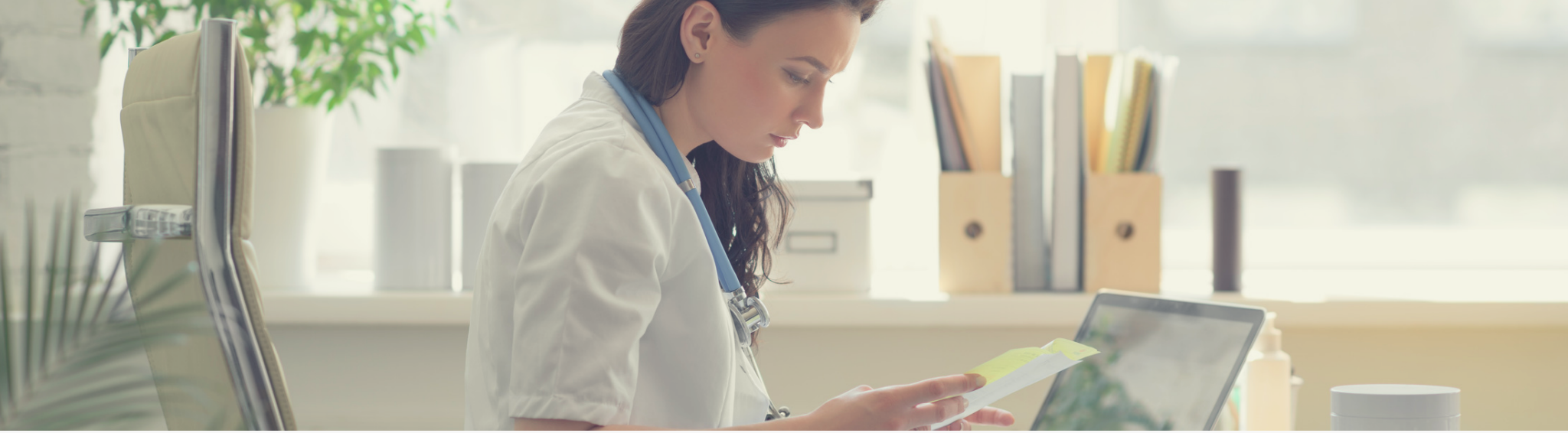
6 HIPAA-COMPLIANT MYTHS REVEALED

qliqSOFT

What will you discover?



TAKING A CLOSER LOOK: EXPOSING MYTHS AND SHARING INFORMATION

Misinformation about secure texting is rampant in healthcare. This grip of bad facts keeps organizations from embracing modern communication practices. With fears over personal health information (PHI) breaches or misunderstanding the very definitions and applicability of HIPAA, it's time to clear the air.

To ensure you have the right information, QliqSOFT is sharing some common myths about HIPAA-compliant messaging. It's time to break down the barriers associated with healthcare communication. These obstacles are keeping you tied to pagers, faxing, and other antiquated tools. With a fresh look at how to remain HIPAA-compliant using a secure texting app, you'll learn that these myths shouldn't be distracting you from progress.

KEEP READING TO LEARN THE TRUTH ABOUT THESE SIX MYTHS

1. Think HIPAA laws don't apply to you because you don't bill Medicare, only use paper, or any other factor? There isn't an opt out when it comes to HIPAA compliance.

2. Convinced text messaging is never HIPAA-compliant? Not so. Smartphones have the ability to be compliant with a secure texting app.

3. All cloud storage providers are HIPAA compliant and will pass an audit. Unfortunately, that's not always the case. Learn what you need to know about your secure messaging supplier.

4. Physicians, nurses, and clinicians are always prohibited from using a personal device while on the job. With the right technology and secure platform, they absolutely can.

5. Security and privacy of your PHI are the same thing. Sorry, they aren't. Data can be secure but not private.

6. There is no such thing a HIPAA-compliant camera for smartphones. Actually, with the right technology, providers can use their smartphones for pictures.

HIPAA DOESN'T APPLY TO YOU

Sorry, but there's no opt out of HIPAA. It applies to any healthcare provider that transmits, stores, or handles PHI. It's not exclusive to digital information, it applies to printed as well. Some organizations have believed, erroneously, that HIPAA didn't apply to them for some reason, thinking there must be exceptions.

Whether because they were small practices or managed only private pay patients, these organizations thought they had no obligations to follow the law. It's also important to note that it isn't just your system that must be HIPAA-compliant. All your third party business partners do as well. Other entities may use PHI for billing or in various situations, storing and transferring data. You are accountable to how you handle data and how your vendors do.

Bottom line, you and any entities you share information with must have the policies in place to remain compliant with HIPAA. With best practices and providers that are focused on keeping you compliant, it's much easier to do.

TEXT MESSAGING IS NEVER HIPAA-COMPLIANT

First, to clear up any uncertainty, standard SMS text messaging and secure texting are two different things. With this clear delineation, secure texting on an application, which meets necessary requirements and standards, passes HIPAA compliance. There are several factors to determine if the exchange of information adheres to the regulations. The messaging app must be separate from a user's phone. This means that messages and images are never stored on the personal device. It remains on the application behind your firewall.

Be aware that not all organizations interpret HIPAA compliance in the same way. What makes an application more secure is when it "passes through" your provider's cloud. Cloud pass-through technology is fairly new and far superior to other options. Be sure you know what entity has ownership of the data. Don't assume you do because that might not be true.

With the right app, smartphones become a great tool for communication and collaboration. This can improve patient care and reduce a lot of the time lag that results from paging or other inefficient mediums.

YOUR SECURE TEXTING PROVIDER IS ALWAYS HIPAA-COMPLIANT AND READY TO PASS AN AUDIT

It would be great if every healthcare IT provider was vigilant about compliance. While many organizations certainly meet the criteria, it doesn't mean they aren't vulnerable. If they are, you are, too. The risk of exposure occurs when PHI from your organization lives on the provider's servers. Then you don't have control of how secure that data is, which is another reason to consider cloud pass-through architecture.

To ensure you pick the right partner, ask questions about how they transfer and/or store data. Be comfortable with the answers you receive before making a choice. If the provider is serious about compliance and security, the company will follow the framework of the National Institute of Standards and Technology (NIST) in addition to compliance with all of HIPAA's requirements. Your provider should have no concern signing a Business Associate Agreement (BAA), giving your more confidence in their security and compliance efforts.

QUESTIONS TO ASK YOU SECURE TEXTING PROVIDER

1. Do they ever store PHI in the cloud?
2. Will they sign a BAA?
3. Is private and public key encryption available?
4. Can they integrate with your electronic medical record (EMR)?
5. Can images be shared securely on the app?
6. Can you use the app with patients?
7. Does it work for iOS and Android?
8. Is a desktop app available?

PHYSICIANS, NURSES, AND CLINICIANS CAN NEVER USE A PERSONAL DEVICE WHILE ON THE JOB

There are a lot of caveats to what kind of technology you can use in healthcare. Smartphones are an integral part of most any workplace or workflow. In the corporate world, workers can text or instant message someone a few feet away if needed. Hospitals and healthcare settings are in fact a workplace. Peers need to be able to communicate. Thus, healthcare professionals deserve this same convenience.

The data shows that both physicians and nurses are using their personal devices while on the job. A survey found that 80% of physicians use smartphones at work while 67% of hospitals responded that nurses use personal devices to communicate and support workflow. That doesn't mean they should be using them, as different rules govern what personal devices a healthcare worker can use.

THE SHIFT TO BYOD

When smartphones first entered the market, the technology was new and not everyone had them so BYOD (bring your own devices) wasn't even a consideration. Now, they are the most used device in the world. With most all healthcare professionals owning a smartphone, BYOD has become more common. The improvement in technology and security has led to a much wider adoption of the practice. It doesn't mean clinicians should be texting each other from their SMS app. In BYOD facilities, using a personal smartphone isn't simply about using your standard text messaging app. Communications must be on a secure app. That app should have true end-to-end security, including:

- 2048 bits RSA, AES 256 encryption
- Individual public/private keys
- Remote wipe, lockout

An app such as this is much more secure than a legacy client/server system, simply because no PHI is stored or decrypted on the app's server. These sophisticated apps can be downloaded in minutes, keeping care teams connected and reachable. There are still risks associated with BYOD—all of which require careful consideration.

SECURITY AND PRIVACY OF YOUR PHI ARE THE SAME

In the world of HIPAA, security and privacy are two different parts of the puzzle. Data is secure when best practices have been applied to protect against breaches and hacks. This means vendors should have a robust system that meets HIPAA guidelines. While data may be secure, it's not inherently private. HIPAA does regulate privacy associated with PHI as well, requiring a permissible use. This may be related to operations, like quality assessments or development of protocols, or to aid in the treatment of patients.

Within the healthcare ecosystem, PHI is transferred and used in numerous networks. That's a quandary of the modern healthcare system. You are one peice of the larger ecosystem. It only takes one weak link to expose PHI. While most organizations are fearful of a security breach, a privacy breach is just as bad and as costly.

HIPAA-COMPLIANT SMARTPHONE CAMERAS DON'T EXIST

Photos are often a great asset in helping treat patients. From dermatology to wound care to surgery, photos are taken every day in healthcare. Some professionals may have never even heard the term HIPAA-compliant camera, much less, considered that their smartphone could be one.

How can you use your phone as a HIPAA camera? Start with a secure texting app that allows for this functionality. This means the images are never stored on the device or backed up a personal cloud. You'll be able to take images and upload them to an electronic medical record (EMR) in seconds. In some cases, you might want to send them to another clinician for advice. This is possible, too, as long as they have the same secure messaging app.

MYTHS REVEALED: IT'S TIME TO TRY HIPAA-COMPLIANT SECURE TEXTING

Now that we've debunked these six myths, it's time to enable better technology in your organization. If you currently have a BYOD policy or are considering one, then you need a secure texting app in place. Otherwise, you run the risk of noncompliance. No matter what way you communicate internally or externally around PHI, compliance never changes. Take the worry out of how staff are communicating by adopting a platform that keeps you HIPAA-compliant and offers better ways to collaborate and ease the bottlenecks in workflows. One app could revolutionize the way in which your organization communicates. Get started now.

ABOUT QLIQSOFT

Communicate better with HIPAA-compliant tools from QliqSOFT. Increase accuracy, reduce wait times, and improve patient care and satisfaction—all on one platform. Our secure texting platform system is like no other healthcare communication solution because we never store PHI, reducing the risk of human error data breaches. Explore how we can transform your organization today.

QLIQSOFT.COM

(866) 295-0451