UNIVERSITY OF MIAMI
MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE
UNIVERSITY OF MIAMI

Issue 5, Jan. 2008

HIPAA HAPPENINGS

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

Message from the Interim Chief Privacy Officer

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.

We encourage you to use our website as a resource for your HIPAA needs and privacy best practices. If you need additional assistance or have any suggestions, please email us. As always, feel free to call us with your questions, we are here for you.

Thank you for your continued efforts in support of HIPAA and safeguarding our sensitive information.

Respecting Patient Privacy, Building Patient Trust!

Sharon A. Budman, M.S. Ed., CIPP

What's Inside?

Moving Medical Records

Whenever medical records are being moved from one location to another, special precautions should be undertaken to protect these sensitive records during the move. Below are some recommendations for safeguarding records during a move.

- Medical records should not be left in an unlocked room or insecure area.
- All boxes containing medical records should be appropriately labeled.
- Know the contents of the boxes and number them.
- An appropriate administrative individual should supervise all aspects of the move.
- Ensure that the movers are aware of exactly what needs to be moved and proper handling instructions
- Upon completion of the move, immediately make certain all items are accounted for and safeguarded appropriately.

Records removal:

- Medical records should not be taken from appropriately secured medical records areas without proper authorization.
- Records moving between facilities must be properly secured and never left in vehicles.

It is the department's responsibility to safeguard the records whether in the records room or during a move. They are University assets and must be protected.

Should your area ever experience a loss of medical records, immediately report the loss to the Departmental Administrator, the Security office 305-243-6280, and the Office of HIPAA Privacy and Security 305-243-5000.

New CBL Coming Soon!!

Staff members who are responsible for the processing of any HIPAA forms will be required to take the New Forms Training Module that will be available through ULearn. Notification will sent when the CBL is operational.

Request for Amendment of Medical Record

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. However, if it is received by the department, please send it to the OHPS as soon as it is received. By Policy and the regulation, the institution must respond to these request within a 30 day period. All requests are processed by the OHPS. If you need assistance, please call our office at 305-243-5000. For more information, please refer to the University's HIPAA Policy for Patient Amendment of Designated Record Sets.

HIPAA Compliant Authorization—What is it?

An "authorization" is required by the Privacy Rule for uses and disclosures of protected health information. When the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information. An authorization is a detailed document that gives covered entities permission to use PHI for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual. HIPAA compliant authorizations must contain all 9 elements as outlined in the regulation. When you receive an authorization from an outside party, it must contain these elements. Please use our Checklist tool to verify the authorization is HIPAA Compliant. If it is not, you must sent them our HIPAA compliant authorization form for completion.

Important Email Security Tip

It is not acceptable to include PHI in regular email. Emails may be forwarded (accidentally or deliberately) to unauthorized recipients inside and outside the organization. Some form of protection (encryption, password-protected attachment etc) should be employed if PHI is to be included in email. As always, the Minimum Necessary policy applies and dictates that only the minimum amount necessary to accomplish the purpose should be included..

See transmission policy and the minimum necessary policy.

Random Audits

The Office of HIPAA Privacy and Security conducts random document audits of HIPAA documents completed by employees throughout the University. The purpose of these audits is to validate compliance with our HIPAA policies and procedures and determine areas of deficiency that require remediation. Such areas include: improper use of documents and processing of incomplete documents. You may receive a phone call from an OHPS representative requiring you to come for a one on one training session. These sessions are required for those individuals whose submitted documents that are found to be non-compliant. The OHPS is responsible for monitoring of 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, immediately transfer the call or refer the patient to the OHPS by calling (305)243-5000.

Must an Authorization include an expiration date?

The Privacy Rule requires that an Authorization contain either an expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. For example, an Authorization may expire "one year from the date the Authorization is signed." An Authorization remains valid until its expiration date or event, unless effectively revoked in writing by the individual before that date or event. All authorization forms must be dated by the patient.

Frequently Asked Question

Question: Does the HIPAA Privacy Rule permit doctors, nurses, and other health care providers to share patient health information for treatment purposes without the patient authorization?

Answer: Yes. The Privacy Rule allows doctors, nurses, hospitals, laboratory technicians, and other health care providers that are involved in the care of the patient to use or disclose protected health information, such as X-rays, laboratory and pathology reports, diagnoses, and other medical information for treatment purposes without the patient's authorization. This includes sharing the information to consult with other providers, to treat a different patient, or to refer the patient. See treatment activities policy.

To access the latest forms and HIPAA information, please refer to 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