# HIPAA SECURITY BRIEF

**By Computer Networks of Roanoke, Inc.** March 15, 2015 Volume 1, Issue 3
Serving Roanoke and surrounding areas since 2006

## HIPAA THE JOURNEY WITH NO END

If it hasn't already, it will soon become apparent to you that HIPAA compliance is not a "one and done", but, an on-going, perpetual activity for all of us who are required to comply. Covered Entities (CE's) and BA's (Business Associates) all have the same level of responsibility for complying with the law as of September 2013 with the Omnibus changes.

The government has done an awful job of educating all of us as to what we are supposed to be doing and when, not to mention how we should be doing it.

The process frustrated me so much, that I partnered up with a company out of Nevada that has been doing Security Risk Assessments (SRA's) for a number of years to educate us on how to perform an SRA.

Now, we are able to offer you a Security Risk Analysis service where we come onsite, perform the Security Risk Analysis (as required by HIPAA and by Meaningful Use), work with you on getting your Policies and Procedures in place, along with your Contingency Operations (Disaster Recovery) Plan, answer all of your HIPAA questions and give you guidance on the remediation of any issues found (another HIPAA requirement).

Once your first **good** SRA is completed, and you have overcome the hurdles of remediation and received first-rate advice on compliance, then you can move into "maintenance" mode where all you have to do is review your Policies and Procedures regularly and upgrade your Risk Analysis annually (Meaningful Use). This phase is much easier than getting "over the hump" of doing that first real Security Risk Analysis.

If you are stuck at the "hump" give us a call and we can prepare a Proposal to get you to that maintenance mode as quickly as possible.

Our services will get you going in the right direction, and bring some comfort to you in knowing that you have experts guiding you on your way.

Be wary of the companies out there claiming to make you "HIPAA compliant". It is impossible for a 3rd party to do that. You may make your organization compliant, but, that compliance is a snapshot in time. The first staffer that does something without thinking, can compromise all of that hard earned compliance. Your best bet is to begin by fostering a culture of security in your Practice. By thinking about every action from a security standpoint (will this possibly allow data to leak out of my organization?) you will then achieve compliance as a by-product of that security posture. ❖

# HIPAA SECURITY BRIEF

**By Computer Networks of Roanoke, Inc.** March 15, 2015 Volume 1, Issue 3
Serving Roanoke and surrounding areas since 2006

## Mini Audit

(See If You Pass)

1. Do you think you are capable of passing a HIPAA audit?
2. Do you think your data security meets HIPAA's requirements?
3. May I please see your HIPAA Risk Analysis?
4. May I please see the documentation you have to show you have managed your risks?
5. May I please see your written password policies?
6. How many workforce members do you have?
7. May I please see your staff's HIPAA training records, including that your Doctor(s) that show they received their required training?
8. Is there data on servers, local PC's, portable laptops, removable media?
9. Is it encrypted (get out of jail free card with HIPAA)
10. Is it backed up (required by HIPAA)
11. Is there evidence that the backups have been tested and work?

If you are unable to answer any of the above questions, then I believe it is time we had a conversation about your HIPAA compliance and your company's security. I can give you a bunch of examples of fines from the Office for Civil Right (OCR), but, the latest one should be enough to get your attention.

Anchorage Community Mental Health Services (ACMHS) was fined $150,000 after a data breach of 2,743 individuals as a result of malware. There were 4 reasons given by OCR:

- No Risk Analysis
- Failure to implement Policies and Procedures
- A firewall that was not working and no one knew because it was not being monitored
- Running "unsupported" operating systems on their PCs (Windows XP)

I don't know about you, but, I am pretty sure that I can refresh your entire network, bring up your compliance level by several notches and hand you a right fair amount of change back if you were to budget $150,000 to fix your current problems. And, keep in mind that ACMHS still has to spend the money to fix the original problems!

You might as well begin to think of Health and Human Services (HHS) and OCR in the same manner as you think of the Internal Revenue Service. They are there, they wield a big stick with the ability to fine you up to $1.5M dollars if they think you completely ignored the law. (Willful Neglect) These are not folks that you want to mess with. Get compliant now and then stay that way. ❖

## Medical Identity Theft

Medical identity theft is one of the most costly, confusing and potentially dangerous types of fraud -- and a new study shows it's on a sharp rise.

HIPAA SECURITY BRIEF

**By Computer Networks of Roanoke, Inc.** March 15, 2015 Volume 1, Issue 3
Serving Roanoke and surrounding areas since 2006

Medical ID theft soared 22 percent in 2014, The Ponemon Institute said in its fifth annual survey published Monday. Ponemon estimates more than 2.3 million adult Americans or close family members became victims during or before 2014.

Once someone becomes a victim, it's extremely difficult to untangle the fraudulent bills and ruined medical records. Criminals can commit medical ID theft by using victims' personal information -- like names, birth dates, Social Security Numbers or the ID numbers found on insurance cards -- at medical providers' offices to receive services and prescriptions.

They may visit multiple hospitals, emergency rooms and pharmacies to receive care and prescriptions, racking up charges. Perhaps worse: Any medical care a criminal receives while using a victim's ID gets added to the victim's health record -- and may go unnoticed for months or even years.

Ponemon's study found the average victim didn't find out about the ID theft until three months after it happened, and 30 percent of victims didn't know when the crime occurred. And because privacy laws protect the release of health information, fixing the problem is difficult: Victims often have to be a part of the investigation, and it can be tough for victims to prove they're not the ones who actually received treatment. ❖

# No Encryption Means HIPAA Breach for 45K

**'We have taken steps to enhance our security'**

**Healthcare IT News - February 10, 2015**

Some 45,000 people are getting HIPAA breach notification letters after a mental health provider failed to encrypt laptops containing clients' medical data and Social Security numbers.

Aspire Indiana, a mental health organization located in central Indiana, has notified 45,030 of its clients and employees after several unencrypted laptops were stolen from its administrative office back on Nov. 7.

Following an investigation of the incident, Aspire officials determined emails on the laptops contained client and employees' Social Security numbers, names and addresses. 1,548 of those notified had their Social Security numbers compromised. The laptops also contained personal health information of Aspire clients. Health information Aspire collects includes HIV care data, substance abuse treatment and mental health services.

"Our organization is committed to maintaining the privacy and security of the personal information in our control, and we sincerely regret this incident occurred," said Aspire's president and CEO Rich DeHaven, in a public notice. "We have taken steps to enhance our security, including upgrading our alarm and security systems."

*Healthcare IT News* has reached out to Aspire for more details of the breach, but organization officials did not respond by publication time.

According to data from the Department of Health and Human Services, more than 41 million people have had their protected health information compromised in a reportable HIPAA privacy or security breach. **A whopping 54 percent of those breaches involved the theft of unencrypted devices, laptops or paper records.**

Stop here and re-read that previous sentence because it contains some of the most important HIPAA words you need to know. The key word is “unencrypted”. What is

# HIPAA SECURITY BRIEF

**By Computer Networks of Roanoke, Inc.** March 15, 2015 Volume 1, Issue 3
Serving Roanoke and surrounding areas since 2006

the significance? The Omnibus Rules of September 2013 gave you the ability to actually have a Data Breach and NOT REPORT IT. How? By using full-disk encryption on the hard drive of your PCs. Those devices such as laptops and phones, which are portable, are at the most risk. If they are lost or stolen, you are going to have to prove to OCR that there was no PHI on the device. How on earth are you going to do that? The answer is: "You can't".

Take a walk through your Practice, look around at the PCs. Is there PHI on any of them? I know that there is not "supposed to be". But, is there? Did Susie who worked at the front desk a couple of years ago download some transcription to the hard drive of her PC and leave it there, unencrypted? Do you use the PC for ID card scanning? Does the ID card scanning Vendor delete the scanned images out of the temporary files or off the hard drive of the PC after scanning?

Now you are catching my drift. PHI is everywhere. On PCs, on phones, on laptops, in emails, in network shared folders, at the transcriptionist, at the answering service. It is every place on your network because people put it there, probably because it was convenient to do so.

This is why you have to perform a proper Security Risk Analysis and then remediate the problems found including using full disk encryption on vulnerable PCs and other devices. ❖

## SECURITY, SECURITY, SECURITY

**Regulatory Compliance is a Natural by-product of Good Security**

**…'nuff said**

# I HATE MY COMPUTERS

We do this for a living and sometimes we feel the same way. In the past few years, with the proliferation of EHR's, Information Technology has taken over in the typical medical office. You have servers where there once were none, there are wireless devices in the exam rooms where there once was paper, there are scanners for paperless records, cameras for patient photos, Internet for the Patients, too much employee web surfing, viruses, malware and spyware…it just doesn't stop.

Welcome to the new normal.

The whole medical office computer network has gotten so complex, that you have little choice but to hire a great IT firm and let them manage the network for you. That is now a fact of life. IT companies are becoming similar to the power and phone companies. You have to have what they possess and you have to pay a monthly fee to get it. Unless you spend all day learning IT things (and where would you find time to run the Doctor's Practice) then you have to hire out IT. The network's complexity had grown past using your neighbor's, cousin's, kid's, friend from school to take care of the critical infrastructure of a multi-million dollar business. You need to call the pros. ❖

**Hank Wagner**

**757-333-3299 x232**