to the patient.

Frequently Asked Question of the Month

Question: May a health care provider disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (**HEDIS**)?

Answer: Yes. The HIPAA Privacy Rule permits a provider to disclose health information to a health plan for the quality related health care operations of the health plan, provided that the health plan has or had a relationship with the individual who is subject of the information, and the protected health information requested pertains to the relationship. See 45 CFR 164.506(c)(4). Thus, a provider may disclose protected health information to a health plan for the plan's Health Plan Employer Data and Information Set (HEDIS) purposes, so long as the period for which information is needed overlaps with the period for which the individual is or was enrolled in the health plan.

For access to the latest forms and HIPAA information, please visit the Office of HIPAA Privacy and Security website at http://www.med.miami.edu/hipaa or contact the Office of HIPAA Privacy & Security at: Phone: 305-243-5000 Fax: 305-243-7487 Location: PAC Building, Room #409 Locator Code: (M-879)