

# HIPAA SECURITY BRIEF

By Computer Networks, Inc.  
Serving Hampton Roads since 2004

June 15, 2015

Volume 1, Issue 6

## Office of Personnel Management (OPM) Data Breach

Well, it has been a busy couple of weeks on the Security front. The United States Government allowed hackers (presumably the Chinese) to steal the personal data of approximately 4 million current and former federal employees in a data breach of the Office of Personnel Management (OPM) systems. It seems that BASIC network hygiene such as applying patches and bug fixes, restricting administrator privileges and implementing multi-factor authentication (like if you use a new web browser for Facebook and have to put in a 6 digit code you got from the Facebook Code Generator) were not implemented. So, that means that a high level of sophistication may not have been necessary. And, it appears that the funding was approved in 2012 to fix a lot of these issues.

The OPM runs a little program called e-QIP, which processes applications for security clearances for federal agencies, including top secret and above. This bit, from a July 10, 2014 story in *The Washington Post*, puts the depth and breadth of this breach in better perspective:

*"In those files are huge treasure troves of personal data, including "applicants' financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, and names of neighbors and close friends such as college roommates and co-workers. Employees log in using their Social Security numbers."*

That quote aptly explains why a nation like China might wish to suck up data from the OPM and a network of healthcare providers that serve federal employees: If you were a state and wished to recruit foreign spies or uncover traitors within your own

ranks, what sort of goldmine might this data be? Imagine having access to files that include interviews with a target's friends and acquaintances over the years, some of whom could well have shared useful information about that person's character flaws, weaknesses and proclivities. Dumb as a box of rocks.

So, let's apply this lesson to HIPAA.

- Hire a professional firm to perform a Security Risk Analysis to discover potential points of data leakage from your Medical Practice/business
- Find someone who knows the IT business to apply security patches and bug fixes at least once a month
- Do not give the administrator password to everyone in your business
- Restrict access to shared network files and folders that contain sensitive information
- Only give staff the computer access they need to do their job-nothing more!
- Change passwords regularly
- Install a GOOD, HIGH-END Unified Threat Management (UTM) firewall that has Intrusion Prevention, Gateway Anti-virus, GEO-IP blocking (the ability to block entire countries from accessing your network) and other security features that lower your threat profile. ❖

This is what we do for a living.

Call us at 757-333-3299 x200 and let's set up a time to chat about protecting your business.

# HIPAA SECURITY BRIEF

By Computer Networks, Inc.  
Serving Hampton Roads since 2004

June 15, 2015

Volume 1, Issue 6

## Increasing Frequency of Cyberattacks

It's a different threat world nowadays. Think about it.

- *Every 60 seconds, 232 computers are infected with malware;*
- *12 websites are successfully hacked, with 416 attempts;*
- *more than 571 new websites are created;*
- *204 million emails are sent,*
- *278,000 tweets are sent out into the twittersphere – all in a single minute.*

Combine this with the fact that on the black market, medical records may be worth as much as \$100, compared to credit card data, which typically sells for less than \$2. You have been charged with maintaining the privacy of your Patient's health data as a result of HIPAA. It is a huge responsibility and not one that you should take lightly. Your computer network is at the core of maintaining that security.

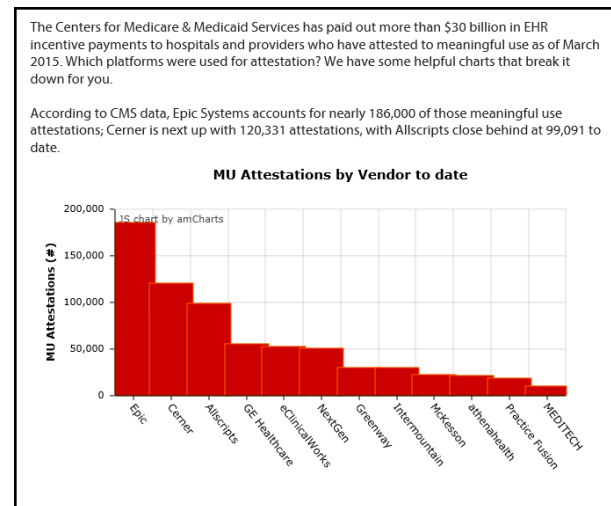
So, you have to take a look in the mirror and ask yourself:

- Do I have the best medical focused IT firm in the area handling my network?
- Are my current IT folks well-versed in HIPAA and the myriad of rules and regulations pertaining to securing my network from the Internet?
- Am I sure that that my current IT folks are always looking out for my business?

If there is any doubt in your mind, then you know what you have to do. It is tough parting company with IT folks that you have come to know and like. But, if they have not kept pace with all of the changes in the Medical space, then they do not need to be handling your IT needs.

You must have a Security focused, HIPAA aware IT group managing your network. That group needs to understand the laws and the consequences of poor network hygiene and how a data breach might destroy your Physician/Owner's business and livelihood. ❖

## Top 12 EHR Vendors



## I Lost My Phone and It Has Patient Information On It

Organizations should develop and implement reasonable and appropriate policies and procedures to safeguard health information, including those specific to mobile devices. Here are some topics and questions to consider when developing mobile device policies and procedures:

### 1. Mobile Device Management

- If the organization allows the use of mobile devices, what should the organization do about managing the use of mobile devices?
  - Has the organization identified all the mobile devices that are being used in the organization? How is the organization keeping track of them?
  - Has the organization assigned responsibility to check all mobile devices used for remote access, to find out if selected security/configuration settings are enabled?
  - Should there be a regular review and audit of the mobile devices?

# HIPAA SECURITY BRIEF

By Computer Networks, Inc.  
Serving Hampton Roads since 2004

June 15, 2015

Volume 1, Issue 6

## 2. BYOD (Bring Your Own Device)

- Should the organization let providers and professionals use their personally owned mobile devices within the organization?
- Should providers and professionals be able to connect to the organization's internal network or system with their personally owned mobile devices, either remotely or on site?

## 3. Restrictions on Mobile Device Use

- Does the organization restrict how providers and professionals can use mobile devices?
  - Can providers and professionals use mobile devices to access internal networks or systems, such as an EHR?
  - Are providers and professionals restricted from using mobile devices when they are away from the organization?
  - Can providers and professionals take their mobile devices home?
  - Should the organization allow texting or emailing of health information?

## 4. Security/Configuration Settings for Mobile Devices

- Will the organization institute standard configuration and technical controls on all mobile devices used to access internal networks or systems, such as an EHR?
  - If so, is the organization's current mobile device configuration document, including connections to other systems/applications, inside and outside of the firewall.

## 5. Information Storage on Mobile Devices

- Are there restrictions on the type of information providers and professionals can store on mobile devices?
  - If so, where and for how long should the data be stored?
- Are providers and professionals allowed to download mobile applications to mobile devices? If so, what type(s) of applications are approved?

## 6. Misuse of Mobile Devices

- Does the organization have written procedures for addressing misuse of mobile devices?

## 7. Recovery/Deactivation of Mobile Devices

- Does the organization have procedures to wipe or disable a mobile device that is lost or stolen?
- Does the organization have standard procedures to recover mobile devices from providers and professionals when their employment or association with the organization ends?

## 8. Mobile Device Training

- How is the organization training its workforce (management, doctors, nurses, and staff) on policies and procedures?
- How does the organization hold its workforce (management, doctors, nurses, and staff) accountable for non-compliance? ❖

## The Biggest Threat To Your Business is Dave...



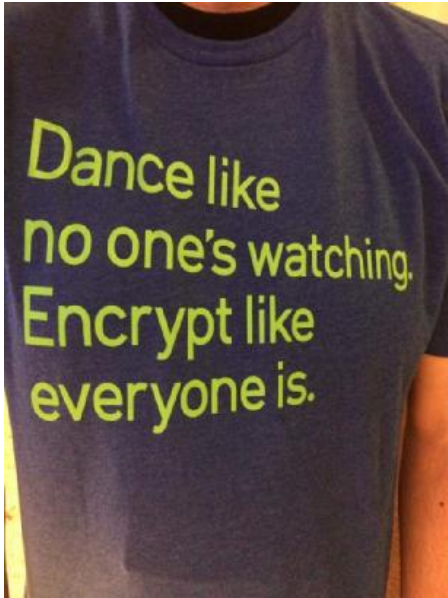
The Security community is rapidly coming to the conclusion that it is not whether or not you will have a breach, but, when you will have yours and how big it will be. Proper preventative measures, such as a professional Security Risk Analysis, good computer network hygiene that lower your threat profile, coupled with regular employee training, can go a long way to making you a less appealing target. ❖

# HIPAA SECURITY BRIEF

By Computer Networks, Inc.  
Serving Hampton Roads since 2004

June 15, 2015

Volume 1, Issue 6



## No encryption means HIPAA breach for 45K

'We have taken steps to enhance our security'

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, 2014.

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.

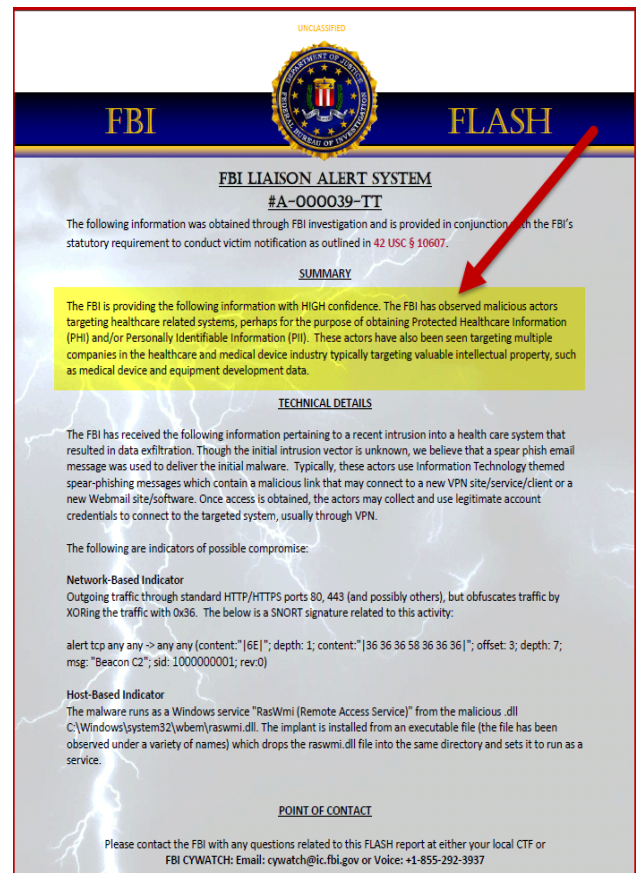
"Our organization is committed to maintaining the privacy and security of the personal information in our

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. ❖

## FBI FLASH ALERT



UNCLASSIFIED

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION  
DEPARTMENT OF JUSTICE

FBI LIAISON ALERT SYSTEM  
#A-000039-TT

The following information was obtained through FBI investigation and is provided in conjunction with the FBI's statutory requirement to conduct victim notification as outlined in 42 USC § 10607.

SUMMARY

The FBI is providing the following information with HIGH confidence. The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII). These actors have also been seen targeting multiple companies in the healthcare and medical device industry typically targeting valuable intellectual property, such as medical device and equipment development data.

TECHNICAL DETAILS

The FBI has received the following information pertaining to a recent intrusion into a health care system that resulted in data exfiltration. Though the initial intrusion vector is unknown, we believe that a spear phish email message was used to deliver the initial malware. Typically, these actors use Information Technology themed spear-phishing messages which contain a malicious link that may connect to a new VPN site/service/client or a new Webmail site/software. Once access is obtained, the actors may collect and use legitimate account credentials to connect to the targeted system, usually through VPN.

The following are indicators of possible compromise:

Network-Based Indicator  
Outgoing traffic through standard HTTP/HTTPS ports 80, 443 (and possibly others), but obfuscates traffic by XORing the traffic with 0x36. The below is a SNORT signature related to this activity:

```
alert tcp any->any (content:"|6E|"; depth: 1; content:"|36 36 36 58 36 36 36|"; offset: 3; depth: 7; msg: "Beacon C2"; sid: 1000000001; rev:0)
```

Host-Based Indicator  
The malware runs as a Windows service "RasWmi (Remote Access Service)" from the malicious .dll C:\Windows\system32\wbem\raswmi.dll. The implant is installed from an executable file (the file has been observed under a variety of names) which drops the raswmi.dll file into the same directory and sets it to run as a service.

POINT OF CONTACT

Please contact the FBI with any questions related to this FLASH report at either your local CTF or FBI CYWATCH: Email: cywatch@ic.fbi.gov or Voice: +1-855-292-3937