Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

December 2014 - Issue 31

What's Inside?

FairWarning Patient Privacy Application is Live

More EHR Audits to Come in 2015

Privacy & Security News

FairWarning Patient Privacy Application is Live

The privacy and security of health information is 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 patient 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 "look up" information of another employee or yourself.
- Any access should be for a legitimate clinical, business, research or educational 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 use my access on healthcare systems to help relatives or friends with their appointments?

A: Accessing the accounts of friends, relatives, coworkers or other individuals is strictly prohibited unless you are specifically required to do so as part of your work-related responsibilities. Do not access any accounts unless you have a specific job-related need to do so. You may always call and assist someone with an appointment by calling the appropriate area.

Have a Question?

hipaaprivacy@med.miami.edu

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

More EHR Audits to Come in 2015

The EHR audits are coming. The Office of the Inspector General will continue to pay closer attention to the healthcare industry's use of electronic health records – in particular HIPAA, EHR incentive payments and fraud, according to the office's recently released 2015 work plan.

As the healthcare industry moves toward digitization of health records, the OIG has requested a $400 million FY 2015 budget, an increase of $105 million and 284 additional full-time employees to help expand OIG audits and reviews, several of them examining IT security, compliance and, yes, even electronic health records. "Important changes are taking place across the healthcare industry," wrote Daniel R. Levinson, U.S. inspector general, in OIG's 2015 work plan justification. These changes, Levinson continued, include "an emphasis on coordinated care and an increased use of electronic health records. OIG will need to adopt oversight approaches that are suited to an increasingly sophisticated healthcare system and that are tailored to protect programs and patients from existing and new vulnerabilities."

Part of the OIG's role in 2015 will include leveraging data analytics and "forensic enhancements" to investigate increasingly sophisticated healthcare fraud, which is, now more than ever, including electronic health records in the process.

To read more, please visit http://www.healthcareitnews.com/news/more-ehr-audits-come-2015

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

PRIVACY & SECURITY NEWS

Court Allows HIPAA Negligence Claim

Legal experts are analyzing the potential national impact of a Connecticut Supreme Court ruling that plaintiffs can sue for negligence if a healthcare provider violates HIPAA regulations for protecting patient privacy. The Connecticut case of Emily Byrne vs. Avery Center for Obstetrics and Gynecology involved a patient who sued a healthcare clinic that released her medical records to a third party without her authorization. But legal experts say the ruling could potentially have relevance in certain data breach cases. "HIPAA does not provide for the 'private right of action,' or [the right of] private folks to sue under the statute," says privacy attorney Brad Rostolsky of the law firm Reed Smith. "Enforcement actions and fines for HIPAA violations are levied by federal regulators. But in a handful of cases, like this Connecticut ruling, courts have allowed HIPAA as the 'standard of care' for negligence claims."

Privacy attorney Elizabeth Hodge of the law firm Akerman LLP explains that in this Connecticut case, HIPAA is the "standard of care" for protecting patient confidentiality that was used to show that a patient's privacy rights were violated. "In data breach cases, plaintiffs could argue that a healthcare provider, insurer or other covered entity did not meet the 'standard of care' with the HIPAA security or privacy rule in protecting records, and that the failure to meet that standard of care was negligent." For more information, please visit http://www.healthcareinfosecurity.com/court-allows-hipaa-negligence-claim-a-7535

Court Upholds $1.4 Million Privacy Verdict

A second state court ruling in recent weeks calls attention to how incidents involving alleged patient privacy violations can lead to negligence lawsuits that invoke HIPAA as a benchmark.

In the most recent case, the Indiana appellate court has upheld a $1.4 million jury verdict awarded in 2013 to a customer that alleged her privacy was violated by a Walgreens pharmacist who inappropriately reviewed and shared the woman's prescription history with a third party.

"It does not surprise me that state-level courts are deciding to find the HIPAA privacy and security rules set the generally accepted standard on how health information may be used and disclosed," says attorney David Holtzman, vice president of compliance at security consulting firm CynergisTek. "Juries deciding these cases are acting on their belief of what is right or wrong after a thorough examination of the facts."

"The privacy protections, like those in the HIPAA Privacy Rule, are the most recognizable tool that allows for evaluating what is acceptable conduct. Just as importantly, courts are supporting the notion that there can be real and demonstrable harm that results from the disclosure of sensitive health information with a malicious intent to cause emotional pain or injure a person's reputation." For more information, please visit http://www.govinfosecurity.com/court-upholds-14-million-privacy-verdict-a-7567

Genomic Researchers Seeking Balance Between Ethics and Patient Privacy

As the genomic research field continues to progress, those in the community are asking where the line between patient privacy and family notification resides, Star Tribune reports. When researchers find something troubling such as a mutation in a patient's blood stream that reveals a high chance of breast cancer, should researchers alert the patient's daughter? And what if the patient wanted such information kept private? Susan Wolf of the University of Minnesota is one of three investigators leading a $2.4 million project funded by the National Institutes of Health to develop guidelines on when to disclose "incidental findings" in genomic research. For more information, please visit http://www.startribune.com/lifestyle/health/281876961.html

Cam Kerry: Surveillance Should Not Overshadow Civil Liberties

In a column for Forbes, Brookings Institution Fellow Cameron Kerry reacts to calls by FBI Director James Comey that default encryption of smartphones will hurt law enforcement's attempts to curb criminal activity and terrorism. Kerry writes, "That is a step too far, because the gain to law enforcement is out of proportion to the erosion of security, privacy and trust." He also notes that "strong encryption is an important element in strengthening defenses against increasing cyber-attacks and data breaches," adding, "Expanded use of encryption may obscure a portion of digital trails, but that still leaves exabytes of information from which to seek evidence." FBI Director Comey was asked if requiring a technical solution to enable surveillance of encrypted communications would amount to putting a “back door” in applications and equipment, Comey said he is seeking a “front door” that would operate with “clarity and transparency.” This makes sense as a legal matter but not as a technical matter. There is a significant difference between interception done under a legally-authorized judicial warrant with accountability, and interception cloaked in nothing but secrecy. But, from a technical standpoint, the FBI’s front door is a hacker’s or spy’s back door. For more information, please visit http://www.forbes.com/sites/realspin/2014/11/06/the-law-needs-to-keep-up-with-technology-but-not-at-the-expense-of-civil-liberties/

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