Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

July 2010 - Issue 14

What's Inside?

Always Encrypt Sensitive Information On Mobile Devices

The new HITECH (Health Information Technology for Economic and Clinical Health) regulation has raised the stakes for healthcare breaches and notification obligations. The act requires organizations to provide notification following a breach of unsecured protected health information (PHI). Unsecured PHI is defined as PHI that is not secured through the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals. What does that mean? In a nutshell, it means the use of encryption.

The most effective way to secure sensitive information is not to store it on mobile devices. Ideally, sensitive information should only be stored on authorized University servers and accessed remotely using secure communication techniques provided by authorized University IT resources. However, University business requirements may sometimes justify storing restricted information on mobile devices. In those limited cases, users must obtain permission from appropriate University management and ensure that reasonable steps are taken to keep the University's sensitive information private and secure.

Mobile storage devices are subject to one principal risk — theft or loss — and secondly, unauthorized access or copying. Assuming that there is a valid and approved business reason for such storage, the active protection must be the use of encryption to protect data stored on the device from unauthorized access. Contact your IT support group for help with encryption and other security measures for your mobile device.

If an **unencrypted** mobile storage device that contains personally identifiable information is lost or stolen, we are required to notify each and every identifiable individual. Depending on the data elements included, the breach triggers either a 45-day notification by State of Florida law or a 60-day notification by Federal law. Please see the Privacy and Security News section on the next page.

All losses/thefts of unsecured health and other personally identifiable information must be reported to the Office of HIPAA Privacy & Security (305-243-5000) immediately upon discovery. The Security Incident Report Form must be completed and either emailed to hipaaprivacy@med.miami.edu or faxed to 305-243-7487.

Related Links

- **Protecting Sensitive Data:** http://www.med.miami.edu/hipaa/public/x349.xml
- **HSA 6.12 Security Incident Report Form:** http://www.med.miami.edu/hipaa/private/documents/hsa6.12incidentreportform.pdf

Frequently Asked Questions

Q: Can I let a coworker access a University computer system with my username and password?

A: Employees are provided a unique username and password for access to University of Miami systems. Access to such systems is governed by the Computer Use and Confidentiality Policy/Agreement and the HIPAA Confidentiality Agreement that employees sign upon joining the medical center. See these agreements and policies at http://www.med.miami.edu/hipaa/public/x372.xml.

It is important to remember that you are responsible for any and all actions taken using your username and password. Therefore, you should never share your username and password with anyone. Also, you should not log into a system and allow others to use your access.

If you suspect your password has been compromised, change it immediately. Audit trails are maintained that track user access to systems. Your access should always be for a valid work-related reason.

Information security and data protection is everyone's responsibility. Please do your part in protecting our institutional assets.

Have a Question?

hipaaprivacy@med.miami.edu

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

Moving? Don't Abandon Sensitive Information

Unsecured PHI and other sensitive information comes in many forms: paper, unencrypted mobile devices, computers, printers, and other multi-function devices.

PAPER: If you are moving your office and need to purge your paper files containing medical or other sensitive information such as Human Resource files, applicant information, billing records, lab reports, images, computer printouts, etc., do not simply leave them in the space being vacated. Contact the **Division of Environmental Services** (Frances Kaniewski, fkaniews@med.miami.edu) for the secure disposal of this information. Medical records and other sensitive information should not be left in unsecured rooms or other insecure areas. Only authorized personnel should have access to such information.

(continued on next page)

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

(continued) Moving? Don't Abandon Sensitive Information

If you are moving boxes containing sensitive information, the information in the boxes should be logged and inventoried. Each box should be numbered and labeled. Records should never be left unattended, even temporarily, including on pavements, in front of buildings, or in hallways. An administrator should supervise all aspects of a move to ensure that the movers are aware of exactly what needs to be transported and proper, secure handling of sensitive information at all times. Once the records have been moved to the new location, immediately make sure all items are accounted for and store the information securely.

To discard electronic media and devices such as computers, biomedical devices, USB drives, CDs, tapes, printers, fax machines, etc., contact **Surplus Property and Storage** at 305-243-9696. Do not leave such devices in regular trash. These items may contain sensitive information that could be used by criminals for identity theft, fraudulent billing, or other activities.

Should there be an incident where records or other sensitive information is lost or stolen, please notify the Security Office at 305-243-6280, ext. 5, and the Office of HIPAA Privacy & Security as soon as possible. The Security Incident Report Form must be completed and either emailed to hipaaprivacy@med.miami.edu or faxed to 305-243-7487.

Related Links

- **Division of Environmental Services:** http://facilities.med.miami.edu/x34.xml
- **Surplus Property and Storage:** http://facilities.med.miami.edu/x39.xml
- **Security Office:** http://ummcsd.med.miami.edu/SECURITY/security.htm
- **HSA 6.12 Security Incident Report Form:** http://www.med.miami.edu/hipaa/private/documents/hsa6.12incidentreportform.pdf

Privacy & Security News

PACS User Accounts Compromised

Griffin Hospital officials suspect that a radiologist, who had been terminated, used passwords of other employees to access patients' radiology reports. The patients received unsolicited phone calls offering professional services at another hospital. Griffin began investigating when patients called about the inquiries. The information was gleaned from PACS, a digital image archiving system that maintains patients' radiological images. It allows authorized physicians to study the images through a secured network in the hospital and remote locations outside of the hospital.

It appears that the physician downloaded image files of 339 out of the 957 patients listed in the PACS directory, hospital officials said. Griffin President Patrick Charmel said the breach, "appears to have been a deliberate intrusion into Griffin's Digital Picture Archiving and Communication System to view patient radiology reports." The hospital notified affected patients, completed an audit and investigation, and is taking steps to improve the security of patient information.

Lost USB Flash Drive

Our Lady of Peace, a psychiatric hospital in Louisville, is notifying 24,600 individuals after a USB flash drive containing unencrypted patient data was lost. A notice of the incident is published on the site of corporate parent Jewish Hospital & St. Mary's Healthcare. The hospital ran a legal advertisement notifying the public in the *Courier-Journal*, Louisville's largest newspaper. Our Lady of Peace is now re-educating employees on ways to protect patient information, implementing encryption technology, and disciplining an undisclosed number of employees, according to a media statement.

Patient Information Stolen from Employee's Car

Paper records with names and Social Security numbers of 554 patients of Wake Forest University Baptist Medical Center were stolen from an employee's car parked at an off-campus outpatient clinic. All affected patients were notified by mail, and Wake Forest Baptist will maintain a phone hotline and has arranged for professional monitoring of financial and credit-related activity that could indicate malicious use of the information. Chief Privacy Officer J.T. Moser said, "our intention now is to prevent any harm to these patients as a result of the theft, and to take steps to reduce the likelihood that this kind of loss will happen again."

ID Theft Ring Stole Records from Physicians Group

Chicago authorities broke up an identity theft ring that stole personal information from patient files while on night shift duty at the Northwestern Medical Faculty Foundation. Cook County Sheriff Tom Dart said the "well-executed" scheme was busted as a result of "Operation Quick Charge," a five-month investigation headed by the sheriff's financial crimes unit with assistance from the U.S. Postal Inspection Service and multiple suburban police departments. Investigators began noticing that many of the victims saw doctors on floors 19-21 of the medical facility and narrowed the search down to the janitor assigned to those floors. The Northwestern Medical Faculty Foundation has set up a hotline for patients to call. "This is another example of why all of us need to be concerned about identity theft," Dart said.

Related Links

- **PACS @ NBC Connecticut:** http://www.nbcconnecticut.com/news/local-beat/Griffin-Hospital-957-patients-affected-in-breach-89416747.html
- **Flash Drive @ Information Management:** http://www.information-management.com/news/data_breach_healthcare_security-10017797-1.html
- **Information Stolen from Car @ Wake Forest Baptist:** http://www.wfubmc.edu/AboutUs/NewsArticle.aspx?id=29701
- **ID Theft Ring @ UPI:** http://www.upi.com/Top_News/US/2010/03/26/ID-thieves-used-medical-patients-files/UPI-84291269610340

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