The HIPAA Dilemma: Hosting a Digital Health App

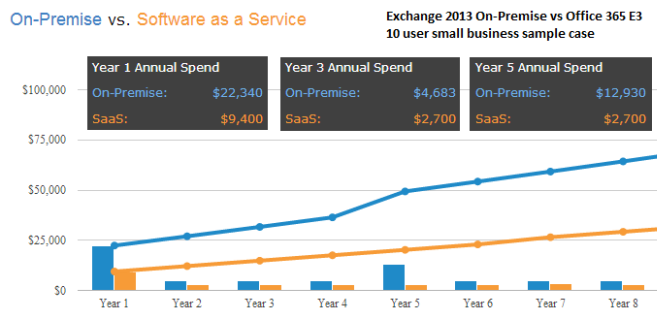
Picture yourself as a digital health startup founder. You are super excited to build something not just revolutionary, but something that will actually impact patients and potentially save lives. It’s a truly awesome and empowering feeling! As you flesh out your product and market fit, you find that you have something that is actually worth building, so you start developing an app. The good times are rolling, but then the hospital you’re hoping to work with asks if your app is HIPAA compliant. Oh. Crap…

Digital Health organizations operate at the critical junction of technology and healthcare.  When incorporating protected health information (PHI) into their offerings and technology, there is often an urgent need to achieve compliance in an efficient and cost-effective manner.  In addition to the added compliance burden, these organizations also face pressures that plague all young companies: too much to accomplish in too little time with too few resources.

One strategy that is almost universally adopted among young companies is public cloud infrastructure. By leveraging the power and flexibility of cloud Infrastructure as a Service (IaaS), organizations can forego capital expenditures without sacrificing scalability when they need it. This flexibility is essential for digital health companies who need to rapidly scale their applications at launch and prepare for rapid customer adoption. If we ignore the compliance concerns for the moment, cloud IaaS is a no-brainer for these organizations.

On Premise vs. Infrastructure as a Service (IaaS)

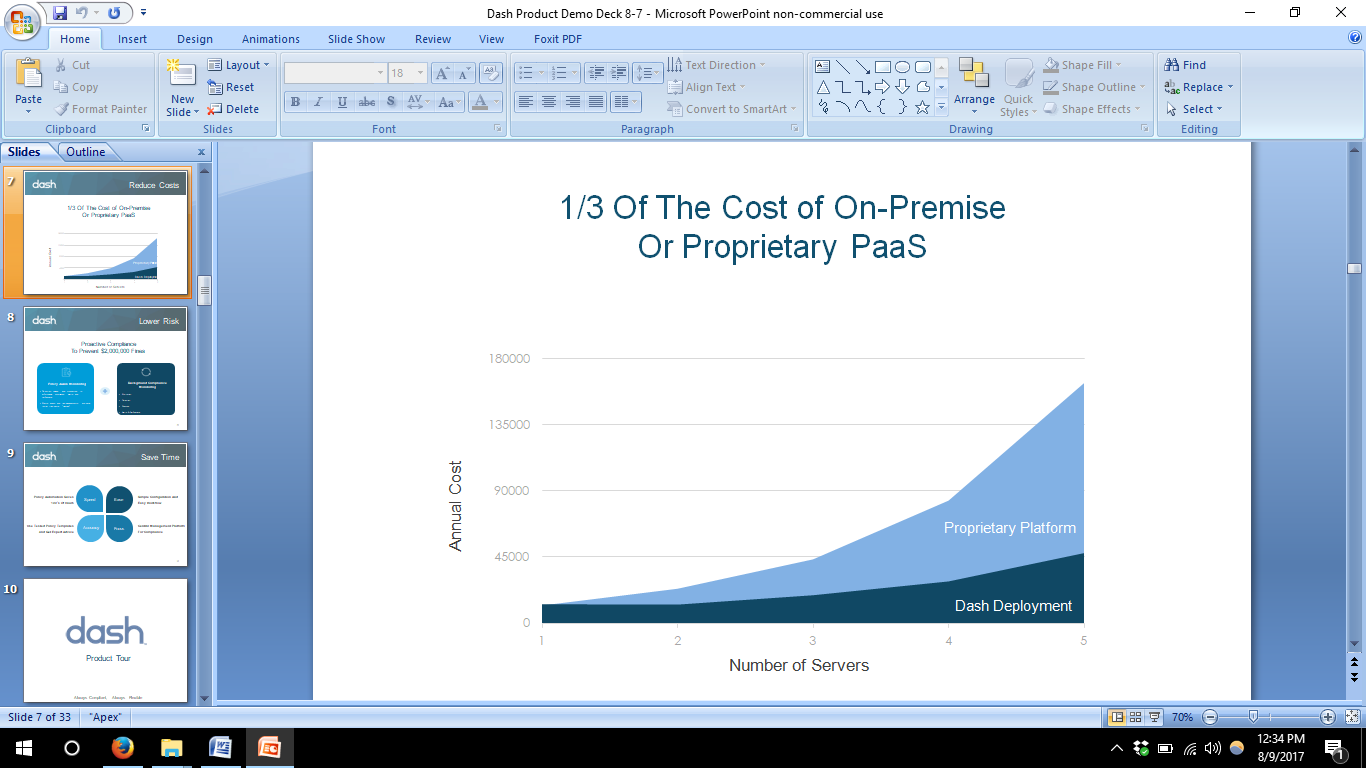
Yearly Costs and Running Total



If we accept that startups and young companies entering the healthcare space are ideal cloud embracers and adopters, we must now turn our attention to the compliance concerns. HIPAA compliance in any network architecture requires both a technical and administrative resource investment. Organizations that are entering the HIPAA space must take care to build both their organization and technology stack in a compliant manner that does not hamstring their future growth potential.

One option in the marketplace today are proprietary HIPAA compliant Platform as a Service (PaaS) offerings. These offerings include a simple monthly pricing plan which scales on demand. Offerings also typically include assistance with the compliance process as well as support, monitoring, and service. There may also be less of a time and resource investment upfront to achieving compliance on these platforms as they are built to simplify that process.

Unfortunately, by absorbing much of the technical responsibility when it comes to compliance, these platforms do not scale in a cost efficient manner. In the example below, consider a small yet growing health startup. Over the course of 5 years they will increase their infrastructure from 1-5 servers. Two actual infrastructure cost models are considered: a HIPAA compliant PaaS, and self directed IaaS with Dash Compliance Automation Suite.



While the results are striking, the PaaS company is somewhat justified in their surplus pricing because they are likely delivering some real time-saving and simplification value. Because HIPAA regulations require constant monitoring and vigilance, it can be tempting to go for the quick “easy compliance” solution that the proprietary platform offers. Unfortunately, by making that decision, startup leaders are often condemning their company to excessively high infrastructure costs down the road.

Ironically, the very same thought process that would cause a digital health company to choose a cloud option over on-premise might lead them to determine that a proprietary PaaS is also a prudent choice. In the short term, and while the company is small, these solutions are great. Ultimately, vendor lock-in, switching costs and lack of internal compliance culture will likely force the organization to proceed on the PaaS route to very high costs down the line.

Furthermore, PaaS providers restrict the immensely valuable cloud services available to their customers in the name of compliance. Rather than providing each customer with their own account in the cloud, these offerings insert their layer between the infrastructure provider (AWS, Google, Microsoft, etc.) and their customer. Because the customer doesn’t have an AWS account, they cannot leverage any of the hundreds of AWS specific services that Amazon offers directly through their platform. Dash liberates these organizations to own their cloud account while maintaining the security and compliance framework within the cloud.

Dash is a lightweight software that plugs into infrastructure providers like AWS that startups already know and want to use. Organizations can then handle policy and process through Dash’s policy automation module, saving them months of time to market. Once the policies are set, Dash measures the enforcement of compliance and performs constant compliance monitoring against each organizations unique policies and process as well as the HIPAA compliance framework.

In order to both innovate in the short term and scale in the long term, digital health startups and small healthcare organizations need to achieve compliance quickly and reliably without paying the price down the line. Dash allows digital health to thrive both now and in the future, paving the way to long term success.

To learn more about how Dash alleviates the compliance burden in the public cloud, contact us for a demo today: