Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

August 2010 - Issue 15

What's Inside?

System Access is a Privilege...User Access is Monitored

Did you know that the HIPAA/HITECH regulations require the active monitoring of healthcare information systems?

As a University of Miami employee, you signed a Computer Use Agreement and HIPAA Confidentiality Agreement. These apply to **all** workforce members regardless of tenure or rank. When you signed these agreements, you acknowledged that the use of University systems is solely for the performance of your job. UChart (EPIC), GE Centricity (IDX), CaneCare, as well as DHRS, KRONOS, and other systems contain audit trails that record user activity, including the specific records and times accessed.

Accessing the accounts of friends, celebrities, relatives, coworkers, or other individuals is strictly prohibited unless you are specifically required to do so as part of your work-related responsibilities. You should **not** access any account unless you have a specific job-related need to do so. Snooping is **not** a permissible activity. Audits are routinely performed on University systems and inappropriate access can result in disciplinary action up to and including termination.

Additionally, employees who are patients of the medical center must go through the same process as our patients who are **not** employees. If you need to schedule an appointment, please contact the appropriate area to do so. If you need to review your bills, you will need to contact Patient Financial Services, the Central Business Office, or the department where you were seen. If you are a UHealth patient, you may sign up for a myUHealthChart account that allows online access to portions of your health records. To learn more, visit http://www.myuhealthchart.com.

Employees who are provided access to University systems must safeguard their usernames and passwords. They should **not** be shared with any other workforce member, including supervisors. Employees will be held responsible for actions committed using their username and password. If you suspect your password has been compromised, please change it immediately. When accessing sensitive information, never leave your workstation unattended for an extended period of time. Before leaving your workstation, secure your desktop by locking it and/or closing the relevant application. Windows users may use <Ctrl+Alt+Del> and select *Lock Computer*.

Frequently Asked Question

Q: If a patient finds an error in his/her medical record, what should I do?

A: Provide the patient with an Attachment 33—Request for Amendment form (https://secureforms.med.miami.edu/hipaa/Forms/D3900031E.pdf). Ask them to complete and return it to the Office of HIPAA Privacy & Security (OHPS) for processing. Should a patient return a completed form to you, please immediately forward it to our office. OHPS will review the request and contact the appropriate physician.

The request may be accepted or denied. In either event, OHPS will correspond with the patient directly. For any questions regarding the process or form, please contact us at 305-243-5000.

Have a Question?

hipaaprivacy@med.miami.edu

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

Related Links

- **Computer Use and Confidentiality Agreement:** http://privacyoffice.med.miami.edu/documents/Confidentiality_Agreement2009.doc
- **HIPAA Confidentiality Agreement:** http://privacyoffice.med.miami.edu/documents/HIPAA_Confidentiality_Agreement.pdf
- **Secure Your Desktop:** http://privacyoffice.med.miami.edu/awareness/tips/securing-your-desktop
- **A045 Computer Access and Confidentiality:** http://www.miami.edu/index.php/a045_computer_access_and_confidentiality/
- **Access Authorization Policy:** https://secureforms.med.miami.edu/hipaa/Security/hsa4.1accessauthorization.pdf

Proper Disposal of Protected health and other Sensitive Information

Proper secure disposal procedures should be followed when discarding protected health or other sensitive information. Such documents should **not** be disposed of in trash cans. The blue recycle bins are used for this purpose. For assistance with the secure disposal of large quantities of files, please contact the Division of Environmental Services (Frances Kaniewski, fkaniews@med.miami.edu). Environmental Services can also handle electronic media such as CDs, floppies, videotapes, etc. Examples of sensitive information include: medical records, human resource files, applicant information, billing records, lab reports, images, printouts, student and parent financial records, clinical trial enrollee data, copies of prescriptions, etc.

You may have heard of "dumpster diving." This is the search for interesting stuff that others have thrown away. As the term implies, dumpster diving literally involves digging through discarded trash for financial statements, medical statements, patient records, and other papers that contain personal information. This personally identifiable information (PII) is a gold mine for

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

(continued) Proper Disposal of Protected Health and other Sensitive Information

identity theft and related criminal activity such as fraudulent Medicare billing. Carelessly disposing of sensitive information puts our patients, students, present and future employees, alumni, donors, and other stakeholders at risk while also subjecting the University to potential regulatory fines, incident response costs, and reputational harm.

Recently, there have been several media reports of various cases regarding the inappropriate disposal of information. Rite Aid Pharmacy has agreed to pay $1 million to settle potential violations of federal privacy rules by failing to protect sensitive customer information in disposing of prescriptions and pill bottles in store trash containers. See the Privacy & Security News section for more information.

Privacy & Security News

Rite Aid to Pay $1 Million Fine for Improper Disposal of Sensitive Information

Rite Aid Corp. has agreed to pay $1 million to settle potential violations of federal privacy rules when the national pharmacy chain failed to protect sensitive customer information in disposing of prescriptions and pill bottles. The settlement followed enforcement of the HIPAA Privacy Rule by the Department of Health and Human Services (DHHS). In a coordinated action, Rite Aid signed a consent order with the Federal Trade Commission (FTC) to settle potential violations of the FTC Act. DHHS' Office of Civil Rights and FTC collaborated on the investigation after television news media videotaped incidents when Rite Aid employees threw out pill bottles with individuals' health information on the labels in dumpsters that were accessible to the public. "We hope that this agreement will spur other health organizations to examine and improve their policies and procedures for protecting patient information during the disposal process," OCR Director Georgina Verdugo said in a statement.

Thousands of Personal Record Files Dumped in Recycling Bin

While making their monthly stop at the Land O' Lakes Recycling Center, Karen and Scott Keith noticed a paper bin bursting at the seams. Inside were what looked to be thousands of pastel and manila file folders. Curious, they pulled out a couple and were stunned to see that they appeared to be medical records. The information inside the files included some that couldn't be more personal — or dangerous: Social Security numbers, copies of drivers' license numbers, and even credit card numbers. "If that was my stuff, I would not want somebody to go through a dumpster and find it," Karen Keith said. "Somebody could definitely steal your identity, in the least."

UF Notifies Patients of Research-Related Privacy Breach

University of Florida officials have notified 2,047 people that their Social Security or Medicaid identification numbers were included on the address labels affixed to letters inviting them to participate in a research study. The numbers, which were included on the address labels so the telephone survey company could identify participants by their number only, were supposed to have been generated randomly. Instead, 647 were Social Security numbers and the remainder were Medicaid numbers, in both cases preceded by an alphabetical character with the hyphens omitted. The letters were sent through the U.S. Postal Service and the information was also shared with a telephone survey company. The problem was discovered about two weeks later and UF officials immediately launched an investigation. Use of Social Security numbers and certain other individual identifying numbers is against University policy.

Massachusetts Hospital Deals with Lost Backup Data Files

A third-party firm contracted by a Massachusetts hospital to destroy sensitive computer files cannot confirm that it wiped the information, leaving hundreds of thousands of patients at risk to identity theft. The names, addresses, Social Security numbers, and credit card data of up to 800,000 people may have been lost, according to Weymouth-based South Shore Hospital. In addition, the lost data contained information on doctors, staff members, and donors. The data was not encrypted. The hospital will notify individuals who may have been affected by the lost information. "I am deeply sorry that these files may have been lost," President and CEO Richard H. Aubut said in a statement. "I recognize that this situation is unacceptable and would like to personally apologize to all those who have trusted us with their sensitive information."

Industry, Advocates React to Web Tracking Report

The Wall Street Journal's recent report on the use of tracking technology by Internet companies "to trail users across the Web and create marketing profiles of them based on sites visited" is getting strong reactions from industry executives and privacy leaders, *MediaPost* reports. The decision by many companies to "omit far more information than they provide when discussing behavioral targeting" has resulted in privacy policies that are "less than transparent," the report states. Citing proposed legislation now being discussed in the U.S. Congress, the report continues on to quote one media commentator's perspective that advertising-supported websites should be "aggressively transparent," suggesting that if more companies shared this view, "the online ad industry might not be facing the threat of regulation."

Related Links

- **Rite Aid Settlement @ Healthcare IT News:** http://www.healthcareitnews.com/news/rite-aid-pay-1m-hipaa-privacy-breaches
- **Records Found at Recycling Center @ Tampa Bay Online:** http://www2.tbo.com/content/2010/jul/19/thousands-personal-record-files-dumped-recycling-b/news-breaking
- **University of Florida Address Label Privacy Breach:** http://news.ufl.edu/2010/07/06/privacy-breach
- **South Shore Hospital Lost Data @ The Boston Globe:** http://www.boston.com/news/local/massachusetts/articles/2010/07/20/hospital_files_with_data_of_800000_are_missing
- **Web Tracking Report @ MediaPost:** http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=133084

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