Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

July 2011 - Issue 19

What's Inside?

Social Networking Policy for UHealth/School of Medicine

Use of social networking sites such as Facebook, Twitter, LinkedIn, etc. continue to experience explosive growth. It's not just individuals; businesses are all scrambling to create a social media presence and strategy. While social networking is great as a means to stay in contact with friends and communicate in general, it remains a relatively new phenomenon. As a result, a social networking policy has been created that provides guidelines for the appropriate use of this medium at the medical campus. In particular, faculty and staff need to exercise caution with protected health information (PHI), personally identifiable information (PII), and other types of non-public information.

It is important that all communication in online communities made on behalf of the University are consistent with the University's standards for business conduct, policies, and applicable laws — including privacy laws such as HIPAA. This Social Networking Policy applies to all Medical Campus social media sites, including access to personal sites while using University equipment and facilities; all such communications are subject to monitoring. Misuse or other inappropriate postings of information related to coworkers, patients, or other non-public information may be in violation of Social Networking, Computer Use, and Human Resources policies that could result in disciplinary action up to and including termination.

To review the Social Networking Policy, please visit http://www.med.miami.edu/hipaa/public/documents/social_networking_policy.pdf.

Frequently Asked Question

Q: Does the HIPAA Privacy Rule prevent reporting to consumer credit reporting agencies or otherwise create any conflict with the Fair Credit Reporting Act (FCRA)?

A: No. The Privacy Rule's definition of "payment" includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following protected health information about the individual: name, address, date of birth, Social Security number, payment history, and account number.

Have a Question?

hipaaprivacy@med.miami.edu

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

The Cost of Non-Compliance — Fines & Corrective Action

The University of California at Los Angeles Health System (UCLAHS) has agreed to pay a fine of $865,500 and has committed to a corrective action plan aimed at remedying gaps in its compliance with the HIPAA Privacy and Security Rules. This is a result of complaints that employees were snooping into celebrity patients' health records. In addition to the fine, UCLAHS has agreed to review, revise, and maintain, as necessary, existing policies and procedures and develop written policies and procedures that comply with federal standards that govern the privacy of individually identifiable health information.

Meanwhile, health insurer WellPoint Inc. settled with the Indiana Attorney General's office over a delayed notification of a consumer data breach that affected the records of 32,051 people. Under terms of the settlement, WellPoint will pay the state $100,000 for the incident, which exposed data that included Social Security numbers, financial information, and health records. In addition to the fine, WellPoint must provide up to two years of credit monitoring and identity theft protection services to Indiana consumers affected by the breach, as well as offer reimbursement to any WellPoint consumer of up to $50,000 for any losses that result from identity theft due to the breach.

It should be further noted that these financial penalties and increased regulatory oversight are in addition to any reputational damage or other incident response and damage control costs.

Related Links

- **UCLA:** http://latimesblogs.latimes.com/lanow/2011/07/ucla-pays-865500-to-settle-celebrity-medical-record-snooping-case.html
- **WellPoint Settlement:** http://www.govinfosecurity.com/articles.php?art_id=3824

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

PRIVACY & SECURITY NEWS

Insecure Home Wireless Network? You Could Receive a Visit from the FBI

Lying on the floor with assault weapons trained on him, the Buffalo homeowner didn't need long to figure out the reason for the early morning wake-up call from federal agents. "We know who you are! You downloaded thousands of images last night," the man's lawyer recounted the agents saying." Law enforcement officials say the case is a cautionary tale. Their advice: secure your wireless router. For two hours, federal agents examined the homeowner's computer, eventually taking it along with his and his wife's iPads and iPhones. Investigators later determined the homeowner was not responsible for downloading the images; someone else was using his wireless signal. Subsequently, agents arrested a neighbor and charged him with distribution of child pornography. You may not be guilty but "you look like the suspect," said Orin Kerr, a George Washington University professor, who said that's just one of many reasons to secure home routers. Indeed, savvy hackers can go beyond just connecting to the Internet; they can monitor Internet activity and steal passwords or other sensitive information. All wireless routers come with encryption capabilities, but setting it up securely usually takes a few additional steps beyond the default installation. Best practices include replacing any default network names and passwords, implementing the best encryption supported by your routers and its connecting devices, and keeping an eye out for security patches or updates.

Facebook Flaws Leaked Data to Third Parties, Claims Researcher

Facebook's reputation for less than stellar privacy and security practices took another battering after a Symantec researcher revealed that as many as 100,000 Facebook applications could have leaked data to third parties. The research from Symantec's Nishant Doshi found that Facebook users' profiles, photographs, chats, and other personal data were leaked to application developers, many of whom are advertisers. According to Doshi, his research team found that some embedded Facebook applications – under certain conditions – inadvertently leaked access tokens to third parties like advertisers or analytic platforms. Each token is associated with a select set of permissions, like reading your wall, accessing your friends' profiles, posting to your wall, and so on. "Needless to say, the repercussions of this access token leakage are seen far and wide. Facebook was notified of this issue and has confirmed this leakage. Facebook notified us of changes on their end to prevent these tokens from getting leaked", he says.

St. Louis University Hacking Affects Nearly 13,000 Employees and Students Using Counseling Services

St. Louis University in Missouri reports that its network was hacked and personally identifiable and protected health information was accessed without authorization. An investigation conducted by the university revealed that some of the affected servers contained personally identifiable information on approximately 12,000 current and former employees as well as contractors. Employee information included Social Security numbers. The servers also contained protected health information on approximately 800 students. For some students who received counseling through the university's Student Health service, the protected health information included names, dates of birth, dates of service, testing assessments, diagnoses, and treatments. The breach was reported to the FBI, which is investigating the incident.

HHS Inspector General Says Push for Electronic Medical Records Overlooks some Security Gaps

The push to computerize medical records has failed to fully address longstanding security gaps that expose patients' most sensitive information to hackers and snoops, government investigators warn. Two reports by the inspector general of the Health and Human Services Department find that the drive to connect hospitals and doctors so they can share patient data electronically is being layered on a system that already has glaring privacy problems. Connecting it could open new pathways for hackers, investigators say. The market for illicit healthcare information is booming. Fraudsters covet healthcare records, since they contain identifiers such as names, birth dates, and Social Security numbers that can be used to construct a false identity or send bogus Medicare bills. The shortcomings in the system "need to be addressed to ensure a secure environment for health data," said the main report, adding that the findings "raise concern" about the effectiveness of security safeguards for personal healthcare information. Responsibility for computer security within the Health and Human Services Department lies primarily with the Office of the National Coordinator, which is leading the drive to computerize records, and the Office of Civil Rights, which oversees the enforcement of existing privacy laws.

Related Links

- **Securing your Home Wireless Network:** http://www.med.miami.edu/hipaa/public/x461.xml
- **FBI Raid @ MSNBC:** http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless
- **Facebook Leaks @ SC Magazine:** http://www.scmagazineuk.com/facebook-may-have-leaked-hundreds-of-thousands-of-user-details/article/202570
- **St. Louis University Hacking @ PHIprivacy.net:** http://www.phiprivacy.net/?p=6205
- **HHS Inspector General @ PBS:** http://www.pbs.org/newshour/rundown/2011/05/report-push-for-electronic-medical-records-overlooks-security-gaps.html

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