HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

August 15, 2015

Volume 1, Issue 8

Healthcare IT News

Published on *Healthcare IT News*
(http://www.healthcareitnews.com)

The Seedy Underworld of Medical Data Trafficking

Posted on Jul 08, 2015
By *Chris Bowen, ClearDATA*

As more healthcare organizations are discovering to their woe, having direct access to patients' personal health information puts a giant target on their backs for cyber thieves that traffic in stolen medical records. Medical data breaches are increasing in frequency and scope, with millions of Americans now victims of medical identity theft. Who are the criminals behind this digital era crime wave?

IBM research shows that the vast majority of cybercrime is highly organized and generating unprecedented profits, noting that the largest bank heist in history was $30 million compared to the annual $445 billion cost of cybercrime. Solo cybercriminals are also out there, however. Trend Micro observes that these different classes of criminals also dwell in different forums, with petty thieves showing up in more easily accessed sites, and organized cyber thieves residing in closed forums of their own.

A foray into the online black market for stolen data — and other goods — is a surreal experience. With names like "DamageLab" and "Hell," many forums have the same features of legitimate online shopping sites, from "buy now" buttons to, in an ironic twist, rating systems that score a dealer's trustworthiness.

The product descriptions, on the other hand, make it quickly apparent that the wares for sale are anything but legit. A recent NPR report described a dealer with exceptionally high marks who had a "value pack" of 10 stolen Medicare numbers for sale. The total pack could be had at a cost of 22 bitcoin (the preferred currency of many cyber criminals), which works out to about $4,700.

With sharks clearly circling the perimeters, why is the healthcare industry such a reliable victim? The answer is that much of the IT infrastructure in the healthcare industry is aging and fragmented with inconsistent security—in short, a cyber crook's ideal target. «

A **Security Risk Analysis** is *required* for compliance. Call us today if you have not done yours or have questions about the process.

Rick Boyles
757-333-3299 x200
rick.boyles@computernetworksinc.com

36 months of HIPAA compliance consulting for one low monthly fee. 0% financing for qualified buyers. Call me for details!

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

August 15, 2015

Volume 1, Issue 8

WALL OF SHAME

Wall of Shame now at 143 million breached individuals

HIPAA Secure Now
Posted: 07 Aug 2015 06:29 AM PDT

Hacking and breaches of healthcare data continue to happen. The scale of the breaches are increasing as well. According to an article over at Data Breach Today, 143 million individuals have had their healthcare related information breached. 70% of the 143 million breached records have occurred just in 2015.

Healthcare organizations are not making security of protected health information (PHI) a priority. Many organizations are in denial that they could be a target. But the reality is that PHI is very valuable and cyber criminals want to get their hands on as much PHI as possible. Whether it is 80 million records from Anthem or 10,000 records from a small medical practice, thieves have set their sights on healthcare data.

While hacking and hackers need to be a major concern for healthcare organizations, other types of breaches should be on the radar as well. Lost or stolen laptops and USB drives are a leading cause of breaches. Organizations need to protect information on portable devices. The use of encryption to protect data on portable devices is increasing but still lacking in most organizations.

Healthcare organizations need to worry about HIPAA compliance but they also need to worry about security of the data. HIPAA compliance and data security should go hand in hand but many times organizations are only concerned with the appearance of compliance. They worry about government fines but have little concern for implementing the necessary security safeguards to protect patient information. Until the mindset switches from check-box compliance to securing PHI, the number of breached records will continue to climb. **«**

MISSED BOAT

So, if you have yet to:

- Take protection of PHI seriously
- Conduct a Security Risk Analysis
- Update an existing Security Risk Analysis
- Develop a Culture of Compliance
- Look at HIPAA as a journey
- Document your compliance

You are missing the boat. The Federal Government is about to “break bad” on the medical offices that are failing or refusing to take the HIPAA process seriously.

You must develop a new way of thinking. Compliance with HIPAA is now a part of everyday life and it is not just about having a Notice of Privacy Practices for your Patients to sign every now and again.

You must have Physical, Technical and Administrative safeguards in place, you must have documentation of how you have met these safeguards and you must have an ongoing review process.

Ignoring these HIPAA rules is akin to ignoring the Internal Revenue Services. You can do it, but, when you get caught it is not going to be pretty and it is going to be very expensive.

Do not put your Physician/Owner's business in jeopardy. Talk to us about a Security Risk Analysis today and what you need to do to get and remain compliant. «

Data Breach Costs Staff Member Their Job

On July 24, Advanced Radiology Consultants, LLC, announced a data security event that exposed the data of a small subset of its patients. The breach report submitted to the Department of Health and Human Services' Office for Civil Rights indicates 855 patients have been affected.

The data breach was caused when an employee of the company emailed a list of patients' PHI to a personal email account. The list of data included patient names, telephone numbers, dates of birth, balance information, patient identification numbers, examination results, treatment information, appointment dates and times, appointment notes, referring physician names, insurance provider, and insurance identification numbers.

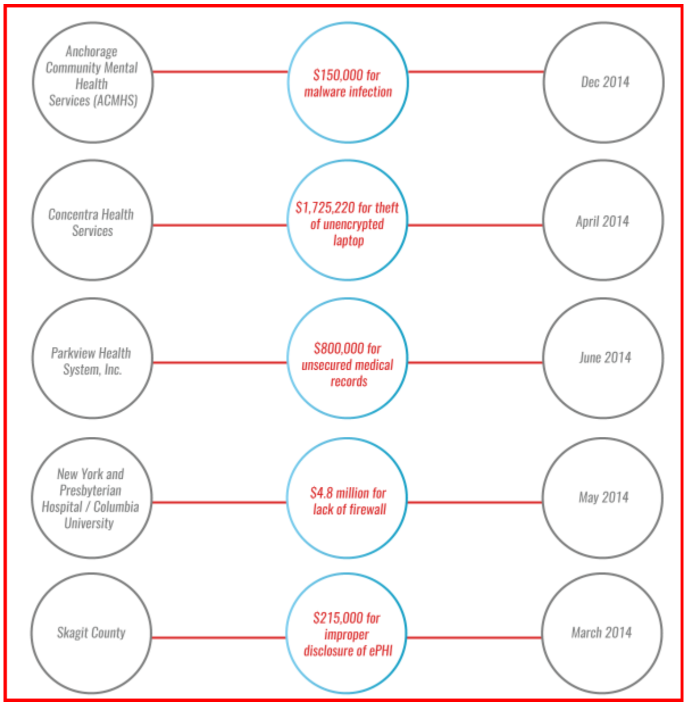
Advanced Radiology Consultants confirmed in a press release that no Social Security numbers, credit card numbers, driver's license numbers or financial account information were included in the email. That said, the information that was copied and emailed outside the healthcare providers' network did contain enough data to enable the employee to file false insurance claims, and potentially commit identity fraud.

No information was provided on the motives behind the sending of the email, although Advanced Radiology Consultants confirmed that the employee's contract was terminated as a result of the data breach, and law enforcement has been alerted to the HIPAA breach. The law enforcement investigation is ongoing.

Upon discovery of the data breach on May 28, 2015, Advanced Radiology Consultants initiated an internal investigation and enlisted the help of a private security firm to conduct a full forensic data analysis. The employee was questioned and instructed to delete the email from her account, which she has confirmed has now been done. She told the company she had not used the data "in an unauthorized manner" and neither did she disclose any information to a third party. «

SAMPLE HIPAA FINES

If you don't think HIPAA violations can happen to you, take a quick look at these fines. Is YOUR Doctor going to be happy paying fines of this magnitude?



Anchorage Community Mental Health Services (ACMHS)	$150,000 for malware infection	Dec 2014
Concentra Health Services	$1,725,220 for theft of unencrypted laptop	April 2014
Parkview Health System, Inc.	$800,000 for unsecured medical records	June 2014
New York and Presbyterian Hospital / Columbia University	$4.8 million for lack of firewall	May 2014
Skagit County	$215,000 for improper disclosure of ePHI	March 2014

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

August 15, 2015

Volume 1, Issue 8

Hackers swipe data of 4.5M at UCLA

The four-hospital UCLA Health System on Friday notified a staggering 4.5 million of its patients that their protected health information and Social Security numbers were compromised following one of the largest HIPAA breaches ever reported.

Despite the cyberattack having occurred nearly a year ago, in September 2014, officials did not notify patients until July 17. UCLA first detected suspicious activity on its networks back in October 2014, according to a company statement.

Social Security numbers, medical diagnoses, diseases, clinical procedures, test results, address and dates of birth were all among the data swiped by hackers in the cyberattack.

"We take this attack on our systems extremely seriously," said James Atkinson, MD, interim associate vice chancellor and president of the UCLA Hospital System, in a July 17 statement. "We sincerely regret any impact this incident may have on those we serve."

UCLA Health System's breach announced today follows a series of similar cyberattacks impacting the healthcare industry in recent months. The Anthem cyberattack reported this February, for instance, compromised the Social Security numbers and personal data of nearly 80 million members and employees. In January this year, hackers also struck Premera Blue Cross, which exposed the financial and medical data of another 11 million members.

To date, the UCLA breach is tied for the fourth largest HIPAA breach ever reported, according to data from the Department of Health and Human Services.

As healthcare security consultant Mac McMillan told Healthcare IT News following the massive Anthem breach, "This should serve as yet another wake up call for those who haven't gotten it yet," he said. "Healthcare is a target."

"In today's security environment, large, high-profile organizations such as UCLA Health are under near-constant attack," UCLA Health officials acknowledged in a statement. Each year, they're able to prevent millions of hacker attempts. But not this time around. In response to the attack, UCLA said it is adding to its internal security team and has enlisted help from outside security firms to help monitor and better protect their network.

This is not the first HIPAA breach for the California-based health system. In 2011, the UCLA hospital system reported a breach after a laptop containing patient medical data was stolen from a former employee's home.

Wake up and smell the coffee folks...get your Security Risk Analysis done, get it documented, fix the problems that you found, then wait a few months and repeat the process. No one is immune. There is PHI in places that you do not believe have PHI, there are staff using work-arounds that expose PHI to others, there are employees who do not understand and sometimes do not care, you have PHI on your Smartphone, at your answering service, with the transcription service...everywhere. Find it. Protect it.