Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

February 2011 - Issue 16

What's Inside?

Best Practices for Use of Portable Storage Devices

With the proliferation of data, many people are requesting portable storage devices such as USB hard and flash drives. These devices now offer extremely large capacities at affordable prices, but the use of these drives is not without risks. Mobile storage devices are subject to one principal risk — theft/loss — and secondly, unauthorized access or copying. A tiny USB flash drive can hold hundreds of thousands of records. Similar paper storage would require thousands of boxes. How easy is it to lose one USB drive compared to thousands of boxes?

This demonstrates the absolute necessity for caution with any type of sensitive information such as protected health information, personally identifiable information, internal business plans, non-public financial data, and any type of information not for release to the public. Inappropriate access or loss of such information can lead to lasting damage to the University's reputation as well as multiple expenses including fines, legal costs, credit monitoring costs, notification fees, etc.

The most effective way to secure sensitive information is NOT to store it on mobile devices. Ideally, sensitive data should only be stored on authorized University servers and accessed remotely using secure communication techniques provided by authorized University IT resources. If you need additional network storage, please request it from your administrator and/or IT support. However, University business needs may sometimes require use of mobile storage. In these limited cases, users must obtain permission from appropriate University management and ensure that reasonable steps are taken to keep the University's sensitive data private and secure.

Assuming that there is a VALID and APPROVED business need for such storage, the active protection must be the use of a recognized encryption feature to protect sensitive data stored on the device from unauthorized access. Drive manufacturers have released versions of USB drives with encryption features. We only recommend purchasing such versions and making sure the encryption feature is enabled before use. Please contact your IT support group for help in purchasing appropriate USB hard and flash drives and ensuring encryption is enabled.

In most cases, encryption requires the use of a password. If you write this information on the drive or otherwise make it easily accessible (e.g., a Post-It note), you have defeated even the most advanced encryption algorithm. Encryption is not a substitute for common sense. Store only the minimum data necessary to satisfy the business function and only for the time needed to perform the business function. Do not "forget" about the device and/or information!

Do not leave devices in open or unlocked areas such as your car or unsecured workplace. USB flash drives should generally be kept on your person, for example, on a keychain. Mobile hard drives should never be left in public places or locations susceptible to theft, such as the back seat of your car (even covered) or unsecured office. Nevertheless, even with the best physical security measures, devices can still disappear. A security concept called defense in depth means applying security in layers. If one layer of security is breached, another may still serve to protect the information. To illustrate, 1) do not store sensitive information unless there is an unavoidable need, 2) physically secure the device, and 3) encrypt the information.

In the event that such a device containing sensitive information (e.g., patient information, Social Security number, etc.) is lost or stolen, immediately complete the Security Incident Report Form and notify the Office of HIPAA Privacy & Security and the Department of Security.

Finally, be sure to erase all sensitive information on devices before discarding. Simply deleting the files on the device does not completely erase the information. There are proper methods for making sure the information is irretrievably deleted. Again, contact your IT support group for assistance with proper disposal of electronic devices. On a related note, Environmental Services handles secure disposal of magnetic media such as CDs, audio and video tapes, etc. Contact them at 305-243-1052.

You can save yourself and the institution a great deal of grief by proactively taking these safeguards.

Related Links

- **Security Incident Report Form:** http://www.med.miami.edu/hipaa/private/documents/hsa6.12incidentreportform.pdf
- **Environmental Services:** http://facilities.med.miami.edu/x34.xml

Frequently Asked Question

MyUHealthChart.com

Q: Who do I contact for patient questions about MyUHealthChart.com, including how to access the system?

A: Please direct all such requests to AskMyUHealthChart@med.miami.edu.

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

UMC Workers Fired for Violating Patient Privacy After Congresswoman Shooting

Three employees at Tucson's University Medical Center have been fired for violating patient privacy in connection with accessing confidential medical records in the high-profile shooting rampage that killed six people and left Congresswoman Gabrielle Giffords in critical condition, hospital officials said. "The hospital has terminated three clinical support staff members this week for inappropriately accessing confidential electronic medical records, in accordance with UMC's zero-tolerance policy on patient privacy violations," says a statement issued by UMC officials. Hospital officials stressed they are not aware of any confidential patient information being released publicly. "Any potential breaches of patient privacy by UMC staff will be investigated and appropriately addressed," a hospital news release stated.

UNC Cancer Researcher Fights Demotion After Data Breach

A University of North Carolina cancer researcher is fighting a demotion and pay cut she received after a security breach in the medical study she directs. Bonnie Yankaskas, a professor in the Department of Radiology and principal investigator of the Carolina Mammography Registry, was demoted from full professor to associate professor with tenure after one of two servers used by the program was hacked, placing the personal data of more than 100,000 women at risk. In fact, then-interim provost Bruce Carney sent Yankaskas a letter in October 2009 notifying her of the university intent to dismiss her from the faculty because her role in the security breach "constitutes a neglect of duty." Carney also charged that Yankaskas obtained sensitive HIPAA-protected patient data from UNC hospitals without the proper authority, which also rose to the level of neglect of duty. Yankaskas has appealed the demotion to the UNC Board of Trustees.

University of Hawaii Faces Class Action Lawsuit Over Data Breach

When University of Hawaii alumnus Philippe Gross applied for a job at the state Department of Health in February 2010, he was amazed to see four other names associated with his Social Security number. Subsequently, he discovered the unauthorized use of his credit card at nine gas stations in Georgia. Believing the incidents could only be a result of the recent information security breaches at the University of Hawaii, Gross has filed a class-action lawsuit in federal court. The suit targets the University of Hawaii, President M.R.C. Greenwood, Board of Regents Chairman Howard Karr, and Chief Information Officer David Lassner. The University of Hawaii has suffered three major data breaches in the last two years, involving collectively more than 108,000 individuals. The most recent incident involved the posting online of Social Security numbers, grades, birth dates, and other personally identifying information belonging to 40,000 of the University's former students. The exposed student information was available for more than a year before being taken down. The University was informed of the exposed information by an outside entity. UH leadership has said they recognize that "improvements are necessary and that resources must be reallocated to improve IT security." It also recognizes that its decentralized approach is not adequate.

Attorney General Sues WellPoint Over Breach Notification Delay

The Indiana attorney general's office has filed a lawsuit against Indianapolis-based health insurance provider WellPoint for taking months to notify state residents whose personal information was breached. The breach enabled personal health information submitted by consumers to be viewed on the site. Protected information included name, date of birth, Social Security number, telephone number, e-mail address, health and financial information. The lawsuit contends that WellPoint violated state law, which requires breached businesses to notify affected individuals and the AG's office "without reasonable delay," Attorney General Greg Zoeller said in a news release. While the HITECH Act gave state attorneys general authority to enforce HIPAA privacy, security, and breach notification rules, the Indiana action is being taken under authority of a state law requiring disclosure of data breaches "without unreasonable delay."

Zoeller said WellPoint took more than four months to begin notifying customers. After learning of the exposure through media reports, Zoeller's office tried to contact WellPoint and did not receive a response until months later. "The delays in notice to both customers and to the AG's office are considered unreasonable," the news release states. The health insurer is facing at least one other lawsuit over the incident, a class-action complaint filed on behalf of customers whose information was breached. The breach was corrected within 12 hours of receipt of the class action suit, WellPoint later acknowledged in a letter to the Attorney General.

Related Links

- **UMC Workers Fired After Congresswoman Shooting @ GovInfoSecurity.com:** http://www.govinfosecurity.com/articles.php?art_id=3261
- **UNC Researcher Demotion @ The Herald-Sun:** http://www.heraldsun.com/view/full_story/9804450/article-Cancer-researcher-fights-UNC-demotion
- **University of Hawaii Class Action Lawsuit @ Honolulu Star Advertiser:** http://www.staradvertiser.com/news/hawaiinews/20101119_UH_sued_over_data_breach.html
- **Attorney General Sues Wellpoint @ GovInfoSecurity.com:** http://www.govinfosecurity.com/articles.php?art_id=3057

Have a Question?

hipaaprivacy@med.miami.edu

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

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