

APR
2015

TECHNOLOGY TIMES

HEALTHCARE IT AND TRENDS

WHAT'S INSIDE

**My Data Is Backed Up,
So I Can Recover It Fast,
Right? WRONG!**

**10 Secret Tricks, Tools
And Cool Features Hiding
In Google**

Win A Lenovo Laptop!

**New Medical Modifiers
to Use Instead of
Modifier 59**

**3 Easy Protections You
Need To Put In Place
NOW To Protect Your
Bank Account From
Cybercrime Schemes**

**Four Areas Your
Healthcare
Organization's Data May
Be Exposed**

**Eligible Professionals
Will Face \$200 Million
in Meaningful Use
Penalties in 2015**

Free Report Download

Tech news, tips and
updates provided by

Clientfit
Technology Consulting

My Data Is Backed Up, So I Can Recover It Fast, Right? WRONG!

Here's a big (and scary) misconception you might have about your data backups: backing up your data guarantees a fast recovery. It does NOT! In short, data backup is nothing more than copying files. There are a number of ways data can be backed up, both manually and automatically—and you don't need to know all the technical ins and outs of them. But what you DO need to know is whether your current backup is set up in a way that would allow for the fastest possible recovery time in the event of a disaster or data-erasing event. You might be shocked to find out it's not as fast and easy as you'd like to think.

Disaster Recovery vs. Data Backup

Let's start by defining what "disaster recovery" is. Disaster recovery is the process by which you will RECOVER the functionality of your data, software programs, devices and business operations in the event of a "disaster."

A disaster can be as simple as a server crashing or a more catastrophic event such as a tornado. But here's the real kicker: MOST data loss is not due to a natural disaster such as a flood, hurricane, tornado, etc. Most data is lost because of simple human error, such as employees accidentally deleting files, faulty hardware or even a virus or hacker attack that brings down your entire network.

Because most businesses believe "that could never happen to me," they are caught completely off guard when there's a major outage or files get deleted or corrupted beyond recovery. They THINK because they have things "backed up" they can instantly get those files back and start working again. Not so.

Here's a perfect analogy: Let's suppose you could back up all the personal items you have in your house—your clothes, furniture, valuables, etc., and somehow maintain a copy of everything in a

Continue reading on last page

10 Secret Tricks, Tools And Cool Features Hiding In Google

If you use Google for searching the web, you're going to love these 10 features, available to everyone that you probably didn't know about. The best way to find these is to simply search for the item in Google.

1. Google's Dictionary Extension for Chrome. Add this plug-in and you can highlight words on a web page to look them up and see how they're pronounced without leaving the page! hours of operation, and photos or videos.
2. Google Forms. Need to create a quick survey? Poll your friends on where to go to dinner? Collect RSVP information to organize a party? Google Forms will allow you to do all of this quickly and for free.
3. Google Keep. This free productivity app is similar to Evernote, allowing you to keep lists, web pages, documents and information organized on the web and on your smartphone.
4. Google Public Data Explorer. This free application makes large datasets (like world development indicators or unemployment statistics) easy to explore, visualize and communicate. false claims are not made. Google will physically mail a confirmation code to your business once your information is submitted which you will need to enter to complete the process. Once reviewed and accepted your information will be available to all people who search locally for your business!
5. Google Fonts. Want a unique font to use on your web site? This public database of typefaces is free and offers a myriad of font choices and selections.
6. Google Mortgage Calculator. Want to know if that new house is within your budget? Google mortgage calculator can quickly calculate a monthly payment for your home for free.
7. Google Sky. For my fellow "trekkies" and sci-fi fans, check out Google Sky. From this page you can view celestial objects, including stars, galaxies, planets and tons of other cool photos taken from space.
8. Google Unit Conversions. Need to convert kilometers into miles or vice versa? Just type in "unit converter" and Google will pop up a web-based converter that will do the math for you in seconds.
9. Google Flight Tracker. Type in any flight number and Google will report its status.
10. AdBlock. This is the most popular Chrome extension out there. AdBlock, which works in Chrome, Opera and Firefox, will remove banner advertisements that can make reading some sites difficult.

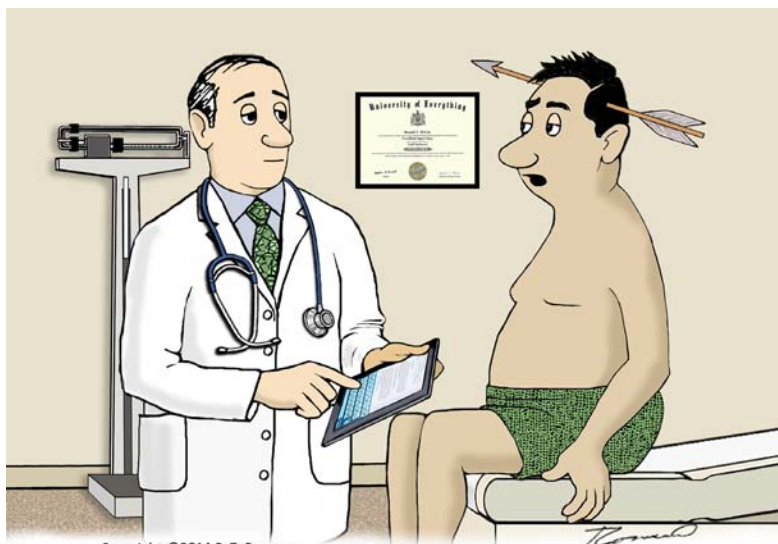
Win a Lenovo Laptop!



We are giving away a Lenovo Thinkpad X1 Carbon Ultrabook (\$1500 dollar value) to the person who refers the most business to us between now and Feb 28th 2014. Here's how the contest works:

1. Call us or email us with your referral information.
2. We will call to schedule an appointment with your referral.
3. Once a meeting is scheduled and completed we will send you a gift card of your choice for \$25 for each referral or donate to your favorite charity.
4. If your referral becomes a client you will receive another \$50 dollar bonus and a \$100 dollars off any future service.
5. The person with the most referrals at the end of the period wins the laptop!

Easy as pie!



Copyright ©2014 R.J. Romero.

"Skip all that medical mumbo jumbo and just give it to me straight, Doc. What's the ICD-10 code for this?"

Cool Website of the Month: www.icd9data.com

Every wondered if the diagnosis code you selected from your EHR is actually billable or correct? With ICD9data.com you can look up various codes and get information such as:

1. Related Codes
2. Coding Standards
3. Whether the code is a billable code or not
4. The ICD-10 equivalent

This tool will help reduce claim denials and rejections due to improper coding and have you coding like a PRO in no time.

Medical Billing Corner : New Medicare Modifiers To Use Instead of Modifier 59 - XE, XS, XP, & XU

Modifier 59 is one of the most widely used (and abused) HCPCS modifiers. The CPT manual defines modifier 59 as "Distinct Procedural Service." CMS has introduced 4 new modifiers that explain this occurrence in more detail.

XE Separate Encounter: A service that is distinct because it occurred during a separate encounter.

XS Separate Structure: A service that is distinct because it was performed on a separate structure /organ.

XP Separate Practitioner: A service that is distinct because it was performed by a different practitioner

XU Unusual Non-Overlapping Service: The use of a service that is distinct because it does not overlap usual components of the main service.

Modifier 59 can still be used only when a more descriptive modifier is not applicable. These changes went into effect Jan 1 2015.



Copyright ©2012 R.J. Romero.

"CMS wants health providers to draw the line on unethical billing practices. Go out and get an Etch-a-Sketch."

The President's Corner - 3 Easy Protections You Need To Put In Place NOW To Protect Your Bank Account From Cybercrime Schemes

82,000. Do you know what that number is? It's the number of NEW malware threats that are being designed and launched online EVERY SINGLE DAY. That may explain why 74% of small businesses report having experienced online bank fraud in a recent survey by the Ponemon Institute, and why they're calling 2014 "A Year of Mega-Breaches."

There's no doubt about it: cybercrime is a thriving business that is on the rise; and simply having an antivirus software and firewall isn't enough anymore to protect yourself. Worse yet, businesses do NOT enjoy the same protections as consumers. If money is wired from your account or drawn by ACH draft, the likelihood of getting that back is SLIM and the bank is not responsible for replacing funds stolen. If you want to avoid being a victim, here are three simple precautions you can take right now.

1. Lock Down Your Environment. If you do online banking, ONLY access your account via a dedicated PC that you don't use for accessing social media sites, web browsing or e-mail. This will limit the chances of a keylogger (a malware program that records your keystrokes) from being installed on your PC to grab your keystrokes.

2. Get Notified. Sign up for e-mail notifications for withdrawals. Many online banking services will allow you to sign up for e-mail alerts whenever a certain amount of money is withdrawn from your account. Since speed of notification is CRITICAL to stopping a cybercriminal from robbing you blind, this could give you the quick notification that a large sum of money has been withdrawn. Notify your bank IMMEDIATELY of any suspicious activities.

3. Have a Unified Threat Management (UTM) in place. Cybercriminals are far more sophisticated in their attacks and can easily bypass traditional firewalls and antivirus software.

With the proliferation of mobile devices accessing your network and the growing use of cloud applications and free social media web sites (Twitter, Facebook and even online reviews), the chances of an employee accidentally infecting your network are growing exponentially. Don't bring a knife to a gunfight; call us today to discuss how we can protect you.

Calvin Dunn, Founder/CEO of ClientFit



Four Areas Your Healthcare Organization's Data May Be Exposed

Data breaches are real and becoming increasingly common in healthcare. Healthcare organizations are a mouth watering treat for hackers due to the high level of confidential patient information that may be stored in their systems. Here are 5 areas organizations should focus on improving in order to keep their patient and business data safe.

1. Implement policies and procedures - Administrative safeguards should be put in place by your organization to control the activities on your employees. Data breach could be as simple as downloading data to a flash drive or a lost company laptop. Creating policies and procedures that outline expected employee conduct when it comes to patient data can help tremendously. Organizations can also remind employees of the penalties/punishments that may be levied if they choose to break any data security rules.

2. Choose a compliance officer or establish a compliance department - Maintaining data security in your organization can be a full time job in itself. With all

the rules, regulation, and technologies out there it can be a bit difficult to keep up at times. Selecting an employee or vendor to manage this process will ensure that your organization remains in compliance.

3. Take a hard look at you email practices! - Does your organization communicate with employees via email? Is your organization using free services such as MSN, Yahoo!, or Gmail to communicate with patients? All sensitive email communications must be encrypted. Not only does you email communication need to be encrypted during transit but also at rest on your email server.

4. IT Support - Do you have someone actively monitoring and managing your computer systems and networks? If you only call your IT guy when there is a problem then the answer to that question is NO! Hiring an managed IT service provider will ensure that your network is safe and secure from hackers viruses and malware. In a managed service agreement your IT company is actively protecting and monitoring your network 24/7/365 days a year.

Eligible Professionals Will Face \$200 Million Dollars In Meaningful Use Penalties In 2015

Did you fail to meet meaningful use by the 2014 Deadline? Turns out you're not alone. The latest data from CMS reveals that eligible professionals will face close to 200 million dollars in MU penalties in 2015. Over 250,000 providers will face penalties ranging from \$1 to \$2000 dollars. These numbers were released shortly before CMS extended the 2014 reporting deadline to March 20th 2015. Eligible professionals must meet MU requirements each year to avoid increasing payment penalties.



Copyright © 2011 R.J. Romero. www.hipaacartoons.com

"One more form, Mrs. Wasley. New federal regulations require that you demonstrate 'Meaningful Use' of your organ transplant or you will have to give it back."

My Data Is Backed Up... continued.

warehouse 1,000 miles away from your current residence. Now let's suppose (and God forbid) your house burns down, destroying everything with it. You'd be relieved that you had a copy of everything somewhere else, so it's not a total loss (which, by the way, is why your backups need to be OFF-SITE, not on devices in your office).

But here's the problem: If your house burned down, you might have a copy of everything you own, but you no longer have a place to put it. So, for starters, you have to rebuild the house. Next you have the project of getting everything out of that storage unit into your NEW house. Then you have to rearrange everything. This is exactly how most backup systems work UNLESS you are running "image" backups. An image will allow you to restore your server, PC, device,

etc., FAST because you're not backing up single items but, instead, the ENTIRE HOUSE.

Understanding how your backup works is imperative to your practice. In fact, it is required by the HIPAA Security rule that you backup your data, test your backups, and store data offsite just to name a few.

Will Your Backup Allow You To Recover FAST?

If you want to learn how you can use image backups for faster disaster recovery, call us at (213) 261-0071 and we'll audit your current backup—for FREE—to reveal if it's actually backing up all of the files you need AND just how fast you could be back up and running again in the event of a disaster.

Free Report: 10 Hidden IT Risks That Threaten Your Practice (Plus 1 Fast Way to Find Them)

Your practice depends on intelligence. But can you count on your technology? This brief paper exposes 10 silent threats that might be quietly undermining your operations now - and proposes one quick, easy, and free way to bring these threats under control now.

Download your free copy today at www.clientfit.net/10risks

or send an email to info@clientfit.net with *Free Report Request* in the subject line.

