Is Dropbox Putting Your Medical Practice's Compliance Plan at Risk?

Since its release in 2008, Internet File Storage tool Dropbox has been a big hit with people who have to keep track of files on multiple computers. Users can download a free program that lets them upload files to "the cloud" (see: a server or servers connected to the Internet), and then can access the files on any other device: other PCs or Macs, any web browser, even a smartphone or tablet. The program puts a small, "dropbox" in the bottom corner of the user's screen and any file dragged into the icon is automatically uploaded. When the user looks at the dropbox on another device, the file is there waiting.

Dropbox has been wildly popular because it is extremely useful: it saves people time and makes them more productive, and is free for the first 2GB of storage. Users can either earn more free storage by referring friends to the program, or purchase more storage with plans that start at $9.99 per month. There are also group plans that allow for centralized file sharing.

In fact, some of your employees could be using Dropbox in your practice right now to let them work from home or the road, or sync multiple work computers, or even give them access to work data on their mobile devices. As all healthcare management professionals know, this has the potential to be a huge problem. The data that is handled in many daily tasks in a medical practice is protected not only by patient confidentiality, but also by federal regulations with some serious financial teeth. On Dropbox's website, they go after the question head on:

> *"Unfortunately, Dropbox does not currently have HIPAA, FERPA, SAS 70, ISO 9001, ISO 27001, or PCI certifications. We'll update this page with any new certifications as we receive them, so please do check back"*

Dropbox is very useful for students, people on the go, and anyone who works from different places and different computers, but it's not really designed for auditable, granular protection of sensitive data. This isn't to say Dropbox isn't safe or secure – although they've had a few problems, they've taken steps to ensure they aren't repeated – they just aren't designed for the security needs of healthcare organizations. Even a great password policy in place for your group won't help if you are relying on tools that were not built for the industry.

So what can a practice do if it needs a cloud-based file hosting solution that can help your team work in different places without jeopardizing your compliance? At Manage My Practice, we use and endorse Box, a leading provider of enterprise class file storage. We like Box so much for healthcare purposes that we partnered with them to bring you FileConnect. Using the power of Box, which has installations in over 80% of the Fortune 500 companies, FileConnect supplies fully auditable, granular file storage to your practice while working in lockstep with your existing HIPAA compliance plan.

Click below to contact us to learn more about what FileConnect can do for you!

Click Here to Talk to Us About Fileconnect in Your Practice!

12 Ways to Supercharge Your Practice in 2012: #8 Leverage "The Cloud" for Real Results

Is Your Practice Struggling?
Click Here for 12 ways to
SUPERCHARGE IT!

Three technology trends are creating big opportunities for healthcare providers and managers to improve their bottom line, drive savings, and empower a mobile workforce with "The Cloud":

1. **Improved cellular and network access to the Internet at all times, from all devices.**
1. **More powerful, less expensive smartphones and mobile devices to harness this improved access.**
1. **The move to deliver computing services to these mobile devices, as well as traditional personal computers through these ubiquitous, powerful Internet connections, so that most of the work is actually done "In the Cloud"- saving a lot of resources.**

The Cloud is more than just a fashionable concept – this is a **real change in the way people work**– and leading organizations are looking past the buzz into the substantive improvements that technology can offer in work flow and cash flow.

NOTE: For those who have not heard the term before, you can

> *always substitute "the internet" for the cloud. Do you get your email in a web browser? Cloud-based email! Do you like to stream your movies to your TV? Media in the cloud! Do you have anywhere you save important stuff online for either security or posterity? Yep – this is cloud-based storage!*

By relying on offsite computing power and a constant high-speed Internet connection, the Cloud has all sorts of advantages over a traditional, on-premise model.

How can the Cloud change your practice today?

The cloud can actually protect things better than you can. For less money.

If you have your valuable documents stored in on-site servers, or on personal desktops, you are at risk. Cloud services offer auditability, encryption, and redundancy, and with strong end-user security practices in place, can provide healthcare organizations with absolute top of the line data security AND put the replacement and maintenance back on the vendor. **You pay for access, and pay only for what you need.**

Moving documents to the cloud not only protects them physically, but keeps them at your fingertips and the fingertips of permissioned users. **Separated data facilities, redundant storage, and professional grade encryption are all more secure than the traditional, "server in the closet" model.**

The cloud can mobilize your practice, but keep everyone on the same page.

The modern medical practice employs providers and administrative and clinical staff that bring powerful mobile devices to work everyday – and take them home too. By giving your key decision makers access to their work files outside of the office, you give them the tools of a work computer anywhere they go. Physicians can handle office tasks on their own schedule, and in their own setting. Administrators can access critical documents from a phone, or a home laptop as easily as they would their desktop. **The access you pay for is *everywhere*: if you have a web or wireless connection, you can access your files**.

Tedious, in-house FTP setups, or VPN'ing into the network can be complex and costly solutions; work-arounds like emailing yourself the work files you need, or loading USB flash drives can introduce security risks. And, how can you be sure you remembered to send the latest version? If your work data is hosted in the Cloud, the availability of what you are working on is as much of an afterthought as the lights and water at your office. Updates to files are pushed to everyone immediately too, so you know your team always has the latest. **With mobile applications and network access, employees can not only work from home – they can work from anywhere they have a mobile device and service.**

The Cloud turns computing power into a utility.

In terms of your practice cash flow, cloud computing enables you to flatten IT spending into a much more predictable outlay. If you own your server, you are very familiar with the "update cycle". Determining the right time for updates,

upgrades, replacements and expansion to keep up with your needs, comply with new regulations, ease pain points for the staff, or improve security can be an endless loop of spending lots of time and money.

In effect, a practice is never out of the upgrade cycle, they are only on the easier end of one for a while. The cloud allows you to simply pay your monthly access and storage fees to your providers, and change plans as soon as you need more or less. **Upgrades are pushed automatically, and built into monthly fees.** You "pay as you go" for what you use – and only that. *Scaling* your IT resources up and down as you need them lets you fine tune your budget to your needs, and lets you turn your upgrade cycle into a predictable fixed expense. **Employees can "B.Y.O.D." or "Bring Your Own Device"- to give them a familiar hardware and software interface, and to give employers lower hardware costs.**

How many of the things on this list are taking up space in your office, and are at risk of being misplaced? How many can you locate and share with your employees, physicians and stakeholders right now?

- *Physician Credentials, Privileges, Re-appointments, CME*
- *Monthly and Quarterly financials*
- *Daily work – Deposit slips, EOBs, Checks, Superbills*
- *Practice Management reports*
- *Accounts Payable invoices*
- *Contracts*
- *Partial or full paper charts that will not be included in the EMR*
- *Personnel files*
- *Personnel policies and employee handbook*
- *PTO requests*
- *Board agendas and minutes*

- *Applicant resumes and paperwork*
- *Benefit plan books*
- *Retirement plan documents*
- *Tax documents*
- *Agendas and Minutes of Staff and Board Meetings*
- *Policy changes and reviews*
- *Templates and forms*
- *Equipment user manuals*
- *Referring physician holiday card or gift list*
- *Anything else stored offsite or in your office that doesn't need to be taking space and costing $$$*

Where do I start?

Manage My Practice thinks leveraging the cloud is an important way for medical offices to achieve efficiency and reduce costs. In fact, we think it is so important that we have partnered with cloud leader Box to bring you MMP Fileconnect – a product specific to healthcare that allows you to manage your practice documents from anywhere. Box has installations in more than 70% of the Fortune 500 companies, and we think it's the right product for you. Contact us to learn how Fileconnect can start helping your practice today!

What Can We Learn About HIPAA

From Phoenix Cardiac Surgery?

Phoenix Cardiac Surgery probably never thought they would be a poster child for HIPAA safeguards, but this 5-physician cardiothoracic practice in Prescott, Arizona has become famous for something no medical practice wants to be famous for – not protecting their patient information.

Today's HHS Press Release reads as follows:

HHS settles case with Phoenix Cardiac Surgery for lack of HIPAA safeguards

Phoenix Cardiac Surgery, P.C., of Phoenix and Prescott, Arizona, has agreed to pay the U.S. Department of Health and Human Services (HHS) a $100,000 settlement and take corrective action to implement policies and procedures to safeguard the protected health information of its patients.

The settlement with the physician practice follows an extensive investigation by the HHS Office for Civil Rights (OCR) for potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The incident giving rise to OCR's investigation was **a report that the physician practice was posting clinical and surgical appointments for its patients on an Internet-based calendar that was publicly accessible**. On further investigation, OCR found that Phoenix Cardiac Surgery had implemented few policies and procedures to comply with the HIPAA Privacy and Security Rules, and had limited safeguards in place to protect patients' electronic protected health information (ePHI).

"This case is significant because it highlights a multi-year,

continuing failure on the part of this provider to comply with the requirements of the Privacy and Security Rules," said Leon Rodriguez, director of OCR. "We hope that health care providers pay careful attention to this resolution agreement and understand that the HIPAA Privacy and Security Rules have been in place for many years, and OCR expects full compliance no matter the size of a covered entity."

OCR's investigation also revealed the following issues:

- Phoenix Cardiac Surgery failed to implement adequate **policies and procedures to appropriately safeguard patient information**;
- Phoenix Cardiac Surgery failed to document that it **trained any employees on its policies and procedures** on the Privacy and Security Rules;
- Phoenix Cardiac Surgery failed to **identify a security official and conduct a risk analysis**; and
- Phoenix Cardiac Surgery failed to obtain **business associate agreements with Internet-based email and calendar services where the provision of the service included storage of and access to its ePHI.**

Under the HHS resolution agreement, Phoenix Cardiac Surgery has agreed to pay a $100,000 settlement amount and a corrective action plan that includes a review of recently developed policies and other actions taken to come into full compliance with the Privacy and Security Rules.

Individuals who believe that a covered entity has violated their (or someone else's) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rule may file a complaint with OCR at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html.

The HHS Resolution Agreement can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf

Additional information about OCR's enforcement activities can be found at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.

What Can We Learn?

1. **You won't escape the notice of the HHS just because you are a small practice.** Every practice, hospital, facility, healthcare entity and anyone that has access to Protected Health Information (PHI) must be compliant with the HIPAA Privacy and Security Rules.
2. **Patients are paying attention and want their information protected!** Patients will not hesitate to report a practice if they feel their privacy is being breached. Let your patients know that you take their privacy seriously and what you are doing in your entity to protect their privacy.
3. **Physicians are not exempt from responsibility.** Most physicians do not want to use the hospital or practice network email – they want to use their personal Gmail, Yahoo, Hotmail or AOL account for office business. This is a bad habit. Emails to and from the physicians announcing meetings and reminding them of tasks are fine, but it is easy to forget and use personal email to hand off patients, discuss appointments and ask for refill approvals. Non-secured email services are NOT the right way to send any patient information.
4. **Understand your technology.** This is why the risk assessment is so important – you must identify any process or technology you are currently using that has the potential for PHI to be accessed inappropriately. Understand and mitigate your risk!

;

Resources

Health Information Privacy for For Small Providers, Small Health Plans, and other Small Businesses here

Summary of the HIPAA Privacy Rule

Summary of the HIPAA Security Rule

There are lots of resources available from the AMA, your state medical society, your specialty society and MGMA. There are also a number of consultants specializing in this area.

Don’t forget to talk to your IT person – they should be looking after your best interests and helping you with privacy and security issues.

For practices looking for a secure place to share files and collaborate on documents with encrytpted upload and download capability, please consider FileConnect, a product brought to you and supported by Manage My Practice. For more information, call Abraham at 919-370-0497 or email him at abe@managemypractice.com.

Collections Basics – Part 1: Know Your Payers

In a traditional healthcare setting, the revenue cycle begins with the insurance companies who pay the majority of the bill. There are multitudes of payers and each payer can have many plans. How can a healthcare organization catalog this information, keep this information updated and make this information easily accessible to staff so they can discuss payments with patients in an informed and confident way?

Start by breaking your payers into five main categories as a logical way to organize the data.

1. Payers with whom you have a contract
2. Payers with whom you do not have a contract
3. State and Federal government payers (Medicare, Medicaid, TriCare)
4. Medicare Advantage payers
5. Patients

Payers with whom you have a contract

Your organization has signed a contract with a payer and you have agreed to accept a discounted fee called an allowable, and to abide by their rules. What is the information you need to collect?

- A copy of the contract
- A detailed fee schedule, or a basis for the fees, such as “150% of the 2008 Medicare fee schedule.”
- Any information about the fees being increased periodically based on economic indicators, or rules (notification, timeline, appeals) on how the payer can change the fee schedule.
- The process and a contact name for appealing incorrect payments.
- Information on what can be collected at time of service. Hopefully your contract does not have any language that prohibits collections at time of service, but you must know what the contract states.
- Process for checking on patients’ eligibility and benefits: representative by phone, interactive voice response (IVR), website or third-party access.

The contract allowables should be loaded into your practice management system so you can calculate the patient’s responsibility at check-out and you can identify incorrect payments at the time of check-posting. If your practice

management system does not have this feature, you will need a cheat sheet for each contracted payer, showing the most common services, the allowables, and the percentages of the allowables for fast calculation of the patient's portion at check-out. The same or a modified cheat sheet will work for the check posters so they can verify the payer is reimbursing according to the contract.

Your cheat sheet should look like this:

Plan A							
Service	Allowable	20%	40%	50%	60%	80%	90%
99213	75.00	15.00	30.00	37.50	45.00	60.00	67.50

The check-out staff will write the patient's portion on the encounter form (you may call it a charge ticket, fee ticket, rounding slip, or superbill), add the numbers together and give the patient the total. Alternately, the computer system will total the patient's portion based on the payer and the plan for the check-out person.

The balance of the information collected will be used to develop a payer matrix that might look something like this:

Payer	Employers	Collectible At TOS	Elig/Benefit Verification	Plan Year	Contract Dates	How to Notify
XYZ	WalMart	Deductible & Co-Pay	website	July-June –	Exp Dec 2013, must neg. <Aug1, 2012	Call June Jones at 1-800-555-1212
	State Employees	Deductible & Co-Ins.	Website	Jan –Dec	same	same

Another excellent way your organization can catalog payer and plan information is electronically in a document management system such as **FileConnect,** which I use and recommend.

FileConnect is an electronic filing cabinet with many great attributes, one of which is particularly helpful in this

scenario. Every time there is a change in a payer contract, or a new plan is added by a local employer, you can update the staff's spreadsheet tools simultaneously and the newest version will be instantly available on their desktops.

Payers with whom you do not have a contract

Your primary payers in your community or region will most likely offer you a contract. Payers with less covered lives will not find it worthwhile to contract with healthcare providers, so you must decide how you will work with these companies and with these patients.

You are not required to file claims with payers that you are not contracted with. Most healthcare providers do file claims with non-contracted payers to ensure patient satisfaction. Where providers may differ, however, is whether or not they will ask patients with non-contracted payers to pay in full at time of service, and assign the payment to the patient OR ask the patient to pay only the expected patient portion at time of service and assign the payment to the provider. This decision will be made as part of your Financial Policy (covered in Part 2.)

State and Federal government payers (Medicare, Medicaid, TriCare)

There has been a tremendous discussion in healthcare for the last several years about physicians limiting how many Medicare patients they will see, or even discontinuing to see Medicare patients completely. The rate at which Medicare pays is not enough to support the provision of services in most ambulatory practices, so some physicians do not participate in the Medicare program but still see Medicare patients (the fee they can charge Medicare patients is federally controlled and is called the "limiting" charge) or have opted out of the

Medicare program altogether and will see Medicare patients on a cash basis only.

If a practice does accept Medicare patients, whether participating or not, there are set amounts to be collected from patients with Medicare – deductibles and co-insurance, as well as services that are never covered by Medicare.

Make sure that current Medicare allowables for your locality are loaded into your computer to do the math for you. You can use the same type of spreadsheet shown above to develop a cheat sheet of 80% of the Medicare allowable.

Service	Medicare Allowable	20% Owed by Patient
99213	66.74	13.34

What is confusing to most providers is what an insurance that is secondary to Medicare will pay. Many providers do not collect any fees at time of service for Medicare patients with a secondary payer, as there may or may not be any balance left that is the patient's responsibility.

Medicaid pays less than Medicare does, and based on the very low fee schedule, many ambulatory providers will not accept Medicaid patients. Many Medicaid patients must depend on health departments, hospital clinics, federally-qualified health centers (FQHCs) and rural health clinics (RHCs) for care.

Tricare may be accepted on a case-by-case basis. A healthcare provider does not need to accept the health insurance for retired military across the board, and may decide individually whether to accept a Tricare patient or not.

Medicare Advantage

Medicare Advantage Plans, formerly called Medicare Choice + and now called Medicare replacement plans or Medicare Part C,

are plans offered by non-government payers which replicate Medicare benefits for seniors, sometimes offering enhanced benefits as part of the package. There are several types of Medicare Advantage Plans, but the main types are local or regional HMO plans which require you to sign a contract, and the Private Fee For Service Plans (PFFS), for which no contract is required. If you see a Medicare Advantage PFFS patient, you have in essence agreed to accept their terms. The one thing you should ask prior to accepting a Medicare Advantage PFFS plan/patient, is what percentage and what year of Medicare rates are they paying.

Patients

So we finally arrive at the payer with whom most healthcare entities have the most difficulties – the patient. Why is it so difficult to collect from patients?

First, as we have seen throughout this article, insurance can be very confusing. Without a plan for organizing and sharing information, a healthcare provider may have significant difficulty assessing the patient's payment responsibility.

Second, it has been a cultural norm until recently that patients do not have to pay at time of service, with the exception of their co-pay, and will be billed for their portion after insurance pays.

We know now that we must collect the correct payment at time of service. This is the only way to reduce the administrative expense of billing the patient for the balance and/or refunding the patient if too much has been collected. This is also the only way to maintain adequate cash flow as much of what used to be paid to the providers from insurance companies has now become the responsibility of the patient. Higher co-pays, higher co-insurance and most of all, extremely high deductible plans have left patients owing much more out-of-

pocket and largely being unprepared to pay it at time of service.

In the next part of this series, Collections Basics Part 2: Develop Your Financial Policy, we will discuss setting up your financial policy so both patients and your staff can understand it, and how to collect from patients according to your policy.