UNIVERSITY OF MIAMI
MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE
UNIVERSITY OF MIAMI

Issue 6, Apr. 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?

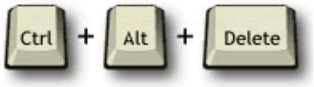
University of Miami Health System Notice of Privacy Practices

We have updated the Notice of Privacy Practices to reflect this name change. It is important that you order updated Notices and begin using them immediately. The Notices are NOW available through our University Vendor – Printfarm. Orders must be placed online through the following web link www.printfarm.com/um. If you have any questions regarding the process, delivery, or need to speak with someone regarding your order, please contact Lesley @ Printfarm @ (305)592-2895. You may also access the link from our website forms section. Printfarm has assured us that the Notices are available and are ready for delivery as soon as the orders are placed.

All other processes regarding to the distribution of the Notices, obtaining the Acknowledgement of Receipt, and sending these to the Office of HIPAA Privacy and Security for scanning remain the same. The Notice is to be provided to all new patients who are seen at any of our sites of service for the first time.

If you have any questions regarding the Notice, please contact the Office of HIPAA Privacy and Security at (305)243-5000 or visit our website for the latest updates, policies, newsletters, Security Awareness Tips, and training.

CTL + ALT +Delete
When you're out of your seat!



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.

Laptop Security
Do you know where your laptop is?

It is easy to misplace a laptop and thieves often target laptops for the data they may contain. It is important to know where your laptop is at all times. If possible, avoid storing sensitive data on your laptop. If you must store such data, or your laptop can be used to access sensitive data on university systems, then it is your responsibility to adequately safeguard your laptop.

Avoid leaving your laptop unattended. Do not walk away from it in an airport or restaurant. If you must leave your laptop, be sure that it is secure in a locked desk drawer or cabinet, locked trunk or that it is secured via a cable to an immobile object. Backup any data on your laptop frequently to a network drive or other secure storage media. Secure access to your laptop's data behind a username and strong password and/or biometric device such as a finger print scanner. Use an encryption mechanism for particularly sensitive data. Consult your IT group for further details.

Release of records for purposes of a malpractice action

When releasing records for purposes of a malpractice action, you will know this because the document will cite Florida Statue 766.204 or required the response within 10 business days. Please make sure this request is complied with **immediately**. The requested records need to be provided to the attorney within 10 business days per Florida Statute. Usually the request comes in the form of an Authorization with an attorney letter.

Verify to make certain the authorization is HIPAA compliant. Please refer and use the Authorization Quick Reference Guide to check for compliance. If the authorization is not HIPAA compliant, an Attachment 46—Third Party Authorization form should immediately be sent to the attorney for completion. Contact us for a sample letter. We must comply within 10 days, if we do not, we waived certain defenses should this matter go to litigation which could result in detrimental consequences for the University. If you have questions or concerns, please contact our office by calling (305)243-5000.

Workers Compensation Subpoenas

Workers Compensation is an exception under the HIPAA Privacy Regulation. Therefore subpoenas for records for a Workers Compensation case are not required to be HIPAA compliant. Subpoenas for Workers Compensation cases do not require either a Qualified Protective Order or Documentation of Notice to the Patient with Non-Objection Certification. They do have to be served in person by a process server. **Additionally the area releasing the records is required to complete an Attachment 45**. 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 & Security for scanning into the central repository. For more information, please refer to University Policy for Accounting for Disclosure.

Subpoena received for Deposition

All subpoenas are required to be HIPAA compliant before any protected health information is released even when the subpoena is for a deposition. For example, when a physician is subpoenaed to give a deposition or to testify at a trial, the subpoena must be HIPAA compliant before the physician may disclose protected health information, whether verbally, in writing, or electronically. If physician is ordered by subpoena or court order to give a deposition or to testify at trial, the physician should contact Risk Management at (305)243-1400 for advice, whether or not the University of Miami is party to the case. Please refer and use the Subpoena Quick Reference Guide to make certain the subpoena is HIPAA compliant before proceeding with the release. ***Remember***: By law and policy, we are required to Account for Disclosure using Attachment 45.

Mandatory Employee Privacy & Security Training

All new employees receive mandatory HIPAA training through New Employee Orientation via the ULearn system. Additional training should be provided by the department liaison specifically to their job function. Any employees who has not yet had HIPAA training, should log into the ULearn system and take the training.

Those employees handling subpoenas and Third Party authorizations should also take the Subpoena CBL, also available on ULearn. The training may be accessed through the ULearn system: http://ulearn.miami.edu/

Quick Tip

Please remember that all privacy forms that are bar coded must be sent to the Office of HIPAA Privacy & Security for scanning into the central repository. HIPAA forms should not be copied on colored paper. All original forms should be provided and a copy should be kept in the medical records.

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