Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

April 2010 - Issue 12

What's Inside?

Use of Photographs Without Patient Authorization

We have been advised by the Office of General Counsel that publishing full facial photos of patients being treated in Haiti is a HIPAA violation if these images have been published without a patient authorization or without de-identifying the protected health information. Under the HIPAA regulation (45 CFR 164.514), de-identification requires removal of several identifiers, including but not limited to names, dates of birth, and full face photographic images and any comparable images.

Many may think that HIPAA doesn't apply to the Haiti situation, but the Department of Health and Human Services (HHS) has indicated that the definition of an individual under the privacy regulations does not exclude foreign national beneficiaries. If these images were used without authorization, patients could attempt to sue for violation of their privacy rights or tortuous interference. Please see *Hospital Employees Disciplined for Shark Bite Photos* in the Privacy & Security News section on page 3.

Related Links

- **Office of General Counsel:** http://www.miami.edu/generalcounsel
- **Photo Authorization Form (English)** https://www.med.miami.edu/hipaa/private/documents/D3900055E.pdf
- **Photo Authorization Form (Spanish)** https://www.med.miami.edu/hipaa/private/documents/D3900055S.pdf

Frequently Asked Questions

Q: May I use my access privileges on healthcare information systems to assist my relatives or friends with their appointments?

A: System access is a privilege. As a University employee, you sign a computer use agreement as well as a HIPAA confidentiality agreement. By signing these documents, you acknowledge that the use of the system is solely for the performance of your job. Accessing the accounts of friends, relatives, coworkers, or other individuals is strictly prohibited unless you are specifically required to do so as part of your work-related responsibilities. Do not access any account unless you have a specific job-related need to do so.

Have a Question?

hipaaprivacy@med.miami.edu

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

HITECH Regulations Bring New Penalties

The Department of Health and Human Services (HHS) has issued final regulations for the Health Information Technology for Economic and Clinical Health Act (HITECH) which increases the civil penalties for HIPAA Privacy and Security violations based on a tiered penalty structure. Below are the HITECH penalty structures:

- If the covered entity was unaware or would not have known of the violation by exercising reasonable diligence, the minimum civil penalty is $100 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.
- If the violation was due to reasonable cause and not to willful neglect, the minimum civil penalty is $1,000 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.
- If the violation resulted from willful neglect but is corrected within a 30-day period after discovery, the minimum civil penalty is $10,000 per violation, with a maximum of $50,000, and an overall limit of $1,500,000 for identical violations during the calendar year.
- If the violation is due to willful neglect and is not corrected, the minimum civil penalty is $50,000 per violation, with an overall limit of $1,500,000 for identical violations during the calendar year.

The HITECH Act also authorizes each state attorney general (AG), for the first time, to begin pursuing civil actions for HIPAA privacy and security violations that have threatened or adversely affected a resident of the AG's state. Attorneys' fees are also allowed to be collected by an AG for pursuing civil actions for HIPAA privacy and security violations. The final regulations took effect on November 30, 2009, and apply to violations occurring on or after February 18, 2009.

Related Links

- **Buck Research:** http://www.buckconsultants.com/buckconsultants/Portals/0/Documents/PUBLICATIONS/Newsletters/FYI/2009/FYI-11-18-09a-HHS-Issues-Interim-Final-Regulations-on-Increased-Penalties-for-HIPAA-Violations.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

Request for an Amendment to Medical Records (Attachment 33)

If a patient indicates there is an error in his or her medical record that needs correction, the individual should be provided an Attachment 33, Request for Amendment of Health Information form. The patient should be instructed to send the form to the Office of HIPAA Privacy & Security (OHPS). If the completed form is received by the department, it should be forwarded to OHPS as soon as it is received. All requests are processed by OHPS.

By policy and regulation, we must respond to these requests within 30 days of receipt. For more information, please refer to the University's HIPAA Policy for Patient Amendment of Designated Record Sets or call OHPS for assistance.

Related Links

- **Attachment 33:** https://www.med.miami.edu/hipaa/private/documents/D3900031E.pdf
- **Patient Amendment of Designated Record Sets:** https://www.med.miami.edu/hipaa/private/documents/ppp_amendment.pdf

Twitter, HIPAA, & Free Speech Clash at Mississippi Medical Center

A snarky tweet has sparked a HIPAA compliance and public relations mess at Mississippi's University Medical Center. As a result, the administrative assistant who posted the tweet is out of a job.

The controversy began when the governor of Mississippi posted this tweet on his Twitter page: "Glad the Legislature recognizes our dire fiscal situation. Look forward to hearing their ideas on how to trim expenses."

Jennifer Carter, the UMC administrative assistant replied publicly: "Schedule regular medical exams like everyone else instead of paying UMC employees over time to do it when clinics are usually closed." She heard that a few years ago, the governor had come into UMC for a physical over a weekend and the clinic had to be staffed up with 15-20 workers just for his visit.

Two days later, Carter was in UMC's compliance office for violating HIPAA's privacy provisions. The Compliance Department told her the governor's office tracked her down and told them to deal with her, according to local news station WLBT.

Carter says she was suspended without pay for three days and "strongly encouraged to resign," which she did.

A healthcare lawyer uninvolved with either side of the incident told the TV station that even the protected health information of public officials is protected by HIPAA. UMC was investigating the incident, but now says the matter was closed with Carter's resignation.

Related Links

- **WLBT:** http://www.wlbt.com/Global/story.asp?S=11713360

Tax Season Approaches: Tax Refund & Stimulus Payment Scams

Fraudulent emails are again promising tax refunds or stimulus payments. These scams, called *phishing attacks*, pretend to come from legitimate Internal Revenue Service (IRS) email accounts. The emails tell users to follow a link to a website or to complete an attached document, requesting personal information that may include credit card numbers, bank account numbers, etc. Criminals use the information to empty the victims' bank accounts, run up credit card charges, and apply for loans or credit in the victims' names. Both the website and document have the appearance of genuine IRS material. Some fake stimulus payment sites try to look authentic with pictures of the president, the White House, Congress, the American flag, etc.

Remember, the IRS does not initiate taxpayer communications through email. The Federal Trade Commission (FTC) warns that the promise of stimulus money in return for a fee or financial information is always a scam.

The IRS never requests detailed personal information through email, nor do they request PINs, passwords, or access information for credit cards, banks, or other financial accounts.

If you receive an email claiming to be from the IRS or directing you to an IRS site, do not reply, do not open any attachments and do not click any links.

Related Links

- **Beware of Phishing:** http://www.med.miami.edu/hipaa/public/x249.xml
- **IRS:** http://www.irs.gov/privacy/article/0,,id=179820,00.html?portlet=1

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

Hospital Employees Disciplined for Shark Bite Photos

Several employees at a Florida hospital have been disciplined after taking unauthorized cell phone pictures of a shark attack victim. Hospital officials are Martin Memorial Medical Center launched an investigation after learning that employees may have violated patient privacy laws. Officials are asking anyone with copies of the photos to destroy them. Disciplinary actions have included written warnings, suspensions, and demotions, though nobody was fired. "Ultimately, we have determined that these inappropriate actions were taken by good people who exercised poor judgment," the hospital said in a statement. It has started a re-education and re-training program on patient privacy laws and cell phone usage for hospital employees.

UNC Breach Exposes 163,000 to Identity Theft

University of North Carolina at Chapel Hill has disclosed a data breach of one of its servers that exposed the identities of 163,000 women. The breach could date as far back as 2007, and has exposed Social Security numbers, dates of birth, and other sensitive information about study participants. The women were participating in a mammography study conducted by the UNC School of Medicine.

The exposed information was on one of two servers that housed data on more than 662,000 women. The data was being collected as part of the Carolina Mammography Registry, a project that compiles and analyzes mammography results submitted by radiologists in North Carolina. UNC officials are sending out breach notification letters to all 236,000 study participants. The university began phasing out Social Security numbers as patient identification codes several years ago, according to the report. The university said it has also "tightened" its reporting system for the project.

Woman Sentenced in Johns Hopkins Employee Breach

A woman who worked as a patient services coordinator for Johns Hopkins Medicine has been sentenced to 18 months in prison for stealing patient information. The thirty-one-year-old woman of Baltimore was also ordered to pay more than $200,000 in restitution. According to her plea agreement and court documents, from August 2005 to April 2007, the woman provided a conspirator with Social Security numbers, names, addresses, date of birth, telephone numbers, parents' names and medical insurance information of more than 100 current and former patients of Johns Hopkins. That information was used to apply for credit cards.

Malware Opens Door to Possible Information Exposure at Penn State

A computer in the Penn State Dickinson School of Law that contained 261 Social Security numbers from an archived class list was found to be infected with malware that enabled it to communicate with an unauthorized computer outside the network. The computer was taken offline as soon as the university became aware of the malicious software installed . Although it cannot be determined with certainty that any data was pulled from the computer by the infectious software, the university's policy is to notify individuals who may have been affected. Penn State is notifying those involved via letters that will include contact information should recipients have further questions.

Related Links

- **Martin Memorial @ TCPalm.com:** http://www.tcpalm.com/news/2010/feb/26/medical-ethicist-martin-memorial-needs-to-be
- **UNC @ SearchSecurity.com:** http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1369651,00.html
- **Johns Hopkins @ Dept. of Justice:** http://www.justice.gov/usao/md/Public-Affairs/press_releases/press08/HospitalEmployeeSentencedforStealingPatientInformationForFraudScheme.html
- **Penn State @ Penn State Live:** http://live.psu.edu/story/43583

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