Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

July 2015 - Issue 32

What's Inside?

Mobile Device and Text Messaging

As the use of mobile devices continues to increase in the work place, there is a heightened risk of a potential breach of protected health information (PHI) or protected identifiable information (PII). Given the security risk that mobile devices present, employees are not permitted to text message patient information or take photos of medical records or patients with their cell phones. Mobile devices are particularly vulnerable to loss and theft because of their small size and portability. The data on the devices are not encrypted, therefore keeping PHI or PII on them in any format is a violation of University policy and practice.

In November of 2014, the cellphone of a manager of St. Peter's Health Partner in Albany, New York was stolen. That theft exposed PHI of 5,117 patients who were treated at the facility. According to www.bizjournals.com, the stolen cellphone had access to corporate email systems and PHI for patients of St. Peter's Medical Associates, P.C., which included patient name and date of birth, as well as the day, time and location of medical appointments, with a general description of the reason for the appointment.

To read more, please visit: http://blogs.hcpro.com/hipaa/2015/01/cellphone-theft-results-in-breach-of-phi-of-more-than-5000-patients/%23sthash.ZtmdfRMe.dpuf

Frequently Asked Question

Q: I have access to UChart, may I view my own record, appointments and invoices?

A: No, it is against University policy. Employees who are patients must go through the same process as any other patient. We encourage you to use the https://myuhealthchart.com portal to access your patient information.

Have a Question?

Call us at (305) 243-5000 or email hipaaprivacy@med.miami.edu

The following security features are required on any mobile devices (smart phones, tablets) used to access University systems and PHI:

- **PIN:** If you do not already have auto-lock configured on your mobile device, a five-minute idle auto-lock value will be automatically configured (e.g., after five minutes of inactivity, you will be required to enter a PIN to access your mobile device).
- **Tamper wipe:** If a user enters a device PIN incorrectly 10 times in a row, the smart phone will be completely wiped, erasing all data, videos, pictures, etc. from the device.
- **Remote wipe:** In the event a smart phone is reported lost or stolen, please immediately contact IT at (305) 243-5999 which will initiate a remote wipe of the device. When a remote wipe takes place, all data, videos, pictures, etc. will be removed from the smart phone/device.
- **Encryption:** Where appropriate your mobile device should be encrypted. All portable media devices are required to be encrypted (USB, SD cards, portable hard drives, CDs, DVDs, laptops, etc.)

For additional information regarding mobile devices, please contact IT at (305) 243-5999.

Data and Media Destruction

Before discarding computers, bio-medical devices and other electronic media including USB drives, printer/scanners, tapes, CDs, DVDs, X-ray film, the data must be destroyed in a way that makes it unreadable and irreproducible. You should not dispose of these items yourself. The following are best practices for data and media disposal:

- Contact Information Technology when you have unneeded or non-functional computers, external drives, flash drives, medical devices with internal electronic storage (hard drives), or other media, to ensure secure disposal.
- Before disposal, shred any sensitive information on paper. Locked paper recycling receptacles are available. Environmental Services http://facilities.med.miami.edu/divisions/physical-pl/enviromental-services coordinates this service and can also assist with disposal of small electronic media.
- Contact Facilities and Support Services http://facilities.med.miami.edu for disposal of bio-medical devices.
- Secure handling of sensitive information in any format is critical when moving departments or information. An Administrator/Supervisor should manage all aspects of the move.

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

Mandatory Compliance Training - BOLO

It's that time again! HIPAA Privacy and Security Training will be arriving soon. The federally mandated HIPAA Privacy Regulations 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. A critical part of the safeguarding process is making sure that all workforce members are knowledgeable about HIPAA compliance and receive training. By law, all workforce members who have direct contact with protected health information are required to complete awareness training. The new mandatory training will be available via ULearn soon. Please be on the lookout!

FairWarning - Privacy Monitoring System

Please do your part by ONLY accessing patient information in our systems for legitimate clinical or business needs. The FairWarning patient privacy monitoring system was implemented on, August 11, 2014 to allow UM to proactively monitor the clinical systems that house patient information and provide data related to activities including, but not limited to, users accessing medical records of VIPs, family members, other UM employees or accessing their own record. Individuals who engage in inappropriate activity regarding patient information (accessing information for a non-business or clinical need) are subject to sanctions, as determined by Human Resources and/or Faculty Affairs. We appreciate all that you do for UHealth and ask that you make it a priority to respect patient privacy. Please remember that it is NOT an acceptable practice to ask a co-worker to access information of another employee or even your own information, any access should be for a legitimate clinical, business, research or teaching need related to the normal job functions which you have been hired to do. Remember to follow standard practices for access to your health information either through the https://MYUHealthChart.com portal or by contacting the medical records department of the facility or provider where you received your services. If you have any questions, please contact OHPS at (305) 243-5000.

PRIVACY & SECURITY NEWS

Six Biggest HIPAA Breach Fines

Since the HIPAA breach notification requirement took effect in 2009, nearly 31.4 million people have had their protected health information compromised in privacy and security breaches. The Office for Civil Rights, the HHS division responsible for enforcing HIPAA, has levied more than $25.1 million in fines against healthcare organizations responsible for violating the privacy and security rules.

To read more, please visit http://www.healthcareitnews.com/slideshow/6-biggest-hipaa-breach-fines?page=0

Insurance Giant Anthem Hit by Massive Data Breach

Department of Health and Human Services (HHS) Office for Civil Rights (OCR) has currently listed the Anthem, Inc. data breach as one of the largest breaches in their database. Anthem, Inc., one of the nation's largest health insurers, reported on March 13, 2015 that a total of 78.8 million customers' information was stolen in a cyber-attack. Data information that was stolen included names, dates of birth, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data. Reported by CNN Money, "Anthem stated that the breach was a result of a "very sophisticated external cyber-attack," and that law enforcement agencies were still working to identify the perpetrator." All affected individuals will receive identity fraud protection.

To read more, please visit http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html

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