Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

February 2012 - Issue 21

What's Inside?

Healthcare Face Challenges Protecting Patient Privacy & Security

Healthcare organizations and other industry players are falling short in protecting the privacy and security of patient information, according to a report from consulting firm PwC. A survey of 600 executives from hospitals, physician groups, health insurance companies, and pharmaceutical and life sciences companies found that theft accounted for 66 percent of reported health data breaches in the past two years. Some of this is medical identity theft, the report said. Thirty-six percent of surveyed hospitals and physician groups said patients had sought services using somebody else's name and identification. The rapid rise of mobile devices also has flummoxed many healthcare organizations. Fifty-five percent of those surveyed said they had not addressed privacy and security issues associated with mobile technology. Under a quarter of respondents had come to grips with the privacy and security implications of social media. More than half of healthcare organizations said they'd had at least one issue with information security and privacy since 2009. The most frequently observed issue--reported by 40 percent of providers--was the improper use of protected health information by someone who worked in the organization.

PwC found that electronic data breaches occur three times as often as paper-based breaches and affect 25 times more people when they occur. Most electronic breaches, however, are not related to computer hacking, but to insider theft or human errors, such as the loss of a computer device. The new HIPAA security provisions expand the coverage of business associates of providers. But only 36 percent of health organizations perform a pre-contract assessment of their business associates such as business partners and vendors, and just 26 percent conduct post-contract compliance assessments, says PwC. Also of note: While three-quarters of healthcare organizations said they either will seek or intend to seek "secondary uses" for health data, less than half of those entities address related privacy and security issues. "Top challenges for the industry related to the use of secondary data were establishing information security functions, appropriately encrypting data, and creating multiple levels of separation between the data and the end consumer," the report noted.

Frequently Asked Question

Q: Can I use my personal storage devices such as USB flash drives to store University information?

A: No. University information, and in particular, sensitive information, should only be stored on University approved and authorized devices. If you have a business need contact your IT support or Central IT for advice and selection of approved (and encrypted) devices. Further guidance on this topic will be forthcoming

Have a Question?

hipaaprivacy@med.miami.edu

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

Using USB Hard Drives or Flash Drives?

Faculty and Staff are reminded of the critical importance to protect sensitive data. The institution continues to experience incidents related to loss of such devices. Examples of sensitive data include personally identifiable information (PII), protected health information (PHI), social security numbers, credit card numbers and other confidential University data not for public exposure. Ideally University sensitive data should NOT be stored on mobile devices such as USB hard drives and flash drives. Such sensitive data should only be stored on authorized University servers/storage and accessed remotely using secure communication techniques provided by authorized University IT resources. If there is an undeniable business reason for storing University sensitive information on mobile devices, users must obtain permission from appropriate University management and ensure that reasonable steps are taken to keep such data private and secure. Mobile storage devices are subject to one principal risk — theft or loss — and secondly, unauthorized access or copying.

In any case, disclosure of potentially sensitive data can damage the University's reputation as well as lead to a myriad of expenses including fines, legal costs, notification fees, etc. Departments/business units from which such incidents originate will be responsible for meeting such costs. The principal precaution, again, is not storing sensitive data on the mobile device. However, assuming an unavoidable business need, the active protection MUST be the use of industry-standard encryption. Should the device be lost or stolen, the sensitive data would be protected from inappropriate access/use. For operational details on implementing suitable encryption measures contact your IT support group and/or Central Information Technology.

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

Stanford Hospital Sued for $20M over Data Breach

Twenty million dollars for 20,000 patients: That's how much Stanford Hospital & Clinics stands to owe if patients win a class-action lawsuit filed against the leading hospital. Stanford is vowing to fight the lawsuit filed by the patient, who represents thousands of patients whose information was exposed online for almost an entire year, reports Palo Alto Daily News. The data breach was discovered on Aug. 22, 2011 and the information was removed the next day when Stanford Hospital began an "aggressive investigation," according to a Stanford press release. Stanford pointed to the billing contractor (and co-defendant) Multi-Specialty Collection Services LLC (MSCS) as the culprit for mishandling patients' data. The hospital sent encrypted data to MSCS, according to Stanford Hospital. MSCS's executive vice president allegedly created an unencrypted electronic spreadsheet and sent it to an unauthorized person to create bar graphs and charts. The unnamed third party allegedly posted it to the public Student of Fortune, a homework help site. The data breach included patients' names, diagnosis codes and hospital account numbers. A MSCS marketing vendor converted the spreadsheet and forwarded it to a job applicant as part of a skills test, MSCS told The New York Times. The vendor said the breach resulted from "a chain of mistakes which are far too easy to make when handling electronic data."

Hard Drive Theft Prompts Insurer to Spend $6M to Encrypt Data

After thieves stole 57 hard drives containing information on about 1 million of its members, Tennessee BlueCross BlueShield resolved that a similar incident would never happen again. The insurer recently announced that it has spent about $6 million encrypting all of its data at rest. The HITECH Act made encryption a safe harbor for covered entities (CEs) and business associates under the security breach notification provision. Privacy and security experts view this provision as an implicit mandate for encryption. The plan to encrypt its data in all states had become “more of a philosophy” at BlueCross BlueShield of Tennessee, says Michael Lawley, VP of Technology Shared Services. The insurer had planned to adopt encryption as the technologies became available but after the theft occurred in October 2009, Lawley says the company kicked into high gear and not only reviewed all of its policies and procedures, but also began a meticulous inventory of all the places where data reside in the organization. They took a “maniacal approach” to the task because “we wanted to make sure that we didn’t go through this journey and then have to repeat it,” he says. The insurer spent $6 million, 5,000 man hours and just over a year to encrypt all of its data at rest, including 885 terabytes of mass data storage, 1,000 server hard drives, 6,000 desktop and laptop computers, 25,000 phone call recordings and 136,000 volumes of backup tape.

DropBox Drops the Ball on Data Security

Dropbox, a provider of cloud-based data storage services, is in hot water with the Federal Trade Commission over claims that it lied and intentionally deceived customers into believing that their data is more private and secure than it really is. Whether Dropbox was deliberately misleading, or just failed to clearly communicate policy changes, the complaint filed with the FTC illustrates concerns over online data security. At issue are Dropbox's terms of service. Previously, the company stated in its terms of service that "all files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account password." But, Dropbox has continued to modify the terms of service, and backpedal on exactly how secure customer data is--sometimes putting its foot in its proverbial mouth.

Google Announces New Privacy Policy/FaceBook IPO

Since Google announced its new, controversial privacy policy in January, 2012, interest in online privacy has spiked as more people question how Google and other companies are managing their data.
Search for dinner recipes on Google, and you may see a recommendation for a KitchenAid video clip the next time you visit YouTube. That, as one example, is what the online search giant says changes to its privacy policies will mean for its millions of users. But the seemingly simple plan to combine user data across the company's lineup of services — Gmail, Android, YouTube and others — is generating concern from lawmakers, privacy advocates and legal scholars. For starters, users will not be able to opt out of the update when it goes into effect March 1, 2012. They'll still be able to keep their information separate via roundabout options, but certain services won't work as well.
On a broader scale, some say the change is an example of digital identities becoming the linchpin of revenue growth for Internet goliaths such as Google and Facebook — at the expense of user privacy. Facebook, whose primary asset is the information users share, filed to go public at an estimated valuation of $100 billion. As a publicly traded company, the social network will likely face added pressure to squeeze more digital dollars out of those status updates. "A bad situation for privacy is bound to get much, much worse," said Paul Ohm, an associate professor of law at the University of Colorado School of Law. "It's especially bad because now we've got really vigorous competition between Google and Facebook, and they're competing on our secrets, basically. Whoever can make money out of our secrets is going to win this battle."

Related Links:

- Class Action Against Stanford: **http://www.paloaltoonline.com/news/show_story.php?id=22744**
- Hard Drive Theft - Encrypt :http://aishealth.com/archive/hipaa0911-06
- Dropbox Left User Accounts Unlocked http://www.wired.com/threatlevel/2011/06/dropbox/
- Google’s Privacy Policy http://www.denverpost.com/business/ci_19907563#ixzz1ljR2HuCT

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