Privacy & Data Protection Update

Newsletter of the Office of HIPAA Privacy & Security

Respecting Patient Privacy, Building Patient Trust!

December 2013 - Issue 27

What's Inside?

Ransomware

Imagine you are working on your computer and suddenly you see a message telling you that your personal files have been encrypted and will not be accessible to you unless you pay a fee. This is known as Ransomware. It's a type of malware that restricts access to the infected computer system and demands payment before the restriction is removed. There are two types of Ransomware. The type illustrated above is known as encryption ransomware. But not all of them encrypt your data. Non-encryption ransomware for example can stop a victim from using their web browser until they pay the ransom.

One version of ransonware is called CryptoLocker. It targets several versions of Windows including Windows XP, Vista, Windows 7 and 8. It searches for images, word documents, spreadsheets, presentations, videos, databases and numerous other file types. Once personal files have been encrypted it will display the ransom message with a count down. One version of CryptoLocker gives the victim 72 hours or 3 days to pay $300 (times and amounts can vary) so that the files can be decrypted.

CryptoLocker is being spread though phishing emails containing malicious attachments. One version of the email mimics legitimate companies such as FedEx and UPS tracking notices. The attached file looks like a pdf but it is actually an .exe file. The malware can encrypt files contained in local drives, USB Drives, external hard drives and network files shares.

Frequently Asked Question

Q: What should be done with the completed HIPAA request/forms?

A: All HIPAA related attachments such as Request for Access to Health Information, Authorization for 3rd Party Disclosure, & Accounting for Disclosures should be sent to the Office of HIPAA Privacy & Security for scanning into the central repository. You may also keep a copy in the records. For further information, please contact the Office of HIPAA Privacy & Security at 305-243-5000.

Have a Question?

hipaaprivacy@med.miami.edu

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

The CryptoLocker hackers have made it hard for law enforcement to track them because they continue to change the servers where CryptoLocker is being hosted. An anti-virus company called Bitdefender Labs found that during one week CryptoLocker servers "hopped" to several countries including Russia, Germany, Kazakhstan and the Ukraine. They also found that in one week more than 12,000 computers were infected with CrytoLocker, with most of them being in the United States. For the full story please go to http://privacyoffice.med.miami.edu/awareness/tips/ransomware-what-is-your-personal-data-worth

Safeguarding Patient Information

Sensitive information on paper is the same as sensitive information on a computer. Both need to be protected from unauthorized access or disclosure and should be treated with caution and discretion.

Recommended safeguards for paper records include:

- Medical and other sensitive records should not be left in an unlocked room or insecure area. Only authorized personnel should have access.
- All boxes containing medical records should be numbered and appropriately labeled so as not to misplace them.
- Records should never be left unattended, even temporarily, including on pavements or in front of buildings.
- There should be a tracking or logging process surrounding the use, transport, and storage of paper records in order to identify the user as well as the location of the record. Each box should be numbered and labeled.
- An administrator should supervise all aspects of a move to ensure proper, secure handling of sensitive information at all times and that the movers are aware of exactly what needs to be transported. Once the records have been moved to the new location, immediately make sure all items are accounted for and store the information securely. The University has contracted with Iron Mountain for secure off-site storage of records. Please contact Records Management for further information.

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.privacyoffice.med.miami.edu
Phone: 305-243-5000
Fax: 305-243-7487

PRIVACY & SECURITY NEWS

Cedars-Sinai Medical Center Latest To Boot Nosy Workers

The latest case of celebrity records snooping involves five employees and a research assistant from Cedars-Sinai Medical Center. According to the Los Angeles Times, the employees were fired after 14 patient records were accessed inappropriately from June 18th to June 28th. Cedar-Sinai isn't the first hospital to struggle with celebrity records snooping incidents. In 2009, UCLA Health System entered a resolution agreement due to employees snooping the records of two celebrities. Some hospitals have even taken proactive measures to protect privacy. Beth Israel Deaconess Medical Center in Boston posted the following message on their intranet "Violation of these [privacy] regulations and policies will lead to disciplinary action up to and including termination of employees. This was after admitting victims in the Boston Marathon bombing.

WellPoint Slapped With $1.7M Fine for HIPAA Violations

Insurance provider WellPoint will pay a fine of $1.7 million due to HIPAA violations. The company left the names, social security numbers and personal health information of over 600,000 people accessible through the internet. The information was available from October 2009 till March 2010. The Office of Civil Rights (OCR) said that this was due to not establishing the proper administrative and technical safeguards in the online application database. The company has notified the affected individuals and have provided credit monitoring and identity theft insurance.

Seven-Figure HIPAA Settlement Prompted by Photocopier Breach

Affinity Health plan, Inc. reached a settlement with the Office of Civil Rights (OCR) of over $1.2 million for HIPAA violations. The company failed to erase the personal health information (PHI) of more than 300,000 individuals when it returned several photocopiers to a leasing company. Affinity failed to include the data stored on photocopier hard drives as part of their HIPAA Security policies and procedures. OCR imposed a Resolution Agreement and Corrective Action where Affinity will retrieve the photocopier hard drives and erase the PHI stored in them.

Behemoth Breach Sounds Alarm For $4M

Advocate Health System announced the theft of four unencrypted computers compromising the protected health information and social security numbers of over 4 million patients. This is the second largest HIPAA violation ever reported. The theft occurred on July 15th at one of its administrative buildings. The computers contained patient names, addresses, dates of birth, social security numbers and clinical information. Local law enforcement has been contacted but has not been able to locate the computers. To prevent this from reoccurring they have enhanced their security measures which include adding a 24/7 physical security presence at the location where the burglary took place.

International Hackers Stole Millions in Largest U.S. Hacking Scheme

Five men from Russia and the Ukraine are involved in what is being known as the largest hacking and data-breach scheme ever prosecuted in the United States. The men infiltrated the world's largest financial institutions and businesses including Dow Jones, NASDAQ, and 17 major retailers. Between 2005 and 2012, the men stole approximately 160 million credit and debit card numbers from these institutions. Three corporate victims have already reported losses of over $300 million. The five men are accused for uploading malware to the companies' computer systems. Through those programs they were able to take information and resell them around the world. The stolen credit card information was put into the magnetic strip of plastic cards and used to withdraw money from ATMs or to buy goods. By doing this, they are able to "cash out" millions of dollars in just a few hours.

Related Links

- **Cedars-Sinai Medical Center Latest To Boot Nosy Workers:** http://www.healthcareinfosecurity.com/blogs/more-celebrity-records-snoopers-fired-p-1513?rf=2013-07-16-
- **WellPoint Slapped With $1.7M Fine for HIPAA Violations:** http://www.clinical-innovation.com/topics/privacy-security/wellpoint-slapped-17m-fine-hipaa-violations
- **Seven-Figure HIPAA Settlement Prompted by Photocopier Breach:** http://www.healthlawpolicymatters.com/2013/08/15/seven-figure-hipaa-settlement-prompted-by-photocopier-breach/
- **Behemoth Breach Sounds Alarm For 4M:** http://www.healthcareitnews.com/news/behemoth-hipaa-breach-sounds-alarms
- **International Hackers Stole Millions in Largest U.S. Hacking Scheme:** http://www.nj.com/essex/index.ssf/2013/07/five_hackers_stole_160_million_credit_and_debit_card_numbers_through_international_attacks_federal_i.html

Office of HIPAA Privacy & Security
Professional Arts Center (PAC), Suite 409 (M-879)
http://www.privacyoffice.med.miami.edu
Phone: 305-243-5000
Fax: 305-243-7487