UNIVERSITY OF MIAMI
MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE
UNIVERSITY OF MIAMI

Issue 7, August 2008

PRIVACY & DATA PROTECTION UPDATE

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

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

What's Inside?

Protection of Sensitive Information

Sensitive information on paper is the same as sensitive information on a computer. Both need to be protected from unauthorized access and should be treated with caution and discretion. In particular, protected health information (PHI) in all forms is covered by the HIPAA regulations. Sometimes, it may be necessary to print out sensitive electronic information on paper and make copies. Do not leave these copies lying around in open areas within your workspace as this information may be seen or even taken by unauthorized parties. If you would not want someone to read that information on your computer, you probably would not want them to read the same information on paper.

Keep printouts of sensitive information such as medical records in a secure location, such as a locked desk, locked filing cabinet or a safe. Avoid leaving sensitive documents unattended, especially in high traffic areas. Medical record areas are to be secured and limited to authorized personnel.

Always shred copies of sensitive information when disposing - do not simply toss them in the trash. Cross-cut shredders are very useful in making printed sensitive information both unreadable and unusable. Remember to shred any printouts containing any information that would be useful to identity thieves, an ever-increasing problem. This includes documents containing any personal, financial or protected health information.

The University Of Miami School Of Medicine has a contract to provide centralized shredding services. These services are available to all School of Medicine departments. For more information, please contact Frances Kaniewski in Environmental Services by email at fkaniews@med.miami.edu.

HIPAA Privacy & Security Training

The federally mandated HIPAA Privacy Regulation and Security Rule require the University of Miami to implement administrative, technical and physical safeguards to ensure the confidentiality, integrity, and availability of protected health information and protect it against any reasonably anticipated threats or hazards, and/or unauthorized uses or disclosures. It also requires that all workforce members complete the mandatory awareness training classes. The mandatory training classes are available via the ULearn http://ulearn.miami.edu/ application under the Compliance category listed as HIPAA. For assistance with ULearn, please contact PDTO at 305-243-3090.

Complaints

When employees receive medical care at UM Health Systems they become patients and are afforded the same privacy and confidentiality of their health information. If you have any questions concerning the privacy and confidentiality of your health information at the University of Miami or suspect that your records have been inappropriately accessed, please contact our office at 305-243-5000. All complaints maybe made anonymously. Please see the Patient Resources section of our site for more information concerning your rights as a patient.

Identity Theft

Identity theft is a crime where personally identifiable information such as name, Social Security number, date of birth, credit card number, health insurance number, etc. is acquired — usually stolen — and used without authorization to commit fraud or other crimes. These crimes may include using the stolen information to purchase items on credit, obtain a mortgage, gain access to restricted data, file fraudulent health claims, or to establish services such as credit cards. While some identity theft victims can quickly resolve their problems, others may need to spend significant time repairing damage to their good name and credit record. Victims of identity theft may lose out on job opportunities or be denied loans for education, housing, or cars due to negative information on their credit reports. Some may even be arrested for crimes they did not commit. To read more on ID theft including steps to protect yourself and the institution please visit http://www.med.miami.edu/hipaa/public/x357.xml.

IMPORTANT INFORMATION

Computers, laptops, and other hardware must be disposed of appropriately to prevent unauthorized access and retrieval of any sensitive date stored on the device. Simply deleting files and emptying the recycle bin does not completely erase the data. Please contact Medical IT for additional information on disposal.

The HIPAA office provides one-on-one and small group training specifically related to release of information (by subpoena) and other related topics. To schedule your staff, please contact our office by calling 305-243-5000.

Frequently Asked Question

Question: Are we required to obtain a copy of a drivers license or other identification when record request is faxed or mailed?

Answer: No...If an Attachment 46 - Authorization for Third Party Disclosure or an Attachment 19 - Access to Health Information is received by fax or mail for release of records, we must verify the signature on the document by checking against signature documents on file or via other reasonable means such as a drivers license. Once records are released, any copies of drivers licenses or identification containing sensitive information should be shredded.

For additional information, please contact OHPS at 305-243-5000.

Authorization for Third Party Disclosures

If a patient is requesting his/her medical record to be released to a Third Party, an Attachment 46 - Authorization for Third Party Disclosure should be provided to the patient for completion. Once records are released, the original Attachment 46 should be sent to the Office of HIPAA Privacy and Security (OHPS) for scanning.

If an authorization is received from an outside entity/attorney, please consult 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 for assistance.

All staff responsible for the release of records should take the CBL available on the ULearn system that discusses HIPAA Subpoena Attorney Requests and Other Third Party Disclosures.

ANY QUESTIONS

Submit to
hipaaprivacy@med.miami.edu

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