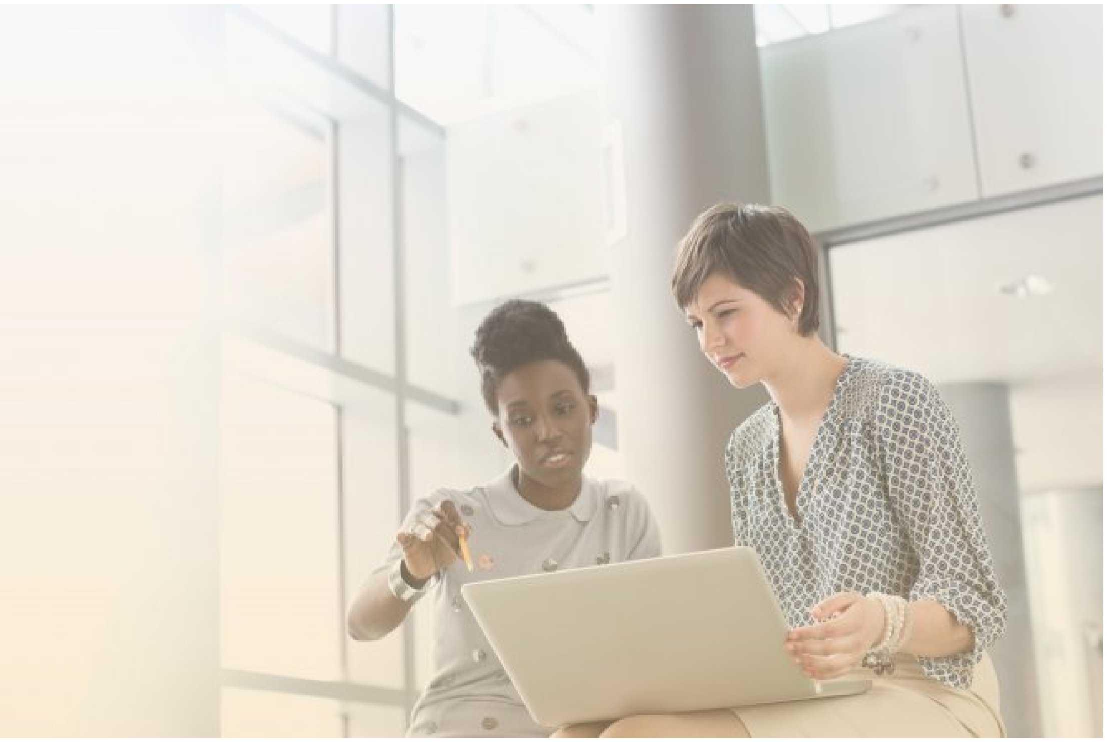
Vonage Business

Balancing HIPAA Cloud Compliance: Why It's Worth It

By JOE HEWITSON - Contributor

Health Insurance Portability and Accountability Act (HIPAA) cloud compliance can be a challenge at times. Until recently, enterprises subject to HIPAA regulations have struggled with the thought of releasing sensitive data into a cloud environment. From access control to encryption, compliance needs have caused IT professionals to keep a watchful eye on cloud services. Recent progress, however, has made the cloud a hospitable home for companies, industries, and certain types of data subject to various regulations.



HIPAA cloud compliance may sound odd, but it's worth putting regulated data in the cloud.

If you've ever had concerns about transitioning business processes and systems to the cloud while remaining in compliance with regulations such as HIPAA, you've undoubtedly come across a few questions of your own. Here are a few helpful tips to get your data safely into the cloud:

HIPAA Cloud Compliance

So, why is it worth putting regulated data in the cloud? The reasons include cost, flexibility, and efficiency — and access to the data anytime, anywhere. When a HIPAA-covered entity puts data in the cloud, you're able to focus your limited resources on strategic initiatives.

Furthermore, organizations that find themselves hesitating when considering a cloud migration often worry about compliance and security. They should, as data protection shouldn't be taken lightly in today's digital world. Covered entities are usually worried about the following:

- Encryption of stored data and data in transit
- Control over low-level read/write access to data
- Comprehensive governance of physical security and monitoring
- Durability and availability of data
- Latency of data access
- Integration of data with existing business cloud services

Fortunately, cloud vendors must meet all of the above concerns in order to be HIPAA-compliant. Simply put, there's no reason why you can't maintain the same level of data security in the cloud as you do in a private environment. Better yet, you'll have access to a whole suite of features only the cloud can offer. In the case of phone systems, that includes CRM integration, seamless experience from desktop to mobile, and built-in video, voice, and web collaboration features.

The bottom line is that cloud benefits are numerous and well-documented. Compliance concerns, on the other hand, are often more stigmas than impregnable barriers. Just as cloud services take the burden of IT management off your shoulders, they can also share the work of compliance and regulation.

Regulated Data

Regulated data in the cloud is certainly a worthwhile endeavor, but it's not without a few challenges. Questions inevitably arise. For example, is a Business Associate Agreement (BAA) really necessary?

The answer is yes — at least in most circumstances. In fact, you probably need a BAA before you even move your data. While some may consider cloud service providers to be data conduits, they're still considered business associates by HIPAA in most circumstances.

As such, you'll need to get the cloud service provider to sign off on a BAA before any data touches their servers. Failure to do so could find you in violation of HIPAA. And yes, you still need the BAA even if data is always encrypted, whether your cloud service provider holds a decryption key or not. Be sure to read your BAA carefully to ensure that it accurately reflects the desired level of security and/or compliance. For more information, see the Department of Health & Human Services' "Guidance on HIPAA and Cloud Computing."

What About Using Data on the Go?

HIPAA outlines some compliant use cases that may surprise you. Do you want to leverage your data on a mobile device? That's fine by HIPAA guidelines, provided you follow the privacy and security guidelines laid out by HealthIT.gov. Coupled with cloud services, making use of electronic protected health information (ePHI) and other regulated data for business processes on the go makes a whole lot of sense and highlights the benefits of managing protected data in a cloud setting.

Speaking of data on the go, you may have a handful of reasons to make use of data service across the pond, and that's fine by HIPAA — with some caveats. As mentioned above, you must enter into a BAA with the overseas (HIPAA-compliant) service provider. There are also additional data security concerns for countries that meet specific criteria, as outlined by HIPAA.

Using cloud-based content delivery networks to push data overseas for low-latency applications is a growing use case for many organizations — and one that HIPAA-compliant cloud providers can tackle with ease.

All cloud providers are not the same. Before entrusting them with your sensitive data, do your homework and understand the level at which they can support HIPAA compliance. Many cloud providers only deliver HIPAA-compliant infrastructure-as-a-service (IaaS) platforms, misleading customers into believing they have full HIPAA compliance when signing up.

Ultimately, the cloud has been innovating data-driven business processes for some time. The only thing holding some organizations back is government compliance and regulation concerns. While this can be a delicate balancing act at times, remember that it's one worth undertaking and probably not as difficult as you think. Just as cloud services take the burden of IT management off your shoulders, they can also share the work of compliance and regulation.

Finally, before undertaking a cloud-based solution, be sure to consult your legal advisers to understand the HIPAA requirements applicable to your business, potential liabilities, and what you should be requiring of your cloud providers.

Contact Vonage Business to learn more about how cloud-based communications can help your company.