Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

March 2011 - Issue 17

What's Inside?

Securing your Smart Phone and its Contents

As we increasingly rely on our phones as an extension of our computers, a substantial amount of personal and business information is stored on them. While the phones themselves are desirable targets for the resale value, the information stored on the phone may prove even more valuable to the thief. As with your computer, the most basic thing you can do to protect your data is to use a password. Imagine if your phone was stolen today and it was not password protected. The thief can look at ALL of your email, texts, contacts' phone numbers, photos, etc., both work-related and personal. Do you have confidential information in your email or stored on your phone that you would not want others to see? The thief can also easily reply to your emails and even post to your Facebook page.

The first step in protecting your device is to implement the use of a password and to set the device to lock after not being used for a period of time. This is similar to a password protected screen saver on your workstation which activates after a certain period of inactivity. Once your phone is equipped with a password, most smart phones can be set to automatically erase your phone's data if the wrong password is entered too many times. Be sure to provide yourself with adequate attempts to enter your password so you do not lock yourself out and automatically erase all of the data on the device. Using this password and lock feature protects the information on the device from being compromised.

There are also tools to find your phone, erase the memory, lock the device, and even display a message when you're not in possession of the device. There are apps (some free, some paid) that perform these functions, including Apple's Find my iPhone, Android's Where's My Android, and Blackberry's Find My Phone – but the key to using these tools is setting them up BEFORE your phone is lost or stolen.

For additional tips and information regarding what to do if your device is lost or stolen, please visit the OHPS website below.

Related Links

- **Protect the Data on your Smart Phone:** http://www.med.miami.edu/hipaa/public/x468.xml

Frequently Asked Question

Q: Am I required to renew my Privacy and Security Awareness Training?

A: All medical school faculty and staff are required to renew mandatory awareness training, as mandated Spring 2009. Faculty and staff will begin receiving notifications shortly from the ULearn system advising of the need to renew this mandatory training requirement.

Have a Question?

hipaaprivacy@med.miami.edu

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

Massachusetts General Hospital Settles Potential HIPAA Violations

On February 14, the U.S. Department of Health and Human Services Office for Civil Rights entered into a Resolution Agreement with The General Hospital Corporation and Massachusetts General Physicians Organization, Inc., (Mass General) to settle potential violations of the HIPAA Privacy and Security Rules. In the agreement, Mass General agrees to pay $1,000,000 and enter into a Corrective Action Plan to implement policies and procedures to safeguard the privacy of its patients. "We hope the healthcare industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information," said OCR Director Georgina Verdugo.

OCR opened its investigation of Mass General after a complaint was filed by a patient whose PHI was lost on March 9, 2009. OCR's investigation indicated that Mass General failed to implement reasonable, appropriate safeguards to protect the privacy of PHI when removed from Mass General's premises. The impermissible disclosure of PHI involved the loss of documents consisting of a patient schedule containing names and medical record numbers for a group of 192 patients, including patients with HIV/AIDS. These documents were lost on March 9, 2009, when a Mass General employee, while commuting to work, left the documents on the subway train that were never recovered.

Related Links

- **Mass General @ BusinessWire:**
http://www.businesswire.com/news/home/20110224006491/en/Massachusetts-General-Hospital-Settles-Potential-HIPAA-Violations

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

Cignet faces $4.3 Million Penalty for Violations of HIPAA Privacy Rule

On February 4, the U.S. Department of Health and Human Services Office for Civil Rights (OCR) imposed a civil monetary penalty of $4.3 million on Cignet Health for violations of the HIPAA Privacy Rule. The OCR investigation began in response to complaints filed by Cignet patients attempting to access their medical records. Part of the penalty – $1.3 million – was imposed for denying 41 patients access to their medical records when requested between September 2008 and October 2009.

An additional $3 million in penalties was assessed against Cignet for its profound failure to cooperate during the agency's investigation. Specifically, OCR found that Cignet did not cooperate with OCR's investigations into the complaints and failed to respond to OCR's demands to produce the records, including failure to respond to a subpoena. OCR found that Cignet's failure to comply with the Privacy Rule and its refusal to cooperate with the investigation amounted to willful neglect, which appears to have led to the imposition of the maximum penalties permitted by law.

Related Links

- **Cignet $4.3 Million Penalty @ HHS:** http://www.hhs.gov/news/press/2011pres/02/20110222a.html

PRIVACY & SECURITY NEWS

National Coordinator for Health Information Technology Highlights Privacy Issues

As he prepares to step down as leader of the Office of the National Coordinator for Health Information Technology, David Blumenthal is calling for stepped-up efforts to protect the privacy of patient information, especially as more electronic health records are created and exchanged. "ONC will be concentrating on creating conditions of trust and interoperability that are essential for health information exchange," Blumenthal said in his keynote speech at the recent Healthcare Information and Management Systems Society (HIMSS) Conference in Orlando. A key priority, he said, is "to assure the public that privacy and security is ever-present on our minds and can be provided in the context of health information exchange." Blumenthal had a message for his successor and the team at ONC: "My hope is that the department will take on comprehensively the privacy and security needs to ensure system interoperability over the next several months."

Healthcare Fraud 'Most Wanted' List Posted

Federal authorities have created a "Most Wanted Fugitives List" of 10 suspects sought on charges of submitting over $124 million worth of fraudulent claims to Medicare and Medicaid. The Department of Health and Human Services' Office of the Inspector General has created the list to enlist the public's assistance in tracking down those suspected of fraud. Much like the FBI's "most wanted" lists that are familiar on the walls of post offices, the new online fugitives list includes photos and profiles of those sought, along with a detailed description of their cases. Inspector General Daniel Levinson says his office is seeking a total of 170 fugitives.

Among those on the "Most Wanted" list are:

- Carlos, Luis, and Jose Benitez, brothers accused of submitting $110 million in fraudulent claims to Medicare from their Miami-area HIV infusion clinics
- Susan Bendigo, accused of collecting $10 million in fraudulent claims from the California Medicaid program for home health services provided by unlicensed, rather than licensed nurses
- Leonard Nwafor, who is alleged to have collected, with his co-conspirators, $525,000 in fraudulent Medicare claims for durable medical equipment, including motorized wheelchairs

Health Breach Tally Hits 6.5 Million

The federal list of major health information breaches now includes at least 240 incidents affecting no fewer than 6.5 million individuals. That number soon could grow substantially as a result of incidents that made headlines recently. Not yet included is a health information breach at New York City Health and Hospitals Corp. that may have affected as many as 1.7 million. That incident involved the theft of backup tapes from an unlocked, unattended truck. Also not included is a breach that stemmed from a stolen computer at St. Francis Health System in Oklahoma, affecting 84,000. Since January 21, 15 incidents affecting a total of 457,000 have been added to the official tally. Roughly 22% of all incidents on the list involve business associates, and more than half involve the theft or loss of computer devices. The two most significant breaches added to the tally in recent weeks involved hacking incidents at clinics:

- Seacoast Radiology in New Hampshire reported an incident that affected 231,000 people and involved hackers using a server to gain bandwidth to play a video game
- Ankle & Foot Center of Tampa reported a hacking incident that affected 156,000. A server containing its practice management system was accessed

Related Links

- **Privacy Issues @ Healthcare Info Security:** http://www.healthcareinfosecurity.com/articles.php?art_id=3376
- **Most Wanted List @ HHS Office of the Inspector General:** http://oig.hhs.gov/fugitives
- **Breaches Affecting 500 or More @ HHS:** http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.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