Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

March 2013 - Issue 25

What's Inside?

Tax Season is Here; File Early to Avoid Scams

As faculty and staff receive their W-2s and other tax documents, it is time to start thinking about filing income tax returns early. This is also the season when identity thieves go into overdrive, attempting to file fraudulent tax returns. Tax fraud is now the third-largest theft of federal funds after Medicare/Medicaid and unemployment-insurance fraud. South Florida, already the leader in Medicare fraud, is also taking the lead in tax-identity theft. Florida has the highest rate of identity theft in the country, with 178 complaints per 100,000 residents in 2011. Tax-identity theft exploded to more than 1.1 million cases in 2011 from 51,700 in 2008. The Treasury Inspector General for Tax Administration reported discovering an additional 1.5 million potentially fraudulent 2011 tax refunds totaling in excess of $5.2 billion.

Fraudulent tax returns can come in the form of tax-identity theft, refund fraud, or return-preparer fraud. With e-filing, evidence of fraud is difficult to find. There are no signed tax forms, envelopes or fingerprints, and e-filing promises quick refunds. For criminals to e-file in your name, they need your name and Social Security number, combined with a phony W-2 (wages) or fabricated Schedule C (business income). ID thieves steal your personal information to file a fake tax return in your name, usually tweaking the numbers to get a large refund. The refund can be posted to an anonymous "Green Dot" prepaid Visa card purchased at a drugstore, Walmart etc. Such cards have a routing and account number suitable for direct deposit.

The taxpayer whose ID has been stolen will not find out until he/she attempts to file the real return and then is informed by the IRS that the return has already been filed and the refund sent. This is the primary reason to file as early as possible, before criminal attempts to do so on your behalf. To see additional steps to protect your tax identity, please visit http://privacyoffice.med.miami.edu/awareness/tips/tax-season-is-here-file-early-to-protect-yourself

Frequently Asked Question

Q: Do I always need to use a cover sheet when faxing PHI?

A: Yes, a cover sheet with the approved disclaimer language must always be used. To see the disclaimer language as well as best practices for faxing please visit Best Practices for Faxing Communication.

Have a Question?

hipaaprivacy@med.miami.edu

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

HHS Issues Final HIPAA Omnibus Rule

The U.S. Department of Health and Human Services (HHS) has released its highly anticipated modifications to the HIPAA Privacy and Security rules. HHS Secretary Kathleen Sebelius said, "The new rule will help protect patient privacy and safeguard patients' health information in an ever-expanding digital age." The rule specifies when data breaches must be reported to the Office for Civil Rights (OCR), sets new requirements for use of protected health information in marketing and fundraising and expands direct liability to "business associates" of HIPAA-covered entities. OCR Director Leon Rodriguez said the changes "enhance a patient's privacy rights" and strengthen "the ability of my office to vigorously enforce" the HIPAA privacy and security rules. The omnibus rule is made up of four main rules altering the privacy, security, enforcement and breach notification regulations under HIPAA and is based on HITECH & Genetic Information Nondiscrimination Act of 2008 (GINA) statutory changes. It includes final modifications to regulations set forth by the HITECH Act; changes to the HIPAA Enforcement Rule; the Breach Notification for Unsecured Protected Health Information under the HITECH Act, and the HIPAA Privacy Rule as mandated by the GINA.

Center for Democracy & Technology Health Privacy Project Director Deven McGraw commented, "We are very pleased to have the final rules implementing most of the HITECH modifications to HIPAA. Congress intended for these privacy protections to be in place as the EHR incentives went into effect. The delay was unfortunate but now the rules are out and we can begin the process of understanding and implementing them."

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

AG Sues Accretive Health for Privacy Violations

Minnesota AG Lori Swanson has filed a lawsuit against Accretive Health, a debt collection agency, for failing to protect the confidentiality of health care records and not disclosing to patients its extensive involvement in their health care through its role in managing revenue and health care delivery systems at two hospitals. Accretive lost a laptop containing unencrypted health data of 23,500 patients. The lawsuit alleges that Accretive gained access to sensitive patient data through contracts with the hospitals and numerically scored patients' risk of hospitalization and medical complexity, graded their "frailty," compiled per-patient profit and loss reports, and identified patients deemed to be "outliers." "The debt collector found a way to essentially monetize portions of the revenue and health care delivery systems of some nonprofit hospitals, without the knowledge or consent of patients who have the right to know how their information is being used and to have it kept confidential," said AG Swanson. The lawsuit alleges that Accretive violated state and federal health privacy laws, state debt collection and consumer protection laws. It seeks an order requiring Accretive to fully disclose to patients: (1) what information it has; (2) what information it lost; (3) where and to whom it has sent information; (4) the purposes for which it amasses and uses information about Minnesota patients.

How Our Online Experiences Affirm What We Already Believe

Based on companies' abilities to collect data on individuals online in order to send targeted ads based on behaviors, "99 percent of us live on the wrong side of a one-way mirror, in which the other one percent manipulates our experiences," reports Scientific American. Unseen hands "curate your entire experience" and predetermine the news you see and even the people you meet, which serves to "affirm, instead of challenge, what we already believe to be true." Technology enables Google, Facebook and others to gather information about us and use it to tailor the user experience to our own personal tastes, habits and income. Advertising currently drives the vast majority of the Internet industry by volume of revenue. Silicon Valley is excellent at funding companies that give you free apps and then collect and sell your data when you use them. However, data collection is going beyond strict advertising and enabling insurance, medical and other companies to benefit from analyzing your personal, highly detailed "Big Data" record without your knowledge. These companies then make decisions about you including whether you are even worth marketing to at all.

Maryland AG Puts Privacy in the Spotlight

Maryland AG Doug Gansler has made "Privacy in the Digital Age" his initiative for 2013. Gansler identified several points of focus for the initiative: (1) creating transparency in data collection and dissemination practices, (2) empowering consumers with opt-out controls, (3) ensuring that consumer are protected against data breaches, (4) confronting financial privacy and mobile payment issues, (5) bringing attention to location privacy, (6) improving cybersecurity awareness, and (7) increasing protection against cyber-bullying. Gansler also announced the formation of a new Internet Privacy Unit. The unit will "monitor compliance with state and federal consumer protection laws, including the Children's Online Privacy Protection Act," as well as "examine weaknesses in online privacy policies and work alongside major industry stakeholders and privacy advocates to provide outreach and education to business and consumers." California's AG Kamala Harris announced a similar unit in 2012.

Breach Class Action Suit Advances

A recent appellate court ruling in Florida might pave the way for the first U.S. class action lawsuit involving a health data breach to move forward to trial. The case involves the theft of laptop computers from the Florida offices of AvMed. The laptops contained personal information on 1.2 million AvMed health plan members. Among the members were Juana Curry and William Moore, plaintiffs in the case that was filed by the Edelson McGuire LLC. The suit alleges that both Curry and Moore became victims of identity theft after the AvMed laptops were stolen. The case alleges that plaintiffs' sensitive information was used to open various financial accounts. The U.S. Court of Appeals Eleventh Circuit decision reversed an earlier district court decision that dismissed the case, in part, due to failure to state a cognizable injury.

Related Links

- **AG Sues Accretive Health for Privacy Violations:** http://www.ag.state.mn.us/Consumer/PressRelease/120119AccretiveHealth.asp
- **How Our Online Experiences Affirm What We Already Believe:** http://www.scientificamerican.com/article.cfm?id=rich-see-different-internet-than-the-poor
- **Maryland AG Puts Privacy in the Spotlight:** http://www.hldataprotection.com/2013/01/articles/consumer-privacy/maryland-attorney-general-to-focus-on-privacy-establishes-internet-privacy-unit/
- **Breach Class Action Suit Advances:** http://www.databreachtoday.com/breach-class-action-suit-advances-a-5126

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