HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

November 17, 2015

Volume 1, Issue 11

It Can Happen To You!

the date, even if you lost it later or changed it, you're done." *Pilot writer Jeff Hampton contributed to this report.*

1,040 Sentara patients told of security breach

NORFOLK

The August theft of two portable hard drives from Sentara Heart Hospital's electrophysiology labs led hospital officials to send letters about a security breach this week to 1,040 patients.

The theft occurred during the weekend of Aug. 14. The patients who were informed had tests in the labs between Sept. 4, 2014, and Aug. 14. The hard drives included birthdates, names, diagnoses, types of procedures and other clinical notes. There were no Social Security numbers or addresses on the hard drives.

Because of the number of patients affected, Sentara is required by federal law to notify patients and the news media and to post a notice on the health system's website.

The theft led to new protocols. Portable hard drives are now secured in a locked drawer at all times.

Patients who have questions or need more help can call 844-322-8235 between 8 a.m. and 6 p.m. and refer to incident No. COE151471.

– *Elizabeth Simpson, The Pilot*

Loaf of Bread

Some of you might not know me from a loaf of bread, so I am going to take a couple of minutes to bring you up to speed:

1997 – 1998	**Medic Computer Systems** Field Engineer
1998 – 2001	**Misys Healthcare (purchased Medic)** Virginia Beach Branch Manager-Field Engineering
2001 – 2004	**Misys Healthcare** Advanced Implementation Services Engineer-1 of 7 in the U.S. charged with successful implementing Misys EMR/EHRs
2004 – 2015	**Founder Computer Networks, Inc.** Healthcare Information Technology Computer Support HIPAA Risk Analyses Disaster Recovery

So, if you do the math, I have been in Healthcare Information Technology for the past 18 years, 11 of them as Owner of my own firm.

If you take a peek around at some of the other IT firms in our area, you will see that they do not specialize in Healthcare IT, that their Owners/Founders do not have a background in Healthcare IT, and consequently do not always understand the challenges presented in Healthcare.

Specializing in a particular vertical market is the same thing that many of your Physicians have done. You have picked a particular field of study and become an expert in that field. So have we.

Looking further into those other IT companies who are "playing" in this space, those firms are your Business Associates (BAs) under HIPAA because they are exposed to Protected Health Information (PHI) when they are on your network or because they store your backup data offsite.

Being the BA of a Medical Practice carries some pretty important duties, the first of which is that **all BAs must be HIPAA compliant**. That means that they are required by Federal Law to have completed a Security Risk Analysis (SRA) just as you are; they are required to develop Polices and Procedures for dealing with PHI, just as you are; and that they are required to train their staff on HIPAA, just as you are.

- Has your Information Technology firm completed the necessary steps to become HIPAA compliant?
- If so, can they offer proof of that compliance?
- If not, why are they in Healthcare IT?

This is a serious concern. The Office for Civil Rights (OCR) plans to do more audits this year. And they have made it known that they are going to ask you for a list of your Business Associates (BAs) when they audit you and then OCR is going to audit the BAs as well. ☸

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

November 17, 2015

Volume 1, Issue 11

SEND ME THE MONEY!

CMS AUDIT REQUIRES RETURN OF $132,000

Last year we quoted a Medical Practice on a HIPAA Security Risk Analysis (SRA). They declined to do the SRA citing cost as the determining factor.

Fast forward 12 months, and the Centers for Medicare and Medicaid Services (CMS) elects to perform a Meaningful Use audit on 3 of the Doctors in the Practice.

I am going to assume that they failed because CMS is asking for all the stimulus money back for 3 of the Doctors. ($44,000 x 3). In additon, they have called us and are now ready to have a Security Risk Analysis done, which we will begin in a few days.

I can tell you that we are not charging $132,000 for a Risk Analysis, so, it probably would have been in their best interests to have completed a Security Risk Analysis **before** CMS came knocking. It would have been even better to have remediated the problems that were discovered during the SRA before CMS showed up at the door.

Your Practice is not immune. Your Practice is not too small to worry about HIPAA. If you look at the monetary settlements, see will see Practices of all shapes and sizes who have been fined for ignoring the law or failing to rise to the appropriate level of care. ☸

You know where to find me:
Rick Boyles
757-333-3299 x200
rick.boyles@computernetworksinc.com

COMPUTER NETWORKS, INC
www.computernetworksinc.com
4992 Euclid Road, Suite 4
Virginia Beach, VA 23462
757-333-3299 • 866-783-5195

NEW! 36 Month HIPAA Compliance Plan

36 months of HIPAA compliance consulting (includes a complete, onsite, Security Risk Analysis with Remediation Plan, quarterly network scans for 3 years, Policy and Procedure templates including guidance on implementing, incident investigation, breach investigations, unlimited HIPAA compliance questions) for one low monthly fee. Ask, call, or email me for details!

PHI is everywhere. Find it. Protect it.

"Organizations must complete a comprehensive Risk Analysis and establish strong Policies and Procedures to protect patients' health information," said OCR Director Jocelyn Samuels. "Further, proper encryption of mobile devices and electronic media reduces the likelihood of a breach of protected health information."

Senators Demand Answers from CMS and OCR About Medical Identity Theft and Fraud

Nov 13, 2015 | HIPAA Journal | No comment | Healthcare Data Privacy, HIPAA Breach News, HIPAA News

Four senators have put their names to a letter sent to Jocelyn Samuels, Director of the Department of Health and Human Services' Office for Civil Rights (OCR), and Centers for Medicare and Medicaid Services (CMS) Acting Administrator Andy Slavitt, requesting answers about the growing issue of medical identity theft.

HIPAA SECURITY BRIEF

By Computer Networks, Inc. November 17, 2015 Volume 1, Issue 11
Serving Hampton Roads since 2004

Sen. Lamar Alexander, R-Tenn., Sen. Patty Murray, D-Wash.; Sen. Orrin Hatch, R-Utah, and Sen. Ron Wyden, D-Ore have signed the letter, which demands answers to nine questions relating to the role the HHS, OCR and CMS play in monitoring and addressing medical fraud and identity theft stemming from healthcare data breaches.

Healthcare data breaches have exposed the Protected Health Information of over 105,000,000 individuals so far this year, and there are still over six weeks of 2015 to go. That figure is certain to rise.

The problem is a growing concern. The total number of breach victims created over the past 6 years stands at 154 million, which equates to close to half the population of the United States. The senators point out that the situation is only likely to get worse.

The victims of these data breaches face an elevated risk of medical identity theft, and many have already suffered losses as a result of having their PHI exposed. In many cases, covered entities provide assistance and offer credit monitoring and identity theft resolution services to breach victims, but not always. That is largely left to the discretion of the covered entity. If assistance is not provided and the victims suffer losses as a result, where can they turn and what can they do to recover those losses?

Medical identity theft is not only an issue for data breach victims. The letter points out that the Medicare/Medicaid programs, which are funded by the taxpayer, have to budget for approximately $98 billion each year to cover the cost of medical identity theft. That figure corresponds to 10% of the programs' annual budgets. All Americans are affected.

Given the huge number of victims of healthcare data breaches, and the cost of dealing with medical identity theft, the senators believe something must be done to address the risk and damage caused. It may not be possible to prevent all data breaches from occurring, but it is possible to provide the victims with support. They certainly need it, but the question is, where should that support be coming from?

The senators want to know what the CMS and HHS is doing to monitor medical identity fraud and whether the CMS and/or the OCR is actually doing anything to track cases of ID theft and fraud, specifically whether the OCR uses the data collected from covered-entities to monitor potential breach victims and find out if their data have in fact been used by criminals. Information has also been requested on the number of cases of medical fraud uncovered, and whether the massive data breaches that have already occurred this year have actually resulted in an increase in ID theft and fraud.

The HIPAA Breach Notification Rule requires covered entities to issue notifications to breach victims. In those letters the covered entity should outline the actions that can be taken to address the risk of ID theft and fraud. However, the senators want to know whether any education materials or help are offered to breach victims by the CMS and OCR in this regard.

With the OCR already stretched, should the responsibility of tracking and monitoring cases of identity theft come under its remit, or should it be concentrating on policing HIPAA Rules more rigorously? If the OCR or the CMS are not monitoring cases of identity theft, then which authorities are?

The answers to these questions should be provide later this month. The senators have requested a response by November 24. ❁

COMPUTER NETWORKS, INC
www.computernetworksinc.com
4992 Euclid Road, Suite 4
Virginia Beach, VA 23462
757-333-3299 • 866-783-5195

HIPAA SECURITY BRIEF

By Computer Networks, Inc.
Serving Hampton Roads since 2004

November 17, 2015

Volume 1, Issue 11

Cryptowall 3.0

So, as I am looking for content to put in this newsletter, we get a call from a client that they cannot open some of their files. We jump onto the network remotely and start looking around. Our logging shows that one of the staff was checking his personal email (Yahoo, MSN, AOL, whatever) on a company computer a little after 5:00 p.m. last night, clicked on a spam email message and managed to infect the network with some ransomware called Cryptowall.

For the uninitiated, ransomware encrypts all your files then demands a ransom payment to give you the key to unlock the files.

Because this happened a little after 5:00 p.m. yesterday and because we did not get a call until 11:30 a.m. today, the encryption ran all night long, encrypting all of the files it could find, including the files on the network servers that are used by the entire staff.

In last month's HIPAA newsletter, I published an article on Phishing that explains what to look for in a spammy email. I guess that memo didn't make it to everyone.

Because encryption encrypts, the only way to get the data back is to restore it from a backup. If you do not have the key, you cannot unlock the encryption door. Now, this Client is pretty smart and they have our latest and greatest Backup and Disaster Recovery appliance on the network, so we make backup copies of their data every hour.

So, we are beginning the file restoration process from a 4:00 p.m. backup from yesterday, which is one hour before the ransomware showed up on the network. Any data entered this morning is going to have to be rekeyed because we are using yesterday's files to put things back together.

Before you ask why didn't this get prevented, the crooks are playing a high stakes game of whack-a-mole. The criminals change things faster than the companies we hire for detection can write new code to prevent viruses, spyware, malware, ransomware from infecting your network. This is known as a zero-day infection because someone has top be the 1st to get infected.

On our client networks we install high-end Unified Threat Management (UTM) firewalls with Intrusion Prevention Software (IPS), Gateway Antivirus, Content Filtering, and Anti-spam in conjunction with a Desktop and Server antivirus that runs and scans in real time all day long, plus updates hourly and deep scans nightly. This is known as layering the defense. Yet, this particular variant of Cryptowall made it through all the barriers we put up because the writer of the virus made enough changes to get it past those defenses from multiple Vendors of both hardware and software.

However, people are going to always be the weakest link in this chain. If the end user had simply ignored this sketchy email, the network would not have gotten infected. That means that you cannot underestimate the need for repeated staff training about not clicking on email attachments unless you are absolutely certain of the origin. That means preventing users from going to questionable websites. That means using the network and the Internet for business purposes only and not checking one's personal email.

This is a high stakes game when it comes to networks that contain PHI. In this case the Patient information was not at risk because this particular attack was some simple extortion for money. But, the next one could be far worse. Put the right tools on your network to minimize risk.