UNIVERSITY OF MIAMI
MILLER SCHOOL OF MEDICINE

Respecting Patient Privacy, Building Patient Trust!

MILLER SCHOOL OF MEDICINE
UNIVERSITY OF MIAMI

Issue 8, Jan. 2009

PRIVACY & DATA PROTECTION UPDATE

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

UHealth
UNIVERSITY OF MIAMI HEALTH SYSTEM

What's Inside?

Need to Know: Access

Do not access patient information without the need to know.

Updated Forms for UHealth System

All HIPAA-related forms have been updated and are available for download from the Office of HIPAA Privacy & Security website. They now have the UHealth logo as well as time and date stamps, which were added based on a Joint Commission requirement. For example, on the Consent for Treatment form, these fields were added to the lower right corner to comply with the requirement. The addition of this information is required for clinical areas that are hospital-based practices. It is important to begin using these updated forms immediately. These forms must be used in their original format. Photocopying distorts the bar code used for scanning. All forms may be ordered from our printer, Print Farm, at discounted rates. The link is also available in the forms section of our website and through the UM e-Net system.

The Office of HIPAA Privacy & Security audits the completion of the documents for HIPAA compliance purposes. For additional training on our forms, or any other questions about our forms, please contact us at 305-243-5000 or email hipaaprivacy@med.miami.edu.

Release of Psychotherapy Notes

According to Florida law, psychotherapy notes may only be released pursuant to a legally-sufficient written authorization signed by the patient that specifically authorizes the release of mental health information. Additionally, the release of the mental health information must be authorized by the provider. If, in the provider's professional judgment, the release of such information can cause harm to the patient, the provider may decide not to release. An authorization for such release is only valid when not combined with a request for other information.

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

Release of Information based on a Non-Health Care Power of Attorney

A Non-Health Care Power of Attorney does not provide authorization for a personal representative to access health information. A power of attorney that does not include decisions related to health care in its scope, does not authorize the holder to exercise the patient's right under the HIPAA Privacy Rule. A medical or health care power of attorney would be needed or an Attachment 46-Authorization for Third Party Disclosure form, authorizing the information be shared with that third party.

Decedents:
With respect to personal representatives of deceased individuals, the Privacy Rule requires the hospital to treat the personal representative as the individual so long as the person has the authority under law to act for the decedent or the estate. The power of attorney would have to be valid after the individual's death to qualify the holder as the personal representative of the decedent.

HIPAA Security Guide

Staff members who are involved with or administer systems that store and/or transmit electronic protected health information (EPHI) and make EPHI accessible to multiple people are required to take the Security Training Module. It is available through ULearn under learning activities. For assistance with ULearn, please contact PDTO at 305-243-3090.

Law Enforcement & Investigations

Should your department receive an inquiry regarding patient information from law enforcement, including the FBI, or any other government agency, inquiring about our patient information, please notify the Office of HIPAA Privacy & Security and refer them directly to our office. All such inquiries must be received in writing on official letterhead and must be accounted for in accordance with our HIPAA policies and federal law.

We provide one-on-one and small group training specifically related to release of information and other related topics. To schedule your staff, please contact our office by calling 305-243-5000.

Submit to
hipaaprivacy@med.miami.edu

Wireless Access

As high-speed wireless networks become more common, unsuspecting users are giving hackers effortless access to their wireless-enabled laptops, PDAs, smart phones, and the information on these devices. People who think they are signing onto the Internet through a legitimate, wireless hotspot *might actually be connecting to a look-alike network*, created by a malicious user who can steal sensitive information, such as your username and password.

The risk is particularly high at coffee shops, hotels, airports and other places with a high turnover of laptop users. Many malicious individuals are setting up laptops to act as wireless access points with legitimate-sounding names such as “Hilton”, “Free Wireless Access”, “Airport Wireless” etc.

Wireless access for your laptop is definitely convenient and easy, but you must take precautions to ensure you do not compromise the confidentiality of any sensitive data stored or transmitted on or to your device.
Here are some recommended guidelines for use of public wireless access points:

- Turn off your wireless connection when you’re not using it. It also conserves device power!
- Don’t use the defaults. Change default names of your network to a unique name and change any default passwords.
- Connect only to infrastructure points, or official access points, rather than peer-to-peer connections or another user’s computer.
- Avoid banking and other sensitive transactions via untrusted wireless networks.
- Don’t share your files. Turn off sharing before using a public wireless network.
- Keep your software up-to-date. Make sure your browser, operating system, antivirus, anti-spyware, and firewalls have the latest patches.
- Determine from a trusted source that you are using the approved wireless network for the location you are at.

Contact your IT support group for specific assistance with your wireless device and for secure means of accessing University systems and other protective software and practices.

Frequently Asked Question

Question: How can we determine if a vendor is a Business Associate? What is the process?

Answer: Access the OHPS website and click on Business Associates. Read the information provided and complete the form if appropriate. You must click the “submit” button at the end. Fax the consulting agreement to us at 305-243-7487 or email us at hipaaprivacy@med.miami.edu. We will make a determination and send the agreement to the vendor if applicable.

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