Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

May 2010 - Issue 13

What's Inside?

New Photocopiers and Multifunction Devices Loaded with Secrets

A recent CBS news investigation revealed that many digital copiers, printers, and multifunction devices (printer/scanner/copiers) had been disposed of without sensitive information being appropriately deleted. Many of these new devices come with internal storage capabilities, such as an internal hard drive or other electronic storage — just like a computer. Depending on how the device is configured, every time you scan, copy, or email a document, an image of the original document may remain in storage on the device. Without any additional protective measures such as encrypting the document while in storage or securely wiping the data, individuals with some technical capability can recover such information. Examples of information recovered from such devices included medical records, Social Security numbers, birth certificates, bank records, income tax forms, and police reports.

At present, the official supplier of printing/copying devices to the University is Ricoh (formerly Lanier). Among the contractual obligations of this particular vendor is the secure handling of all such devices (i.e., they are required to securely wipe all data from such devices returned from the institution). However, there may still be other manufacturers' devices on campus. Such devices should not be disposed of by simply throwing them in the trash. To arrange for the disposal of such University property, contact Surplus at 305-243-9696. Securing sensitive data is a collective responsibility.

Additionally, many people may also have such devices with internal storage capability at home or in home offices. Imagine the kind of information that you have scanned, printed, or copied at home. Then think about how you may have disposed of these devices. You may have sold the device, donated to charity, sent to a recycling center or dumped in the garbage. Recyclers will in most cases not take any responsibility for any data left on devices. Surplus electronics are increasingly being shipped abroad for recycling. It is up to you to ensure that any sensitive data is appropriately erased before you dispose of such devices.

Related Links

- **CBS News:** http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml
- **CBS News Video:** http://www.cbsnews.com/video/watch/?id=6412572n

Frequently Asked Questions

Q: Why do I need to change my password regularly?

A: Passwords are currently the most vulnerable entry-point to our IT resources. By changing your password on a regular basis, you may prevent unauthorized access by someone who has guessed your password. Hackers use automated tools to guess passwords. Use of lower- and uppercase letters, numbers, and symbols increases the difficulty to guess your password. Never share your password. Passwords that are easy to guess provide hackers and other malicious users with an easy means to gain access to our IT systems. If you suspect your password has been compromised, please change it immediately.

Have a Question?

hipaaprivacy@med.miami.edu

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

Impermissible Disclosures

According to the Department of Health and Human Services, a public hospital was cited for impermissibly disclosing health information in response to a subpoena which was not accompanied by a court order. Contrary to the Privacy Rule protections for information sought for administrative or judicial proceedings, the hospital failed to determine that reasonable efforts had been made to insure that the individual whose PHI was being sought, received notice of the request.

We have created tools to assist you in determining whether documents received are compliant and meet the requirements for release. Use the Authorization for 3rd Party Disclosure Checklist to review any non-UM authorizations for release of patient information. For subpoenas, please consult the Subpoena Quick Reference Guide. For additional questions or training, please contact our office.

Related Links

- **Authorization for 3rd Party Disclosure Checklist:** https://www.med.miami.edu/hipaa/private/docments/auth3rdpartydisclosure.pdf
- **Subpoena Quick Reference Guide:** https://www.med.miami.edu/hipaa/private/documents/Subpoena%20Quick%20Reference.pdf

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

FTC to Create Internet Privacy Framework for Social Networking

Amid growing concerns from privacy advocates and legislators alike, the Federal Trade Commission (FTC) plans to create guidelines on Internet privacy to protect consumers from abuse of their personal data by social networking, Internet search and location tracking companies. The announcement came after a call by four senators seeking improved FTC enforcement and rules. "The FTC is examining how social networks collect and share data as part of a project to develop a comprehensive framework governing privacy going forward," said FTC spokeswoman Cecelia Prewett.

Related Links

- **Washington Post:** http://voices.washingtonpost.com/posttech/2010/04/ftc_says_it_is_creating_intern.html

PRIVACY & SECURITY NEWS

BlueCross Computer Theft Costs $7 Million and Climbing

BlueCross BlueShield of Tennessee has spent more than $7 million to respond to the theft last October of computer hard drives from an abandoned office. Officials said the company may have to spend millions more to assess what was in the missing records and to provide identity protection for affected customers. BlueCross already has notified 220,000 customers in Tennessee and other states. Communications Director Roy Vaughn said the company has received 8,728 member calls related to the theft so far, and about 20,500 members of BlueCross plans have taken advantage of the company's offer for free credit monitoring services from Equifax, Kroll, or Lifelock. To comply with last year's HITECH Act, BlueCross must notify attorneys general in 32 states where at least 500 BlueCross members may be affected by the breach.

Judge Rejects Plea for Florida ID Theft Duo

Ruben Rodriguez and Maria Victoria Suarez entered a plea agreement in US District Court for their involvement in a scheme to steal patient records from Jackson Memorial Hospital and sell the data to personal injury lawyers. US District Judge Joan Lenard rejected the plea offer, claiming that the twelve years for Rodriguez and five for Suarez did not match the magnitude of the crime. The duo was also indicted by the US Attorney's office in March after stealing personal privacy data from a local ambulance service, American Medical Response, and selling the information.

Prison Sentence Handed Down for HIPAA Violations

A former UCLA School of Medicine researcher was sentenced to four months in prison for illegally viewing the medical files of celebrities and others while employed there. Huping Zhou is the first person ever sent to prison for violating the HIPAA regulations. Zhou pled guilty to accessing patient records more than 300 times in one week. "Healthcare companies have to be very aware of these risks of inappropriate insider access to health information," Wiley Rein partner Kirk Nahra, CIPP, told the Daily Dashboard. "We are seeing problems across a wide range of entities, involving celebrities, personal relationships and more sinister motives, such as identity theft and healthcare fraud."

From School Laptops to a Privacy Uproar

The Lower Merion School District of Ardmore, PA has been sued, accused of spying on students and students' families using the cameras in laptops issued to each high school student. Blake Robbins was accused by a Harriton High School assistant principal of "improper behavior in his home" and shown a photograph taken by his laptop as evidence. District officials have said technical staff remotely activated notebook cameras only as part of efforts to recover lost or stolen computers. The Robbins family has denied that Blake's laptop was reported lost or stolen. The lawsuit accuses Lower Merion of violating the federal Electronic Communications Privacy Act (ECPA) and other federal and state statues, including the Pennsylvania Wiretapping and Electronic Surveillance Act, and of violating Blake Robbins' Fourth Amendment rights. The FBI is investigating, and a U.S. Senate subcommittee hearing on surveillance-law issues related to the allegations will be conducted.

Global Attack Snags Corporate and Personal Data

International hackers broke into computers at more than 2,400 companies and government agencies in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft. The damage from this massive attack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the firm that discovered the breaches, showed that hackers gained access to a wide array of data at 2,411 companies, from credit-card transactions to intellectual property. Among the companies affected were Merck & Co. and Cardinal Health Inc.

Related Links

- **BlueCross @ Chattanooga Times Free Press:** http://www.timesfreepress.com/news/2010/jan/26/bluecross-computer-theft-already-costs-7-million/
- **Plea Rejected @ Infosecurity:** http://www.infosecurity-us.com/view/9399/judge-rejects-plea-for-florida-id-theft-duo
- **Prison Sentence @ NBC LA:** http://www.nbclosangeles.com/news/local-beat/Former-UCLA-Healthcare-Worker-Sentenced-Prison-Snooping-92265634.html
- **School Laptops @ Computerworld:** http://www.computerworld.com/s/article/9175739/Pa._school_district_snapped_thousands_of_student_images_claims_lawyer
- **Global Attack @ The Wall Street Journal:** http://www.wsj.com/article/SB10001424052748704398804575071103834150536.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