TECHNOLOGY TIMES

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

By Computer Networks, Inc.

Serving Hampton Roads since 2004

Volume 8, Issue 11 **October 2015**

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Rick Boyles, Owner/Founder
Computer Networks, Inc.

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

SENTARA

Where Are Your Laptops?

Portable hard drives stolen from Sentara Heart Hospital

October 02, 2015
By: Sentara Corporate Communications

The letter copied below was sent this week to 1,040 patients who underwent electrophysiology procedures at Sentara Heart Hospital in one of the electrophysiology labs between Sept. 4, 2014 and Aug. 14, 2015. The patient information on the portable hard drives was

See Laptops Page 2

Inside This Issue

Predictable Results Predictable Fee

We do it all…HIPAA Security Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, IT Consulting. And, we do that for businesses with as few as 10 PCs.

We are looking for a select number of new clients in the medical and professional services fields.

If you are dissatisfied with the level of service you are getting from your current IT Vendor, pick up the phone, call me, Rick Boyles, at 757-333-3299 x200, or feel free to email me rick.boyles@computernetworksinc.com so we can chat a bit about your needs. ❖

A Culture Of Security

The Internet is like the Wild West of olden days. While it has brought speed and convenience to our lives, both personal and business, the Internet comes with ever increasing threats.

Your business must develop a "culture" of security. Size of your business matters not. Your customer's identity is the Grand Prize for these folks.

Every day your computer network is being threatened from the Internet by bad people intent on finding information to steal. Your firewall may have no control over the web sites your staff may visit. Plus, criminals are sending malware "phishing" emails to your staff daily, which will infect your network if opened. Times are a-changin', folks. You have to protect yourself using modern, business grade tools.

Let me know if you want to talk about how to protect your business from the bad people. ❖

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

Laptops continued from Page 1

limited to name, date of birth and a unique patient identification number produced by Sentara, plus physician notes about the procedures.

Background: Due to the number of patients affected, we are required by federal law to provide notification to patients and the news media and post the notification on our website. However, the Sentara Privacy and Compliance team notifies patients under most circumstances involving protected health information, to keep our patients informed and assure them of our continuing efforts to protect their personal information.

Details: The theft occurred over the weekend of August 14 in a procedure area normally restricted to staff and patients. We believe these small portable hard drives were stolen for whatever street value they may have, and not for purposes of identity theft or fraud. The identifying information is so limited it does not facilitate fraud. The information on the drives is purely clinical. Updated procedures are in place for the secure storage of these devices. We sincerely regret any concern or inconvenience the theft of these devices may cause our patients.

Resolution: The hospital's Risk Management team notified Norfolk Police of the theft. The Risk Management team and the Sentara system Privacy manager conducted an internal investigation, including interviews with personnel assigned to Sentara Heart Hospital that weekend, and closed the investigation on September 29. Portable hard drives are now secured in a locked drawer at all times, connected by cable to the laptops being used. Only management personnel have keys. Additional security improvements are planned to further limit access to the clinical area affected.

The Letter:

As part of the Sentara Commitments to you, our patient, we strive to protect the confidentiality of your personal information. Regrettably, we are writing to inform you of an incident involving that information.

On Aug. 20, 2015, Sentara first learned that two unencrypted hard drives were missing from two Electrophysiology labs located within Sentara Heart Hospital in Norfolk Virginia. We immediately began our own internal investigation. The information on the hard drives contained backups of electronic notes taken during procedures performed in those two rooms. The information included your name, unique medical record number, date of birth, procedure date, diagnosis, procedure, surgeon and staff names, allergies, notes and medications that relate only to the procedure performed. The hard drives did not include your social security number or billing information.

We assure you that we are committed to the security of your personal information and are taking this matter very seriously. To help prevent this from happening in the future, we are reevaluating the access to these lab rooms and working to ensure the backup drives will be protected.

If you have any questions, or you need further assistance, you may contact 1-844-322-8235, between the hours of 8 a.m. to 6 p.m. Eastern time. Please refer to incident number COE151471.

Sincerely,
Greg Burkhart
Chief Compliance Officer
Chief Privacy Officer

Let us help! Call our office and receive a FREE Audit to uncover gaps in your company's network.

Our highly trained team of IT pros will come to your office and conduct this comprehensive audit. We'll then prepare a customized "Report of Findings" that reveals specific vulnerabilities and a prioritized Plan of Attack for getting any problems addressed fast. ❖

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

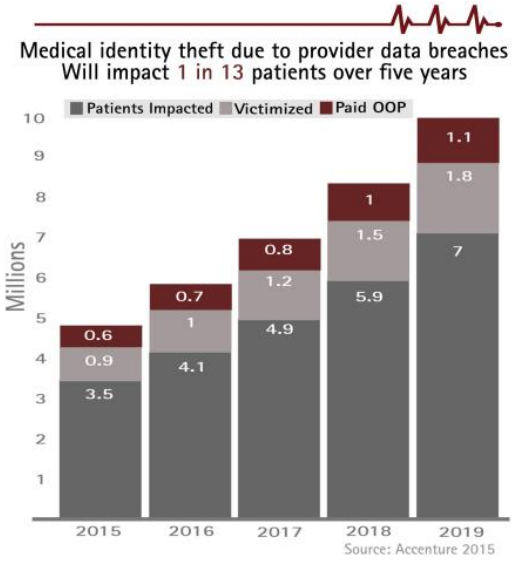
OCT 15, 2015 | HIPAA JOURNAL | HEALTHCARE DATA SECURITY, HIPAA BREACH NEWS

The cost of health system cyberattacks is set to increase substantially, according to a recent study conducted by global management consulting firm, Accenture.

The new study predicts the cost of health system cyberattacks will rise to $305 billion over the next 5 years, and will affect approximately 25 million patients. The company also estimates that 1 in every 13 U.S. healthcare system patients are likely to have their identities stolen and used to commit fraud over the same time period.

The research team calculated that 1.6 million patients have already had their medical data stolen from healthcare providers in 2014. With the number of breach victims already created in 2015, next year's figures are likely to be considerably higher.

Cost of Health System Cyberattacks Will Continue to Increase



For the study, Accenture used data compiled by the Ponemon Institute along with breach reports submitted to the Department of Health and Human Services' Office for Civil Rights. That data was used to determine the number of individuals who were likely to suffer identity theft, then Accenture quantified the patient revenue that would be put at risk. The figures were then projected for the next 5 years.

25% of Breach Victims Will Incur Out of Pocket Expenses

Unfortunately for healthcare patients, criminals are trying to gain access to medical data in order to steal identities and commit medical fraud. When fraud is committed, the victims are often left with few options for recourse. Credit card companies have a legal responsibility to protect card holders, and cases of fraud often see any financial losses suffered reimbursed. With medical identity theft, patients often have to cover the cost out of their own pockets.

Accenture paints a bleak picture for patients. Huge volumes of data are now being stolen, and the company's team of researchers believe the number of cases of identity theft stemming from medical data breaches will impact 25% of data breach victims.

Over the next five years the team estimates that out of the 25 million patients affected by health system data breaches, 6 million will suffer medical identity theft, and 16% of all data breach victims will have to cover out of pocket costs as a result of the theft of their identities. The cost to patients is expected to be $56 billion over the next 5 years.

According to Kaveh Safavi, M.D., J.D., Managing Director of Accenture's global healthcare business "If healthcare providers are complacent to safeguarding personal information, they'll risk losing substantial revenues and patients as a result of medical identity theft." He also said, "What most health systems don't realize is that many patients will suffer personal financial loss as a result of cyberattacks on medical information."

The Lighter Side:

A Pharmacist's Bad Day

Upon arriving home, a husband was met at the door by his sobbing wife. Tearfully she explained, "It's the druggist. He insulted me terribly this morning on the phone. I had to call multiple times before he would even answer the phone."

Immediately, the husband drove downtown to confront the druggist and demand an apology.

Before he could say more than a word or two, the druggist told him, "Now, just a minute, listen to my side of it. This morning the alarm failed to go off, so I was late getting up. I went without breakfast and hurried out to the car, just to realize that I'd locked the house with both house and car keys inside and had to break a window to get my keys."

"Then, driving a little too fast, I got a speeding ticket. Later, when I was about three blocks from the store, I had a flat tire."

"When I finally got to the store a bunch of people were waiting for me to open up. I got the store opened and started waiting on these people, all the time the darn phone was ringing off the hook."

"Then I had to break a roll of nickels against the cash register drawer to make change, and they spilled all over the floor. I had to get down on my hands and knees to pick up the nickels and the phone was still ringing.

When I came up I cracked my head on the open cash drawer, which made me stagger back against a showcase with a bunch of perfume bottles on it. Half of them hit the floor and broke."

"Meanwhile, the phone is still ringing with no let up, and I finally got back to answer it. It was your wife. She wanted to know how to use a Rectal Thermometer."

"And believe me, mister, as God is my witness, all I did was tell her!"

No Explanation Needed

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Did You Hear The One About The CMS Audit?

True to its word, the U.S. Health and Human Services Department's Office of Inspector General has begun to audit individual providers to determine if they met the Meaningful Use requirements, according to attorney Daniel Gottlieb, with McDermott Will & Emery in Chicago.

"The work plan is coming to fruition," Gottlieb said.

OIG is conducting random nationwide audits of providers, according to Gottlieb, who wrote a blog post on this new development April 1. The audits are somewhat different from the ones being conducted by the Centers for Medicare & Medicaid Service's audit contractor Figliozzi & Co., based in Garden City, New York, in that the OIG audits are only looking at certain measures, but over a three-year period.

The CMS audits being conducted by Figliozzi, review all measures, but only for a single attestation year at a time.

Do you have your Security Risk Analysis up to date? ❖