EMV: How Your Practice Will Be Affected By Credit Card Changes in October 2015

At Manage My Practice, we are big proponents of using a Credit Card on File (CCOF) system in medical practices to reduce expenses and improve cash flow. Knowing how your processing vendor's pricing plan and security features work are critical to implementing this system. You have to be able to understand and negotiate your costs, and stay current on best practices and technology that keep your patients' data safe.

Big changes are coming to the technology end of your credit card system in October of this year (as if you won't be busy enough with ICD-10!) and you need to make sure now that you have all the details handled for your employees and your patients. The new technology is called EMV, or "Euro Mastercard Visa" and has been used in most of the rest of the world for awhile now.

Whenever we have questions about anything credit card related, we go straight to Michael Gutlove, Director of Merchant Services at IDT. Michael has been our own vendor, as well as our top recommendation to clients for almost three years now. We asked him to help us sort out the changes.

Mary Pat: Michael, what's your background?

Michael: I've been helping business owners improve their bottom lines since 1997. Reducing costs are critical – now more than ever – for all business owners, and I've been able

to repeatedly reduce operating costs by clearing away the traditional smoke and mirrors of credit card processing.

Mary Pat: Are people in general and patients specifically using credit cards more than they used to? Do you foresee a time when people will only use credit cards, no cash or checks?

Michael: While electronic payment volume has steadily increased year after year it's highly unlikely that cash or checks will ever be completely eliminated. Cash payments serve the "underbanked" population and checks remain a highly effective method of payment for high ticket (luxury) items.

Mary Pat: What about payment via a smartphone or watch – do you see that becoming a predominant part of the American payment experience?

Michael: Apple Pay is the first mobile wallet solution that's made any traction into the payment space. It's opened the door for cell phone manufacturers, wireless carriers, and any/every technology company under the moon to think about getting involved. The problem with suggesting that mobile technology will replace the way we pay (or become the primary way we pay) is that it's not fixing an existing problem. Mobile payments are generally viewed as a convenience as opposed to a necessity and we've become accustomed to carrying a wallet or purse with actual credit cards.

Mary Pat: The new acronym in credit cards is EMV. What is EMV?

Michael: EMV stands for **E**uropay **M**asterCard **V**isa. It's an acronym for the Global standard of chip card technology facilitating electronic payment transactions. The United States is the last major country to adopt this method.

Mary Pat: Why do readers need to know about EMV?

Michael: October 2015 marks the deadline for business owners, accepting credit or debit cards, to upgrade their terminals for chip card acceptance. While it is not legally necessary to upgrade, doing so reduces the liability for fraudulent or counterfeit duplicate transactions.

Mary Pat: What does accepting chip cards have to do with liability?

Michael: EMV prevents "card present" duplicate fraud as the customer always maintains possession of their card. Instead of swiping the mag-stripe on the back, merchants will instruct customers to insert cards into the EMV ready terminal and enter a PIN or signature when prompted. Businesses that do not have the ability to accept EMV cards will be held liable for fraudulent "swiped" transactions.

Mary Pat: Does EMV eliminate fraud?

Michael: EMV is not a cure all for all types of fraud. The programs put in place will help with duplicate card fraud charge-backs, but will not impact others. Visa, MasterCard, Discover, and American Express have different liability shift requirements.

Mary Pat: What about "Card Not Present" transactions?

Michael: EMV only applies to face-to-face transactions. When it was released in Europe increased levels of fraud showed up via ecommerce and MOTO (mail order/telephone order). A similar scenario is expected once the US adopts EMV making PCI-DSS compliance even more important.

Mary Pat: What is PCI?

Michael: PCI–DSS stands for the Payment Card Industry Data Security Standard. Most processors offer comprehensive programs to ensure PCI compliance and validation.

Mary Pat: What should I do now?

Michael: Reach out to your processor and determine your risk level for EMV. Accepting EMV can only help your business but it isn't necessary to do anything prior to October. The majority of POS (point of sale) manufacturers haven't released EMV readers and new hardware might not be necessary depending on your existing terminal make & model.

Making sure you are getting the most you can from your credit card vendor is a critical part of protecting your data and your bottom line in today's healthcare industry. You need to know the steps you and your vendors are taking to safeguard patient data as well as being able to relay those steps back to patients and employees. That's why it's important for managers to understand EMV – and their credit card setup in general. Successful implementation of a credit card on file program or any credit card processing system will always require buy-in and communication.

NOTE: Credit Card on File clients of Manage My Practice should know that Michael Gutlove will be swapping out your current swipers for EMV terminals for chip and non-chip cards at a considerable discount.

For additional information, questions, or anything else credit card related feel free to reach out to Michael Gutlove at 201.281.1621.

Clearing Up the Confusion

Between Security, Privacy, HIPAA and HITECH: An Interview With Steve Spearman

Mary Pat: Your business is called "Health Security Solutions." People often confuse privacy with security. Can you clear up the confusion for us?

Steve: The Privacy rules refer to the broad requirements to protect the confidentiality of Protected Health Information (PHI) in all its forms. So for example, a physician talking loudly on the phone in the lobby of a restaurant about a patient by name is a violation of the privacy rules. **PHI on paper records is covered under the privacy rules.**

The security rules are specifically concerned about protecting the confidentiality (i.e. privacy), integrity and availability of electronic PHI, or PHI that exists in a digital form. So once you are dealing with **electronic health records and information systems, violations tend to fall under the security rules.**

Let me illustrate with an example. A traditional fax machine is generally considered under the rules to be an analog device. So if a practice takes a patient face sheet and faxes it to another another practice who also has a traditional line to line fax machine, it would fall under the privacy rules. However, if one practice has a traditional fax machine and is faxing the document to a practice that has either a fax server or a fax service (like eFax), then the data is digitized before it is processed on the receiving end. That second practice's fax would be covered under the security rules because the data is digitized.

Mary Pat: Okay, that helps a lot. The difference between HITECH and HIPAA can also be confusing – can you clarify?

Steve: That's a great question. **HIPAA** defines the rules related to the privacy and security of patient health information and has been around since 1996 with periodic updates since then.

HITECH is a subsection of the American Recovery and Reinvestment Act (ARRA) legislation that provided incentives to physicians and hospitals to "meaningfully" adopt EHR solutions. But the act also contained elements related to the security of ePHI. Specifically, it clarified and strengthened the law as it pertains to business associates. Prior to HITECH, the liability of Business Associates (BAs) was mostly limited to breach of contract under the terms laid out in a business associates agreement. HITECH clarified that Business Associates were required to comply with all the HIPAA requirements and dramatically strengthened enforcement by specifying that the increased fine levels, up to $1.5M, applied to BAs as well as covered entities. Probably the most significant security related provision of the HITECH Act was the Breach Notification requirement. Under that requirement, covered entities and business associates are required to report to DHHS any unauthorized breach of PHI unless the data was secured through encryption.

As you may have heard, the Omnibus HIPAA regulations were just published and will go into effect in a couple of months. One of the objectives of the rules is to consolidate the HITECH security related provisions under the HIPAA umbrella. So when the laws take effect, those security provisions that were a part of HITECH will be covered under the HIPAA mandates.

Mary Pat: Many practices are overwhelmed with trying to meet all the federal program mandates and keep up with all the other changes. What are two things that all practices should be doing right now to become compliant with the law and

protect their practices?

Steve: I am tempted to give an overly long answer to this question. But I'll try to keep it simple. **One, the practices need to have the required set of security and privacy policies in place.** Most practices have some or many privacy policies in place but, based on my experience, are missing the security policies. For example, every practice has to have the following policies and procedures:

- a sanction policy
- a named security officer,
- an information system activity review an audit procedure, and many more.

A good set of template policies can set you well on your way towards compliance. ***(If you contact me, I am happy to talk to anyone about places they can go to get security policies including a set of free policies that I have recently reviewed)***. Any covered entity with a breach of ePHI that is found to have been willfully neglectful will face heavy fines (as high as $1.5M). Policies and procedures are a first good step to avoid the willful neglect designation.

Two, at the risk of sounding self-serving, they need to protect the ePHI that they are creating, transmitting or storing. And a risk analysis is the first step to that process. It is also the first and a required HIPAA Security safeguard. For most clinics, there tends to be a fairly predictable set of vulnerabilities that they need to address but every practice is different and the risk analysis helps you get to the bottom of these.

Mary Pat: Do small practices have less to worry about as far as security than large practices?

Steve: They don't have less to worry from a compliance standpoint. They have to abide by the HIPAA rules to the same degree as large practices. However, there are elements within

the rules that allow for latitude based on the resources and complexity of organizations. So I might advise an 18-physician orthopedic practice that they need to implement a security measure that I would not advise a smaller practice to implement. In a smaller practice setting, for example, all the employees know each other. So if some unknown person is attempting to get into the data closet, someone will notice and stop them. Although the data closet should be locked in most practices of any size, in a large practice or enterprise it should be alarmed and monitored as well. Although larger practices tend to have more resources at their disposal, in many ways it is easier to get a small clinic into compliance.

Mary Pat: Does using a cloud-based practice management or electronic medical record system alleviate security requirements, or does it make the security requirements more stringent?

This is a controversial opinion but, on net, I think that cloud-based, hosted and Software as a Service (SaaS) solutions make compliance easier. I have two main reasons for that assertion. I believe that a large breach involving multiple records is less likely. The physical security of the server is invariably much, much better with hosted solutions. These solutions are often deployed in SSAE 16 certified data centers which require extremely rigorous security practices. In addition, they are frequently deployed using either a virtual environment or terminal services which means that data is not being stored or cached on the desktop or laptops. **Remember, about 80% of the reported breaches involve stolen laptops and other "client" devices**. Another benefit of SaaS solutions is that they often do much of the heavy lifting related to contingency planning and data backup.

There are some negative trade-offs. Many service agreements with SaaS providers are wholly inadequate. The contract with a service provider should state clearly that the covered entity owns the data. They should also document a procedure to

provide at zero or very minimal cost an exact copy of the ePHI owned by the covered entity in the event that the service provider goes bankrupt or the provider just wants to cancel its contract. The procedure for this transfer of data needs to be spelled out in the service agreement and/or in the practice's contingency plan. And, ideally, it needs to be tested periodically. In addition, I have a concern that many solution providers are unaware that they are bound by all the HIPAA regulations and don't take sufficient precautions in safeguarding their data. Some solution providers do better than others. Another concern, that is becoming less and less true over time, is that access to the record is dependent on a persistent internet connection. Since protecting the "availability" of ePHI is one of the goals of the regulations, dependence on an internet connection makes a compromise in this area a bit more likely. Contingency plans need to address this concern and a redundant connection should be a part of that.

I would finish by pointing out that solution providers can "scale" and can not only afford but have the incentives to invest in security infrastructure and expertise. A hosting provider can afford to hire someone with a Masters in Information Security or with the CISSP certification while the typical practice cannot. Although HIPAA has many components and I have concerns about hosted solutions, the event that will land a provider in the news is a breach involving 100's of records and, based on my experience, this is less likely to happen with a service provider.

Mary Pat: Are HIPAA violations more likely to happen with larger practices, or are larger practices more likely to self-report?

Steve: I honestly don't have a good bead on that. If by "HIPAA violations", you mean unauthorized disclosure of PHI, then I would guess it mimics pretty well the demographics. In other words, the percentage of violations in large practices roughly

approximates the percentage of physicians in large practices. Larger practices seem to do a better job at having incident reporting and response procedures in place and, if this is true, they would be more likely to self-report. But I'm just guessing.

Mary Pat: What importance does the new HIPAA Omnibus Rule have for medical practices?

Steve: I partially covered this in my earlier response. The most significant change is to the breach notification rules. The new rules replace the "no harm" standard with a "probability that data was compromised" standard. The "no harm" standard does not require improper disclosure of protected health information (PHI) to be reported as a "breach" unless "significant risk of financial, reputational, or other harm to the individual" whose data was exposed. This regulation was overturned for being too subjective. According to the new standard, an improper disclosure does not need to be treated as a breach if the covered entity can demonstrate "that there is a low probability that the PHI in question has been compromised." I am not sure how much less subjective that is but I think it will make the need to report a breach more likely.

I have written a pretty extensive summary of the new laws on my blog in a three-part series. **Part One is here.**

Mary Pat: Can you explain what BYOD means and why it is a security concern in healthcare?

Steve: BYOD stands for Bring Your Own Device. It essentially describes the use of personally owned devices such as iPhones, iPads, Android phones and tablets. Enterprises are reluctant to buy these devices for all employees due to cost. However, their use has potential benefits for organizations but also presents some security concerns. The class of devices normally associated with BYOD is mobile devices which are generally a

higher security concern due to the risk of theft or loss. However, that risk is increased with personally owned devices because organizations don't have the "control of ownership." If I am your employer and I hand you your own laptop, you won't think twice if I tell you, "here are the rules about what you can and can't do with that laptop." That ability to make rules, manage behavior and apply technical controls is much easier and clearer when an organization owns a device. It's harder if you don't. However, regardless of who owns a device, that control is essential! The only way BYOD can work from a security standpoint is if management can dictate the rules and controls for the use of personally owned devices. So a physician who wants to use his own iPad should be required to abide by all the policies of the organization such as limiting what applications can be installed, requiring a good complex password, enabling encryption, enabling auto-wipe in the event of multiple unsuccessful logon attempts, etc. There is a type of software called Mobile Device Management that can help enterprises with this effort. In the case of iOS devices, Apple has published some great resources to help companies with this effort which can be found **here.**

Mary Pat: I see that you offer free security tools on your website – what are they?

Steve: They are a hodge-podge of various tools and resources that I have gathered or developed that I have found to be particularly useful. My favorites are the security posters. (*In fact, for the first five readers of this interview that **fill out the contact form on my site here**, I will send full color, 11×17 versions of the "Seriously" and "Bad Links" posters in the mail for free!*) We have some new posters in development which we will be releasing soon. Although not in the free tools section of the website, I have gotten a lot of positive feedback on the Ten Steps to HIPAA compliance, which goes along with one of my most popular presentations. I also really like the free tools from Sophos.

Mary Pat: What question(s) do you wish I had asked?

Steve: I have always wanted to be asked, “Why are you so devilishly handsome?” But it has yet to occur.

How about this question: Should practices outsource their meaningful use risk analysis or do it themselves?

My answer is multi-faceted. If the following two things are true, then it may make sense for a practice to do their own risk analysis. 1) You have access to some IT resources with at least some expertise in IT security and HIPAA. 2) Your objective is just to be able to attest in good faith to meaningful use and the actual security of your information systems is not really a big concern. I might advise a client where those two conditions are met to do their own risk analysis. Let me elaborate on them a bit. Many clinics outsource their IT to outside vendors. Occasionally those vendors are willing to make a meaningful commitment to understanding the risk analysis process as defined by NIST SP 800-30 and to understanding the HIPAA requirements. This is very unusual but not unheard of. In most cases though, IT vendors will readily acknowledge that they do not understand the requirements and are not comfortable being called on to fulfill them. In fact, one of the biggest sources for me of customers are these IT vendors that do not wish to take on the liability associated with HIPAA. Unfortunately, many practices assume that their IT vendor is meeting its HIPAA obligations. This is both unwise and unfair. If this is a practitioner’s expectation, then get it in writing. Adjust your service level agreement to reflect this fact. For most IT vendors though, they are going to charge the customer anyway for their compliance and training efforts.

In some cases, larger practices may have these resources internally. The practice might have its own IT staff and someone could be assigned to the role of HIPAA security compliance and could be given the responsibility and resources

to know and understand what needs to be done and to doing it. Large practices are the ones in which I am most likely to encourage an internally conducted risk analysis.

The point of #2 reflects the reality that many practices just want to be able to do enough to show a good faith effort that will allow them to receive their meaningful use check. Go through the process and assembling documentation to prove that a provider has conducted a risk analysis is not quite as hard as actually securing ePHI. I have conducted a half a dozen risk analysis for clients where I was doing a review or follow-up of a previous risk analysis. In every case, I was able to uncover medium to severe security risks that needed to be mitigated.

Even the Office of the National Coordinator, although clearly disclaiming that a risk analysis must be outsourced, encourages the risk analysis to be conducted by third parties. In its Guide to the Privacy and Security of HIT they state (p.17):

> ***Select a qualified professional to assist you with the security risk analysis. Your security risk analysis must be done well or you will lack the information necessary to effectively protect patient information. Note that doing the analysis in-house may require an upfront investment developing a staff member's knowledge of HIPAA and electronic information security issues. Use this opportunity to have your staff learn as much as possible about health information security.***
>
> ***You however, can conduct the risk analysis yourself. Just as you contract with professionals for accounting, taxes, and legal counsel, so, too, outsourcing the security risk analysis function can make sense….If you need to, outsource this to a professional; a qualified professional's expertise and focused attention will yield quicker and more reliable results than if your staff does it piecemeal over several***

> ***months. The professional will suggest cost-effective ways to mitigate risks so you do not have to do the research yourself and evaluate options.***

Steve Spearman, Founder and Chief Security Officer for Health Security Solutions, has been in the health care industry since 1991. After spending more than a decade observing health care providers struggle with the HIPAA Security and Privacy regulations, he founded Health Security Solutions in the summer of 2010 to help organizations minimize and mitigate the financial, legal, and compliance risks associated with running health care organizations.

Steve alongside his team of security experts, have helped healthcare providers qualify for millions of dollars worth of stimulus funding through a wide range of HIPAA consulting services and solutions, including his very own risk assessment method, **Risk Analysis in A Box**.

To learn more about Steve, Health Security Solutions, and the services they provide please visit **www.healthsecuritysolutions.com.**

---

76 Ways to Use the Cloud in Your Medical Practice (or Any Business)

I've had a lot of questions since last week when I offered to help readers "get on the cloud." Most people want to know – what exactly does getting on the cloud mean?

The term cloud comes from both the look of technical drawings

which depict the relationship between cloud services and consumers, and is also a metaphor for the fact that cloud service providers exist out of sight in some distant location. My favorite definition of the cloud is “Using the Internet to store, manipulate and deliver data.” Here are 76 ways to do just that!

SECURITY & RISK MANAGEMENT

1. Decide user by user which files and folders each employee or stakeholder may have access to. Decide if the user may view information, upload information, download information, invite other collaborators or edit documents. Change the user’s permission instantly, or eliminate their access to everything on the spot.
2. Store critical documents: letter of incorporation, Tax ID assignment, Medicare letters, shareholder agreements, by-laws, etc.
3. Scan in any and all documentation of lawsuits and or legal correspondence about patients.
4. Collate logon information for important sites: CAQH, NPPES, PECOS, state board, specialty board, etc.
5. Collect all information needed for credentialing and privileges for all providers in one easy place: CV, photo, license, board credentials, DEA, state registration, malpractice, references, etc. Keep copies of all credentialing applications in the same file.
6. Keep a licensing and privileges spreadsheet for all professionals so deadlines don’t take you by surprise. Include CPR, ALSC, DEA, state licenses, and board certification and recertification.
7. Never worry if you’ve locked your office, your file cabinet or your desk again. Your information is safe in the cloud.
8. Store important logons and passwords on the cloud along with instructions and know that if something happens to you, the business will recover quickly.

9. Have employees watch for health fairs and special events that your practice can participate in. Develop a calendar for community events that you can prepare for annually.

INFORMATION SHARING

1. Share files up to 2GB (images, video, audio, text)
2. Turn a folder into a public web page.
3. Start a secure referrers' area and give access to those practices that refer to you. Stock it with FAQs, referral forms, maps and directions to your practice, and phone numbers and emails for communication. Keep a referrer satisfaction survey on their pod at all times.
4. Push the patient schedule into the cloud so any provider can check their schedule at any time from anywhere.
5. Store building or suite blueprints.
6. Develop a practice glossary to document all abbreviations and specialty-specific terminology – very helpful for new employees and transcriptionists.
7. Make a secure education area for your patients which they can access from your website or in your waiting area on iPads. Include websites, blogs, patient satisfaction and other surveys, health tracking programs, etc.
8. For those providers on productivity bonuses, push a productivity report to the cloud for them to review privately.
9. Put staff education programs on the cloud for new employee orientation and annual training on compliance, OSHA, HIPAA, fire safety and disaster communication plans.
10. Post photos of the office picnic or Christmas party, or the new baby, or the bride and groom.
11. Use the cloud as a digital scrapbook of events, new employees, new services, accolades, advertising or publicity.

12. Pass around a digital birthday greeting card to all staff except the one having the birthday!
13. Post a job on craigslist. Once you have a group of candidates you want to consider, give them a link to a folder with the position job description, benefits schedule and in-depth information about the hiring time line.
14. Post lunch menus for restaurants and take-outs within several miles of the practice so employees can get lunch efficiently and quickly.
15. Post the office schedule for the year showing which dates the office will be closed for holidays.
16. Post the call schedule and let your answering service and the hospitals view it.
17. Publish your weekly practice newsletter on the cloud – it becomes an instant record of when and how things were communicated.

BUSINESS MANAGEMENT

1. Scan invoices to the cloud for storage once you've paid them.
2. Scan invoices to the cloud for an external bookkeeper to access and pay them.
3. Scan invoices to the cloud for a physician to approve them for payment.
4. Scan the daily accounts receivable work (EOBs, checks, deposit slips, denials, reconciliations) to the cloud and shred the originals at the interval of your choice.
5. Scan documents to the cloud when you are notified that employees are having monies withheld from their paychecks for child support or garnishment, or when they change their deposit information or retirement plan contribution.
6. Track the history of files and folders – when did we change this policy? When did we go to this compensation system? What was the original wording of this contract?

7. Generate reports on employee productivity, looking for patterns of collaboration and innovation.
8. Scan RAC, CERT, ZPIC and other audit letters when they come and keep a spreadsheet of dates records and appeals are due.

COLLABORATION

1. Have online meetings centered around documents in the cloud.
2. Post job protocols and empower employees to change protocols regularly as information and routines change.
3. Start a CME log for each provider that the providers can easily add to.
4. Have your employees collect stories, links and other items in the cloud to push to your Facebook page or website blog.
5. Keep minutes from physician meetings and request all physicians review, ask for changes and sign off.
6. Keep attendance and minutes from staff meetings and ask all staff to electronically sign the minutes.
7. Have each employee keep a continuing education log for face-to-face and online education.
8. Assign tasks. Place something on the cloud and assign staff to respond to it, change it, develop it or implement it.

INCREASE EFFICIENCY

1. Develop a “How Do I?” document for quick information new employees need to know and established employees may not remember. Some examples: How do I reach the inclement weather information line? What do I do if there is a blood spill in the practice?
2. For the manager – develop a staff roster with dates of hire, dates of birth, social security numbers, phone numbers, hourly wage and termination dates. One document

will answer 25% of questions you have or others ask you every day.
3. Standardize protocols and information when you have multiple sites or divisions.
4. Show each employee how to keep their most-used files on their digital desktop to access without a logon and password.
5. Sync desktop folders to cloud folders automatically – documents are updated to the latest version without thinking about it.
6. Restructure your files and folders as many times as you want or need to. Rename files, move and copy files, and delete files if they are not serving the purpose you thought they would.
7. Expand the number of users instantly for special projects.
8. Put every form on the cloud, have employees complete them on the cloud, sign them electronically, then share them with you for your electronic signature.
9. Put new templates or forms on the cloud for everyone to draw from – eliminate old letterheads, logos, addresses, etc. instantly.

IMPROVE MOBILITY

1. Fax documents from the cloud to a fax machine.
2. Email files from anywhere.
3. Search for anything in your cloud by words or phrases. Never lose anything again!
4. Access the cloud from anywhere and from any device – smartphone, PC, iPad…
5. Put the patient schedule information into the cloud so if inclement weather hits, staff can access the schedule at home and contact patients about their appointments.
6. Access your business 24/7/365.

DAY-TO-DAY MANAGEMENT

1. Assign a folder for your CPA to be notified when financials are available for download, or for you and the physicians to be notified when s/he finishes the financials or taxes.
2. Assign a folder for your benefits broker to be notified when new employee applications for medical and dental benefits are available for download.
3. Assign a folder for your banker to be notified when quarterly financials are available for download.
4. Assign a folder for your physicians/owners to be notified when monthly or quarterly financials are available for their review.
5. Post practice calendars for paid time off requested and approved.
6. Develop a physician referral resource tool if your PMS does not organize that information well. Create your own spreadsheet with all the fields of information that are important to your practice and have all employees add to it and correct it routinely. Have someone in the practice or a temp or prn person call every practice/group on the list twice a year and confirm all the pertinent information.
7. Post a "Who Covers Whom" list that spells out who covers primary responsibilities in the practice when someone is out of the office. Building your team 3 deep (for every primary task, there are at least 3 people that can perform that task) is crucial for reducing vulnerability.
8. Video new employees answering a few questions about themselves and post it on the cloud for all staff to view.
9. Put video of all staff introducing themselves and telling what they do on the cloud for new employees to view.
10. Video benefit providers discussing benefits so employees

can watch at any time – medical insurance, dental insurance, vision insurance, short and long-term disability, life insurance and retirement benefits. Employees will get more out of and become more aware of what their benefits are.

11. Make an easy-reference spreadsheet with the payer contracts listed and images of the plan cards for staff to be able to identify the contracts and plans in force at any given time.
12. Keep personnel files on the cloud. You may choose to have a file of documents the employee may see and get a copy of, and a file of documents they may not see or get copies of. Both can be a part of the same folder.
13. Store scripts for your messages on hold, your after-hours message and your scripting for employees.

SAVE MONEY

1. Increase storage space without buying any hardware or software.
2. Scan charts into the cloud as a preliminary repository before implementing EMR, or scan charts of inactive patients in so you don’t have to pay to store them offsite.
3. Never back-up your documents on your computer again.
4. Put your triage algorithm or flow sheet on the cloud. Hire nurses to triage from home.
5. If a manual doesn’t come electronically, scan it onto your cloud. Check the manual before you call the repairman.
6. Preserve your valuable employee knowledge – have each department develop a folder with the important resources for their staff. The billing department may have websites they refer to for coding questions, a primer on evaluation and management coding, a cheat sheet on standard practice fees, and a calendar for the times of the year that different updates and revisions to CPTs,

ICDs and NCCI edits.

Cloud Pre-launch Offer: We'll Get You On the Cloud for Free

We're not quite ready to roll out my new web, social media and cloud solutions company, but I am extending a special offer through the end of April for the Manage My Practice readers who want to know what this cloud business is all about.

Read my post **here** on 76 ways to use the cloud in your medical practice.

Here's how it works.

1. Contact us during the month of April and we'll get you set up on a free Box.net account – no credit card required!

2. We'll do a phone assessment of your pain points and tell you how a cloud can help.

3. We'll teach you how to use Box.net and how to organize your practice or yourself on the cloud (but you'll have to do all the heavy lifting!)

That's it.

If you are interested, contact Abraham Whaley **here.**