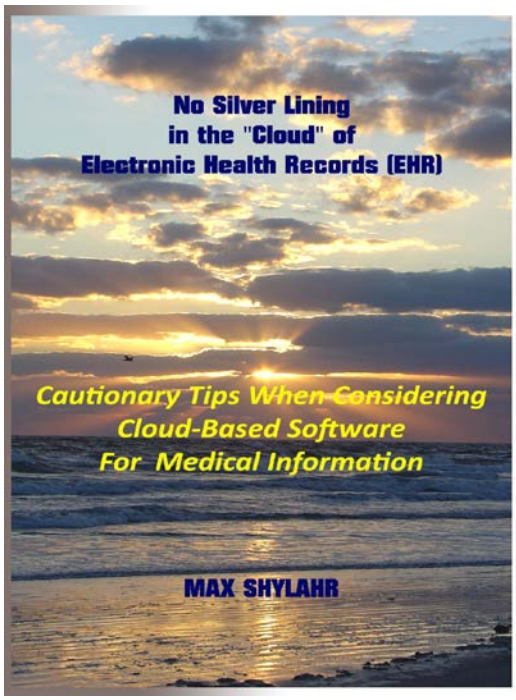

CONSIDERING THE CLOUD?

In addition to selling in-house software, we also have cloud-based offerings. The cloud offers convenience, 24/7 accessibility and continual upgrades. Please understand the following caveats before jeopardizing your patients' info.

LIABILITY: Patient information is listed as the number one target of identity thieves and needs to be protected at all costs. It contains your patients' Social Security info, life threatening illnesses, medications, mental illnesses, where they work, where their children go to school, next of kin info and more.

People have been kidnapped, robbed, fired, bullied and even killed based on far less information than what you possess. As patients blindly sign their forms, entrusting you to protect their family's information, they have no idea which software packages you are considering and/or where their very personal data is being stored. They simply trust you.

Do you have any celebrity or political clients? Consider what chaos might ensue should their data be jeopardized or you can't get to their medications list. Granted, this is a worst case scenario, yet not too far-fetched. Forget malpractice suits. The new legal wave, will have to do with WHAT a thief does when they get their hands on your patients' data.

VULNERABILITY: In your office, you have a finite number of employees that you have personally hired. Once you fire them and they leave your door, they can no longer access your data unless of course, you have a cloud-based system they can access from anywhere. They could potentially destroy data before they leave your parking lot.

In data centers where cloud-based systems are stored, there are hundreds, sometimes thousands of employees. You have no idea who lurks in the computer rooms or what hiring practices they use or enforce. Just one disgruntled employee using the right codes can destroy or steal your data.

Where is your data? Although the corporate address says "Good Ole U.S.A.", many Tier 4 data centers with the highest HIPAA compliancy have servers in China, India, Portugal and more. No matter what is "said", once you go online, you truly have no idea where your data resides.

"But, the banks use the cloud!" Yes, and banks have been repeatedly hacked over the past few years (CitiGroup, MasterCard, Sony, et al). Should you chose to change bank accounts, you withdraw your money. It's a one item deal involving moving a series of digits. Again, it's just money, not lives. Should you choose to change your software, it may be very difficult to retrieve your data in a usable format for a different program. That process alone can take weeks or months, costing thousands of dollars.

CONTINUITY: Software companies can change ownership any given day. They do. Within 5 years, Medisoft was sold to NDC Health, which was later bought out by Per-Se Technologies, later bought out by McKesson. Medisoft went from having over 700 dealers to down to just over a hundred. Another long-established EHR company recently decided to discontinue its cloud-based offering. Wouldn't that be a heck-of-an-email to start your day? Your cloud system could easily be sold to a company in a country not governed by HIPAA. Who will own your data next year?

ACCESSIBILITY: If/when a cloud based company is shut down even temporarily for any reason, for example, if the government has any need to investigate wrong-doings, breaches, etc., you lose access to your data. Even Yahoo's management was recently shaken up over a CEO lying on his resume! What if a cloud-based EHR CEO is caught selling information (there's huge money in that, by the way)? Their servers could be shut down for an indeterminate amount of time until any issues are resolved.

With an in-house system, should the company that originally made the software go out of business, your program continues to work. You have the data safely on your computer. In most cases that data can be easily converted for use in another program whenever you do decide it is necessary.

Still need 24/7 remote access? You can set up one of many secured remote access programs to connect to your office's server. Microsoft Server includes a two user Remote Desktop application which can easily be expanded as needed. Whether or not you use the cloud, a quality firewall appliance is advised to protect your network.

A *great* use for the cloud would be automated, encrypted backups which would save the day should your server crash. If your backup company ever gets shut down, you'll still have the originals on your own computers. Simply find another secure backup company and re-backup your data.

AFFORDABILITY: Cloud companies do not SELL software. They RENT it... forever. "FREE" systems? Those too can easily hit you with fees and raise fees at any time down the road, especially once they have a few thousand of your records in their system. Imagine the downtime of starting over, once you are unhappy with your cloud company?

Personally, I love the concept of perpetual income, who doesn't? If a client insists on paying for a cloud-based system, with a complete understanding of all the risks, we are resellers for several of the top cloud-based ONC-ATCB-Certified EHR systems in the country. We have teamed up with Business Continuity Management Professionals (BCMPros) to ensure the highest vigilance is kept over those you do business with. Let's talk.

FALLIBILITY: Cloud companies will argue "What if your own network fails?" Good point. The simple answer… get good computers. Today's computers are very inexpensive and you need a good, solid network anyway for day to day operations (printer sharing, marketing/graphics programs, payroll programs, presentation software, video editing, etc.).

Besides, if just your Internet router or network switch fails (YOUR ONE CONNECTION FOR ALL COMPUTERS IN YOUR OFFICE), no one can get to your cloud data anyway, right? With most in-house systems, as long as you can get at least ONE computer up and running, you can still have a functioning office.

DEPENDABILITY: Cloud-based companies control what they add or remove and when they add it to their programs. You have no choice but to accept it. With an in-house system, YOU decide if you want to install any updates or upgrades. If your program is working fine, seriously, why would you make changes?

Before NPI numbers were assigned, most practices did not need to upgrade their software for many years. After the ANSI 5010 and ICD-10 changes are handled, a practice may not have a need to upgrade their software for another decade. Cloud users will still be forced to pay "rent" continuously every single month.

SENSIBILITY: If you can be honest with yourself after researching and considering all the above, doesn't it make sense to keep your patients' information safe from the cloud. Your patients' trust is at stake as well as your practice.

Regardless of your choice to do business with us, we sincerely hope the best for your practice and especially for your patients. For an entertaining, worst-case scenario thriller, please read my latest novel, "Malignant Behavior", now available at amazon.com.

Regards,

Max Shylahr
www.shylahr.com