UNIVERSITY OF MIAMI MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE UNIVERSITY OF MIAMI

Issue 3, June 2007

HIPAA HAPPENINGS

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

Message from Director

As patients become more knowledgeable and HIPAA savvy, they will begin to exercise their rights on a more frequent basis. We are beginning to experience this trend. It is important that, as employees, we understand and follow our University of Miami HIPAA Privacy and Security Policies. These policies serve as our guide and answer questions related to the appropriate process to follow.

The following patient rights requests must always be processed by the Office of HIPAA Privacy and Security: Request for Amendment of Health Information (Attachment 33), Request for Restrictions on Use and Disclose of Health Information (Attachment 6), Request for Communications at Alternative Locations or by Alternative Means (Attachment 13). The forms to exercise these rights are located on our website and should be provided to our patients ONLY upon request.

For example, if a patient indicates there is an error in his/her medical record that needs correction, the patient should be provided an Attachment 33, Request for Amendment of Health Information Form. The patient should be instructed to send the form to the Office of HIPAA Privacy and Security. By law, the institution must respond to these request within a 30 day period. If your department receives a request, please send it to the OHPS as soon it is received. If you need assistance, please call the OHPS at 305-243-5000. For more information, please refer to the University's HIPAA Policy for Patient Amendment of Designated Record Sets.

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?

Workers Compensation

Subpoenas and authorizations received related to workers compensation cases fall outside of the HIPAA regulation and do not need to be HIPAA compliant . However, the law requires the institution to account for the disclosure pursuant to Workers Compensation. Therefore, the policy is for the department to complete an Attachment 45, Accounting for Disclosure and send it along with the original subpoena (documentation) to the Office of HIPAA Privacy and Security for scanning into the central repository. For more information, please refer to University Policy for Accounting for Disclosure.

DID YOU KNOW?

All subpoenas need to be served in person by a process server? The University does not accept mailed or fax subpoenas for release of patient information.

Non UM Third Party Authorization Forms

If an authorization is received from an outside entity/attorney, please refer and use the Third Party Disclosure Quick Reference Guide to make certain the authorization is HIPAA compliant before processing the request. If the authorization is HIPAA compliant, write Attachment 46 and the patient's IDX number at the top of the form and send it to the OHPS for scanning. If the authorization is not HIPAA compliant, provide the patient or attorney's office with an Attachment 46. No records may be released on non-compliant authorizations. If you are unsure whether the authorization is compliant, please call the OHPS by phone at 305-243-5000 and/or fax it to us at 305-243-7487 and we will assist you.

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. When we as employees take on the role of a patient, we must follow the same policies as all of the other patients of the medical center. 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 the office will facilitate the request for you.

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

Frequently Asked Question of the Month

Question: May physicians offices use patient sign-in sheets or call out the names of their patients in the waiting rooms?

Answer: Yes. Covered entities, such as physician's offices, may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The HIPAA Privacy Rule explicitly permits the incidental disclosures that may result from this practice, for example, when other patients in a waiting room hear the identity of the person whose name is called, or see other patient names on a sign-in sheet. However, these incidental disclosures are permitted only when the covered entity has implemented reasonable safeguards and the minimum necessary standard, where appropriate. For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem for which the patient is seeing the physician). See 45 CFR 164.502(a)(1)(iii).

Physicians—Fees for Copying Medical Records

When patients request copies of their medical records, the Privacy Rule permits the covered entity to impose reasonable, cost-based fees. Per our University Policy and state law, the Departmental Records Custodian or OHPS shall charge no more than the reasonable cost of reproducing the records and shall not be more than:

- $1.00 per page for the first 25 pages and $0.25 per page for each page in excess of 25 pages for written or typed document or reports.
- For requested charts, records and reports that relate to a workers' compensation injury, the charge may not exceed $0.50 per page or the actual direct cost for x-rays, microfilm, and other non-paper records.
- The patient must be informed in advance of the fees associated with copying of the requested information.

For more information, please refer to the University's Policy on Patient Access to Designated Record Sets.

If a patient has any questions or concerns about the privacy and security of his/her health information, the patient may contact us directly at **305-243-5000**, or email us at **hipaaprivacy@med.miami.edu**

DID YOU KNOW?

Did you know that only the Office of HIPAA Privacy and Security is authorized to respond to Attachments or process 6, 13, and 33? No departmental personnel are permitted to respond to these documents. If you need assistance please call the OHPS.

System Privileges

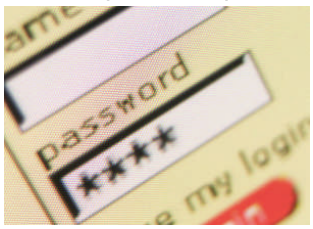
University of Miami workforce members must be mindful of their responsibilities when given access to University information systems. Using such access to look up family members, friends, celebrities and other employees without a genuine, job-related need is an abuse of such privilege and may subject the individual to sanctions, up to and including termination. In particular, the HIPAA federal law protects the privacy and security of patients' health data. University of Miami medical school employees sign HIPAA confidentiality statements and are governed by both University HIPAA policies as well as University information system policies. These policies apply to all workforce members regardless of tenure or rank.

Securing your Desktop

Locking your computer is one of the simplest ways to prevent unauthorized access to the data. When a computer is locked, no one can access your computer or the network through your user account unless they know your password. The Microsoft Windows 2000/XP/VISTA operating systems provide a simple way for users to lock their computers: Type **CTRL+ALT+DEL** and click "**Lock Computer.**" To unlock your computer press **CTRL+ALT+DEL**, type in your password and click "**OK.**" Please remember to lock your computers, even if you are stepping away for only a few minutes; a few minutes is enough time for someone to compromise your data. Please also remember to logoff your computers before leaving for the day.

Passwords

Our systems require the use of usernames and passwords to access the various applications across our campus. Your password is unique to you and should be kept secret. Avoid using familiar names or personal information as your password. Passwords should not be written down and left where they are easily accessible. Do not attach them to your computer screen or leave them under your keyboard where anyone may be able to access them. Never give your password to anyone. If you do, keep in mind that you will be held responsible for any actions taken while your username and password were being used. If you suspect your password has been compromised, please change it immediately.



PHI on Portable Devices

Avoid storing any PHI on laptops or other portable devices such as PDA's or flash drives unless absolutely necessary or you have been granted approval. Consider utilizing suitable safeguards such as encryption.

If such a device is lost, please report it immediately to the department of Security at 305-243-6000 and the Office of HIPAA Privacy and Security at 305-243-5000.

If you have any questions or concerns please call the OHPS at 305-243-5000 or email us at hipaaprivacy@med.miami.edu

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