Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

April 2009 - Issue 9

What's Inside?

Mandatory Compliance Initiative

On April 7, 2009, all faculty, staff, and temporary employees received a communication requiring them to complete the *HIPAA Privacy and Security Awareness Training* CBL in the ULearn system as well as acknowledge the *HIPAA Confidentiality Agreement* and the *Confidentiality and Computer Use Agreement* in the myUM system. The deadline for completion of these items associated with the mandate is May 4, 2009. If you have not done so already, please complete these tasks as soon as possible. For more information, visit the Frequently Asked Questions (FAQs) section of our website.

Related Links

- **ULearn:** http://ulearn.miami.edu
- **myUM:** http://myum.miami.edu
- **Mandatory Compliance Initiative FAQs:** http://www.med.miami.edu/hipaa/public/x426.xml

Leaving Messages for Patients

The Privacy Rule "does not prohibit covered entities from leaving messages for patients on their answering machines or with an individual who answers the phone." However, in order to "reasonably safeguard" the patient's privacy, we should take care to "limit the amount of information disclosed … to the minimum necessary." Leaving your name, place you are calling from (University of Miami), and a number, along with other information necessary to confirm an appointment such as office hours or simply leave a message asking the individual to call back is appropriate.

Related Links

- **More information about phone messages:** http://www.med.miami.edu/hipaa/public/x411.xml
- **Minimum Necessary:** http://www.med.miami.edu/hipaa/public/x409.xml

Photo Authorization

An authorization is required by the Privacy Rule for uses and disclosures of protected health information which includes photos or videos. The patient would need to complete an *Authorization/Release for Photography or Audio/Video Recordings* and an *Attachment 46 – Authorization for Third Party Disclosure* to authorize the University to use photographs and video recordings. Employees should not use camera phones to take photos of patients or other sensitive information.

Related Links

- **More information about patient photos:** http://www.med.miami.edu/hipaa/public/x420.xml
- **Photo Authorization Form:** https://www.med.miami.edu/hipaa/private/documents/D3900055E.pdf
- **Attachment 46 - Authorization for 3rd Party Disclosure:** https://www.med.miami.edu/hipaa/private/documents/D3900052E.pdf

Frequently Asked Questions

Q: May healthcare providers place medical charts on exam room doors?

A: Yes, with reasonable and appropriate privacy measures.

Learn more and see examples at http://www.med.miami.edu/hipaa/public/x421.xml

Important Tip

Use only your University email to conduct official business. Never use outside email accounts or instant messaging to send PHI or other sensitive information.

If PHI **must** be sent via email, start your subject line with *[secure]* to encrypt the message. Med IT has posted complete email encryption instructions at http://it.med.miami.edu/documents/EncryptedEmailInstructions.pdf

Have a Question?

hipaaprivacy@med.miami.edu

Prior newsletters available online
http://www.med.miami.edu/hipaa

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487

University of Miami Registered Agent Policy

University of Miami employees, faculty, and students are not allowed to accept service of process of legal documents such as summons, lawsuits, subpoenas, and notice of depositions on behalf of the University. All process servers serving the University must be directed to serve the University's Registered Agent.

This is the only office at the University authorized to accept service of process of legal documents on behalf of the University. The Office of General Counsel will review the documents for compliance with the appropriate legal and regulatory framework (including HIPAA) and work with the appropriate business units to gather any additional documents/ information required.

Registered Agent
333 Max Orovitz Building
1507 Levante Avenue
Coral Gables, FL 33146

Please refer to the policy that will streamline requests for information directed to the University. The policy sets forth specific procedures that University employees must follow regarding the receipt or service of legal documents. Any questions regarding the policy should be directed to the Office of General Counsel at 305-284-2700.

Related Links

- **Registered Agent Policy:** http://www.miami.edu/policies_procedures/General-Business/PDF-Policies/BSF-080.pdf

What you *need to know* about Medical Identity Theft

Medical identity theft is a criminal act that occurs when a person uses someone else's personal information, such as name and insurance card number, without that individual's knowledge to obtain or make false claims for medical services or goods. Unlike financial identity theft, medical identity theft can harm its victims by creating false entries in their medical records at hospitals, doctors' offices, insurance companies, and pharmacies. These false changes made to victims' medical files and histories can remain on record for years without discovery or correction.

Related Links

- **More information about Medical Identity Theft:** http://www.med.miami.edu/hipaa/public/x358.xml
- **Financial Identity Theft:** http://www.med.miami.edu/hipaa/public/x352.xml

SECURITY NEWS

VA Pays $20 Million to Settle Lawsuit over Data Loss

The Veterans Administration will pay $20 million to settle a lawsuit over stolen laptop data. The class action lawsuit was brought by retired and active duty military personnel over a VA data breach when a laptop was stolen which contained their personal information. The data included names, social security numbers, and dates of birth of about 26.5 million people. The now ex-employee was not authorized to take the data home and the information was stolen during a robbery. After an intensive search following the disclosure of the theft, the laptop was located and it was determined that the data "had not been improperly used." The settlement will be paid to veterans who can show they were harmed or incurred credit monitoring expenses.

CVS Pays $2.25 Million and Toughens Practices to Settle HIPAA Privacy Case

The U.S. Department of Health and Human Services and the Federal Trade Commission (FTC) announced recently that CVS, the nation's largest retail pharmacy chain, will pay the U.S. government $2.25 million to settle potential violations of the HIPAA Privacy Rule.

The Office of Civil Rights (OCR), which enforces the Privacy Rule, opened its investigation of CVS pharmacy compliance with the Privacy Rule after media reports alleged that patient information maintained by the pharmacy chain was being disposed of in industrial trash containers outside selected stores that were not secure and could be accessed by the public. According to the FTC, many CVS pharmacies also disposed of employment applications and payroll information in the same manner, jeopardizing the privacy of employees and job applicants. This is the first time that OCR has coordinated investigation and resolution of a matter with the FTC.

CVS agreed to pay $2.25 million and implement a detailed Corrective Action Plan to ensure that it will appropriately dispose of PHI such as labels from bottles and old prescriptions. The new practice will apply to all CVS retail pharmacies.

Related Links

- **VA @ American HIM Association:** http://journal.ahima.org/2009/02/06/va-to-pay-20-million-in-data-breach-case
- **CVS @ US Dept. of Health & Human Services:** http://www.hhs.gov/news/press/2009pres/02/20090218a.html

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.med.miami.edu/hipaa
Phone: 305-243-5000
Fax: 305-243-7487