Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

May 2011 - Issue 18

What's Inside?

FTC Posts Guidance for Providers, Insurers on Medical Identity Theft

Highlighting health data breaches, the Federal Trade Commission (FTC) recently posted frequently asked questions about medical identity theft for healthcare providers and insurers. Medical identity theft occurs when an individual obtains healthcare services or prescription drugs using the identity of someone else, or when those working in a healthcare provider setting use an individual's personal information to submit false bills to an insurer.

People victimized by medical identity theft often realize the theft has occurred when they get a bill for a service they did not receive, are contacted by a debt collector for medical bills for services they never obtained or from doctors they never saw, or are denied insurance because their records are incorrect. As serious as those issues are, think about the consequences if incorrect information in the medical record is used to make treatment decisions.

The guide makes clear that if a patient reports being a victim of medical identity theft, providers and insurers are expected to conduct an investigation and correct any incorrect information.

An example provided by the FTC states the following: "If your billing department gets a call from a patient who claims she was billed for services she didn't receive, review your records relating to the services performed and any supporting documentation that verifies the identity of the person receiving the services. You also should review the patient's medical record for inconsistencies." The provider/insurer must follow the applicable rules of the Fair Credit Reporting Act, review their data security practices, and provide notification as required under HIPAA or other federal or state security breach notification laws.

The FTC ranks South Florida as the number one metropolitan area in the country for identity theft complaints.

Related Links

- **Medical Identity Theft:** http://www.med.miami.edu/hipaa/public/x358.xml
- **FAQs for Health Care Providers and Health Plans:** http://business.ftc.gov/documents/bus75-medical-identity-theft-faq-health-care-health-plan

Frequently Asked Question

Q: What should I do if I receive a call from a patient stating they are a victim of identity theft?

A: Obtain the following information: full name, date of birth, address, and a telephone number where he or she may be reached.

Ask what documentation they have that makes them believe they are a victim of identity theft and obtain a copy (examples of such documentation may include a billing statement/invoice received, police report/case number, letter from insurance company, etc.). Provide all information to the Office of HIPAA Privacy & Security for investigation.

Have a Question?

hipaaprivacy@med.miami.edu

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

Mandatory Privacy & Security Training Updated

HIPAA regulations and other laws governing the protection of personally identifiable information require an ongoing privacy and security awareness training program. To this end, the Office of HIPAA Privacy & Security has updated its mandatory training.

All faculty and staff of the Medical campus are required to renew this training every two years. For many, this time has already expired or will expire shortly.

Human Resources will require this training be renewed as part of a University training initiative that will meet multiple compliance requirements. This training initiative is currently in the planning phase.

However, the updated module is now available in ULearn. To take this training, log in to ULearn at http://ulearn.miami.edu. The course is titled *HIPAA Privacy & Security Awareness 2011*. Doing this now will remove it from the list of courses you will be required to complete later on.

For questions regarding ULearn, please contact the Professional Development and Training Office at 305-243-3090. For questions related to the content of the training module, please email hipaaprivacy@med.miami.edu.

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

Child Identity Theft Growing Rapidly

Carnegie Mellon's CyLab Research Center, one of the world's premier cybersecurity and privacy research centers, has released the first large child identity theft report ever published.

Based on identity protection scans of more than 42,000 U.S. children, it suggests a previously unrecognized demographic for what the FBI has named the fastest-growing crime in the United States. The report reveals that 10.2% of the child identities scanned had someone else using their Social Security number — 50 times more frequently than the 0.2% rate for adults in the same population. Of this group, 4,311 children had Social Security numbers that were used by other people. 76% of the cases involved malicious fraud — deliberate and intentional criminal activity. 24% were cases of mixed credit file information.

Child IDs were used to purchase homes and automobiles, open credit card accounts, secure employment, and even obtain driver's licenses. The largest fraud ($725,000) was committed against a 16 year old girl. The youngest victim was five months old; 303 victims were under the age of five.

Related Links

- **Child ID Theft; A Lot of Questions Need to be Answered:** http://www.cyblog.cylab.cmu.edu/2011/03/child-identity-theft.html

PRIVACY & SECURITY NEWS

South Florida Medical Office Workers Indicted on HIPAA Violations

Two medical office workers have been indicted on HIPAA violations and related charges for their alleged roles in an identity theft ring that used stolen patient information to access financial accounts. Defendants Erica Hall and Sharelle Finnie worked as office assistants at two separate medical offices in Coral Springs and Fort Lauderdale. The pair allegedly stole patient information, including names, dates of birth, Social Security numbers, and other medical information, then sold it to co-conspirators. If convicted of the HIPAA violations, Hall and Finnie could each face up to ten years in prison. Ten other alleged members of the ID theft ring – all Florida residents – were also indicted on bank fraud, identity theft, and related charges.

Allina Hospitals Fires 32 Employees for Records Snooping

Allina Hospitals and Clinics has fired 32 employees for inappropriately viewing electronic health records of patients involved in a recent mass drug overdose. HIPAA prohibits healthcare workers from accessing the records of patients unless they are participating in some aspect of their care. Eleven people were hospitalized March 17 after overdosing on a synthetic hallucinogen, according to local news accounts. Spokesman David Kanihan stressed that Allina has consistently enforced its privacy policy by dismissing those who access records without a legitimate reason. Every Allina employee receives training on the guidelines for when patient records can be accessed, he points out. "We take our obligation to protect patient privacy very seriously," according to an Allina statement. "Anything short of a zero-tolerance approach to this issue would be inadequate."

Apple, Others Sued over Privacy —Again

Apple, Pandora Media, and The Weather Channel have been named in a lawsuit alleging that the companies did not disclose that personal data was being shared with third-party advertising networks. It targets companies for being able to trace devices using a unique device identifier (UDID). "Because the UDID is unique to each iPhone and iPad, it is ... a means of reliably tracking mobile device users' online activities," the new suit says. "However, unlike with browser cookies, Apple does not provide users any way to delete or restrict access to their devices' UDIDs," it says. The suit also highlights the database that tracks location which has become a target of interest recently. Apple says this data is part of a database of cell towers and Wi-Fi hotspots, which lets devices determine their location more efficiently. Apple claims it has addressed several claims as part of a software update in iOS 4.3.3. Apple has also said that it intends to fully encrypt that database on the device itself in its next major system software update.

FTC: Opt-Out Should Mean Opt-Out

The Federal Trade Commission announced a settlement with Chitika, Inc. over its failure to honor consumers' choice in contrast to claims made in its privacy policy. This is the FTC's first consent settlement relating to privacy with an online advertising network. As disclosed in its privacy policy, Chitika offered consumers the choice of opting out of its online advertising network. However, Chitika did not disclose to consumers that the opt-out would expire only 10 days later. The FTC believes Chitika's actions were false and misleading, constituting deceptive trade practices in violation of the FTC Act.

Related Links

- **South Florida Workers Indicted @ Health Leaders Media:** http://www.healthleadersmedia.com/content/HEP-264739/2-FL-Medical-Office-Workers-Face-Fraud-Charges.html
- **Allina Hospitals @ Star Tribune:** http://www.startribune.com/business/121398054.html
- **Apple Lawsuit @ Yahoo:** http://news.yahoo.com/s/zd/20110511/tc_zd/264350
- **FTC Opt-Out @ Chronicle of Data Protection:** http://www.hldataprotection.com/2011/03/articles/consumer-privacy/ftc-optout-should-mean-optout

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