Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

October 2014 - Issue 30

What's Inside?

FairWarning Patient Privacy Application is Live
OCR Discusses Upcoming HIPAA Audits
Privacy & Security News

FairWarning Patient Privacy Application is Live

The privacy and security of health information are extremely important. Patients trust their healthcare providers to keep their information private and this trust can influence where they choose to receive their healthcare. The updated Florida Information Protection Act of 2014, combined with the national HIPAA/ HITECH Final Rule, call for stricter enforcement and fines on organizations that breach the confidentiality of patients and other sensitive information. Please do your part by ONLY accessing patient information in our systems for legitimate clinical, research, teaching or business needs.

To assist in these efforts, the FairWarning patient privacy monitoring system has been implemented and is live. This tool allows us to proactively monitor our 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 or UM employees. We appreciate all that you do for UHealth and ask that you join in efforts to respect patient privacy and build patient trust.

As a reminder:

- It is NOT an acceptable practice to ask a co-worker to access information of another employee or your information.
- Any access should be for a legitimate clinical, business, research or teaching need related to the normal job functions of an employee.
- Please follow standard practices for access to your health information either through the MYUHealthChart.com portal or by contacting the medical records department of the facility or provider where you received your services.

To read more, please visit http://privacyoffice.med.miami.edu/awareness/tips/implementation-of-automated-patient-privacy-monitoring

Frequently Asked Question

Q: May I allow another employee to access information in UChart or any other system I am logged into?

A: You should not allow others to use your access to any University systems. You are responsible for any and all actions taken using your username and password. Access to University systems is governed by the Computer Use and Confidentiality Policy.

Have a Question?

hipaaprivacy@med.miami.edu

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

OCR Discusses Upcoming HIPAA Audits

The 2009 HITECH Act mandated that the U.S. Department of Health and Human Services Office for Civil Rights (OCR) conduct periodic audits of covered entities and business associates for compliance with HIPAA privacy and security requirements. In February 2014, the agency issued a notice in the Federal Register announcing its plan to survey up to 1,200 covered entities and business associates to select organizations for the next round of HIPAA audits.

Speaking at the September 2014 Privacy and Security Forum hosted by the Healthcare Information and Management Systems Society (HIMSS), OCR Senior Advisor, Linda Sanches, discussed the upcoming HIPAA audits. Although Sanches declined to provide a specific timeline for the audits, the agency now expects to conduct more comprehensive on-site audits than originally anticipated, due to an increased budget for such reviews.

Sanches also stated that pre-screening surveys would be sent to potential audit candidates in the "near future," with surveys going first to covered entities and then to business associates. Covered entities will be randomly selected from a national database, while business associates will be chosen based on their inclusion in vendor lists provided by the surveyed covered entities.

To read more, please visit http://www.hiewatch.com/news/here-come-hipaa-audits-0

Verizon to Pay FCC Record $7.4 Million to Resolve Privacy Violation Investigation

The Federal Communications Commission's (FCC) Enforcement Bureau has reached a $7.4 million settlement with Verizon to resolve an investigation into the company's use of personal consumer information for marketing purposes. The investigation uncovered that Verizon failed to notify approximately two million new customers, on their first invoices or in welcome letters, of their privacy rights, including how to opt out from having their personal information used in marketing campaigns, before the company accessed their personal information to market services to them.

In addition to the $7.4 million payment, Verizon has agreed to notify customers of their opt-out rights on every bill for the next three years. "In today's increasingly connected world, it is critical that every phone company honor its duty to inform customers of their privacy choices and then to respect those choices," said Travis LeBlanc, Acting Chief of FCC's Enforcement Bureau. "It is plainly unacceptable for any phone company to use its customers' personal information for thousands of marketing campaigns without even giving them the choice to opt out." Phone companies collect an array of sensitive personal information about their customers, like billing and location data, and the Communications Act requires them to protect the privacy of that information.

For more information, please visit http://www.bna.com/verizon-pay-fcc-n17179894571/

Facebook Takes Vault of Consumer Data to the Masses

Using the vast amount of data it has gathered from its 1.3 billion users, Facebook has made itself the number-two digital advertising platform in the world, The New York Times reports. Now, it's going to take its targeted ads to the rest of the Internet, rolling out its ad platform, Atlas, which will allow marketers to use the social networking site's detailed knowledge of users to target ads to users on other websites and mobile apps. "Facebook has deep, deep data on its users. You can slice and dice markets, like women 25 to 35 who live in the Southeast and are fans of 'Breaking Bad,' " said Rebecca Lieb, a digital advertising and media analyst at the research firm Altimeter Group. The new Atlas platform, she said, "can track people across devices, weave together online and offline." But such detailed tracking of Facebook users on and off the service also raises privacy concerns. "There is a Big Brother perception that is a side effect of this kind of precision targeting," Lieb said.

For more information, please visit http://www.nytimes.com/2014/09/29/business/with-new-ad-platform-facebook-opens-the-gates-to-its-vault-of-consumer-data.html?_r=2

Nurse's Firing Shows Importance of Thinking Before Posting

The firing of a New York City nurse for her social media use has reaffirmed the hazards of healthcare workers bringing their work online. A nurse at New York Presbyterian Hospital was fired after posting a photo to Instagram of an empty trauma room after the treatment of a man hit by a subway train. The nurse was told she was fired for insensitivity, and not because she had committed a Health Insurance Portability and Accountability Act (HIPAA) violation. Nurses serve on the frontline of healthcare, which means they must take special care in what they post, Nancy Spector, Director of Regulatory Innovations for the National Council of State Boards of Nursing, told *ABC News*. "Most of the nurses that get into trouble have good intentions but they just don't know how far reaching social media can be," she said. "Remember, nothing can really be deleted."

For more information, please visit http://abcnews.go.com/Health/nurse-firing-highlights-hazards-social-media-hospitals/story?id=24454611

Hospital Network Hacked, 4.5 Million Records Stolen

Community Health Systems (CHS), which operates 206 hospitals across the United States, announced that hackers broke into its computer network and stole data on 4.5 million patients. The hospital stated that hackers gained access to patient names, Social Security numbers, physical addresses, birthdays and telephone numbers. The company has hospitals in 28 states but has its most significant presence in Alabama, Florida, Mississippi, Oklahoma, Pennsylvania, Tennessee and Texas. CHS hired an outside cybersecurity company to consult on the incident. The consultants determined the hackers originated from an Asian country and used high-end, sophisticated malware to launch the attacks sometime in April and June this year. The FBI said it's working closely with the company and the consultants "to target, disrupt, dismantle and arrest the perpetrators."

For more information, please visit http://money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/