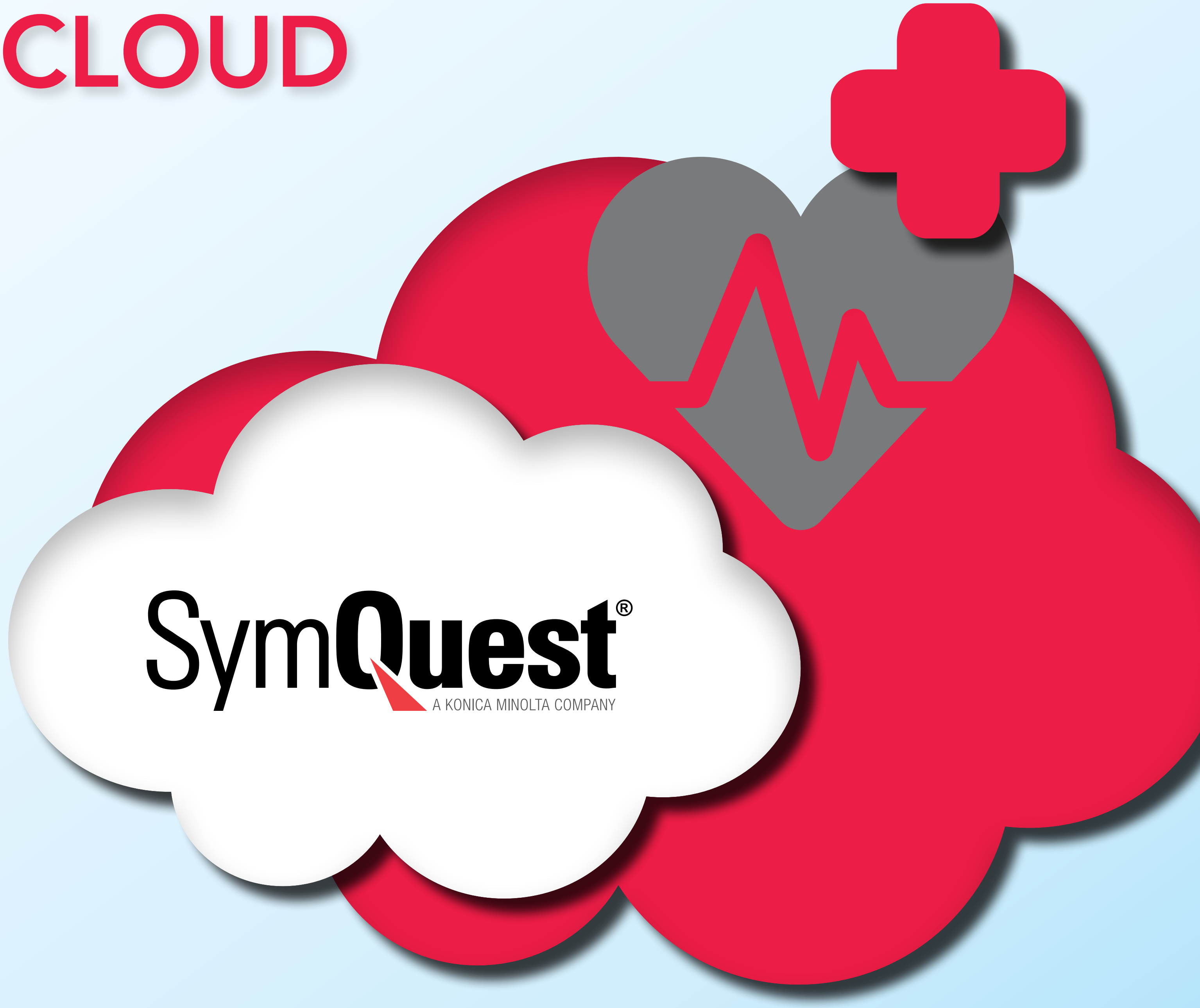
TIP SHEET:
5 REASONS TO MOVE YOUR MEDICAL PRACTICE TO THE CLOUD



Welcome to the wild frontier of healthcare *Information Technology (IT)*. Medical practices across the U.S. are moving their Electronic Patient Health Information (ePHI) to hosted cloud network environments at a rapid pace, but is it safe? Where is ePHI going? What is the big deal with the cloud, and why should practices even consider using a hosted cloud network infrastructure?

In this tip sheet we will outline five reasons to move your network to the cloud and give your physicians and staff more time to do what they do best, focus on patients.

1. SECURITY

The #1 reason to start evaluating your network infrastructure is security. That's why we've put security as our first reason for moving your medical practice to the cloud. If you take a quick inventory of your IT infrastructure does it appear secure? Do you have physical security measures in place to protect your servers from outside intruders? Do your physicians use secure methods to access your network? These are just a few of the many questions you should be evaluating as part of your network security protocols.

By moving your network to the cloud you essentially remove accessibility to your physical servers. Additionally, if you select the right managed services provider (MSP) you can monitor every aspect of your network. Moving to the cloud offers the follow security benefits:

Incident Response: 24/7 IT support keeps the administrative traffic through your office flowing smoothly. By using a cloud provider with afterhours support you have someone to rely on to make your network accessible prior to the start of your business day. If your in-house IT manager is on vacation – who do you call in an emergency? Incident response is also vital in the event of an outside breach, malware attack, or system error.

Social Engineering: breaches go beyond a sneaky virus you picked up on your favorite social media site. Criminals out to steal ePHI can pray on networks that are stored in a physical environment by using *social engineering*. Some social engineers pose as helpful employees for Internet Service Providers (ISPs) to gain access to your server room, or simply walk into your restricted office space while your staff is occupied elsewhere. Social engineers may also target patient data versus network infrastructure. By using the cloud you can digitize your patient information and protect your office from simple social engineering schemes.

Data Protection: speaking of patient information – where do you keep it? Storing your patient data in physical files is the least secure and most cumbersome method of managing such a secure type of information. A good MSP will help you follow the *Technical Safeguards* outlined in HIPAA's Security Rule for ePHI. These safeguards include controlling network access to authorized personnel, auditing the activity and access to systems storing ePHI, outlining measures to prevent altering or destroying ePHI, and rules regarding the access of ePHI while it's transmitted over electronic health networks or within Electronic Medical Record (EMR) systems.

System Updates and Patching: most MSPs are in tune to what's happening in today's technology landscape. When a widespread vulnerability occurs, the MSP typically deploys system updates and patches to keep your network secure. If you're using in-house IT there may be a delay in learning vital IT news that relates to your business. Being backed by a team of engineers increases the response to vulnerability ten-fold, and leaves the worry to the MSP to get the system updates and application patches in place.

2. DISASTER RECOVERY

If your servers are not protected in a locked environment they're vulnerable. Furthermore, even if your servers are behind a locked area, you could still be vulnerable to social engineering. The best place to put your servers is in the cloud. Yes, the cloud still has a physical environment – but it's a physical space you're not liable for. Most MSPs store your network in secure, unpublished, off-site locations.

Another consideration for choosing the cloud is redundancy. If you select the right MSP you can be sure that your data is backed up in two locations. The very best MSPs follow a 3-2-1 principal. *Three* copies of your data, stored in *two* locations, with *one* location off-site from your office. The very best MSPs will back up their cloud data in redundant data centers meaning that if one of their data centers suffers a catastrophic event your data is safe in another location.

The second area of disaster recovery to be concerned with is downtime. You don't have downtime in your medical practice so ensuring your EMR records and network are accessible is imperative. Your business should outline a reasonable Recovery Point Objective (RPO) and Recovery Time Objective (RTO). Your RPO is the time which your MSP is allotted to get your network up and running.

Quality MSPs have RPOs of 2-4hrs which is far better than the typical RPO of 12-24 hours that occurs with in-house IT staff. And it could be worse; if you have to hire an outside network engineer to assess a problem you're looking at a recovery time that could reach 24 – 48 hours. When you establish your RTO you can determine how long your system can be inoperable before you encounter a financial loss to your business. Putting your network in the cloud could help you avoid the RPO and RTO mess all together.

3. ACCESSIBILITY

Let's be honest, work doesn't end when you leave your office. Your physicians and administrative staff often work after hours, or remotely, to keep your business running smoothly. By putting your network in the cloud you can add additional options for accessing your files and applications remotely.

Using the cloud also enables your practice to take advantage of popular computer software used by the business and medical community. Applications can be deployed across all of your PCs and your system administrator or MSP can also determine which PCs need attention.

Accessibility should never be limited to physical access to the workstation or server. Remote access reduces the costly overhead dollars of having someone deploy updates or programs onsite, and streamlines the way your office makes progress in IT.

4. COMPLIANCE

You took an oath to protect your patients. HIPAA compliance is one way to protect your patient's information. The purpose of HIPAA is to protect PHI. Protecting PHI is possible in a hosted cloud network environment. How can you be sure that your MSP understands HIPAA? It's simple, just ask. There is a privacy and security framework that has been outlined by the U.S. Department of Health and Human Services. This framework can be used as a guide to understand your relationship with your MSP, or Business Associate.

Here are a few compliance related questions to ask your MSP:

- Are you aware of the HIPAA guidelines surrounding Electronic Patient Health Information (ePHI)?
- Do you train your employees to protect PHI and ePHI?
- Do you have policies and procedures in place to protect ePHI in your organization?
- Do you have tools that enable email encryption for my business?

- Where will my practice's data/ePHI be stored? How will it be protected?
- Will my practice's data be recoverable in the event of a disaster?

In addition to responsibly answering the questions above, your MSP should be willing to enter into a Business Associate Agreement (BAA). The BAA should hold the Business Associate liable for any breach of PHI that occurred as a result of a vulnerability created by the MSP. It is also recommended that the MSP have a sizeable policy protecting against errors and omissions.

5. SCALEABILITY

The final reason to move your business to the cloud is scalability. Your practice is growing. More patients through your door equates to more ePHI rolling into your system. As you expand your business you're going to need systems and infrastructure that can handle growth. Keeping your network in a physical location is only scalable if you have room for more servers, more filing cabinets, and more employees.

Imagine you've run a spectacular marketing campaign for your practice. The phone is ringing and new patients have been added for consultations. The following month is booked and you're ready to expand, however, your network isn't. Your drives are full and you need to add 12 new patients to your system. When you partner with a good MSP you can scale your network with one phone call. Now you're ready to build your practice and worry about the physical needs of your office while your network runs smoothly, and efficiently.

Scalability is also important for adding additional staff to your practice. If you're ready to take on new employees you need to add PCs and access to your applications and systems. This is very time consuming if you're using in-house IT, but simple if scheduled with your MSP. Your MSP can deploy the software needs to multiple PCs, and have your businesses IT needs ready for each new hire from day one.

SUMMARY

Your network is the key to running a streamlined medical practice. Relying on one person, or one department, may be a gamble in today's healthcare economy. You need to know your practice is backed by professionals who are experienced and available – 24 hours a day, seven days a week, and 365 days a year. A reliable MSP can lift your IT burden and give your medical practice the cloud coverage it deserves. Finally, if you have questions just **give us a call**. We are here to help.