TechRepublic

CLOUD

Key to HIPAA compliance is understanding your data center and cloud risks

Hosting protected healthcare data in the cloud, says Connectria's David Pollard, means you have to find a solid partner and know your on-premise and cloud risks.

By Brian Taylor June 29, 2015, 3:21 PM PST // BrianB2BCopy

Image: iStock

Regarding HIPAA compliance, understanding "risks in your own data center," said David Pollard of Connectria Hosting, "is key to understanding your risks in the cloud." Pollard, Regional Director at Connectria, says that he still encounters executives who believe that hiring a "HIPAA cloud provider somehow mitigates their own needs for compliance." HIPAA is the Federal Health Insurance Portability and Accountability Act of 1996.

Healthcare organizations to need dig deep into their cloud service agreements and also perform a HIPAA assessment to know "where your vulnerabilities lie, allowing you to find a provider that will help you cover your gaps," explained Pollard. Nor can HIPAA cloud providers in the current threat environment say they "have a HIPAA Compliant solution and only provide the minimum infrastructure."

Founded in 1998, and located in St. Louis, Mo., Connectria provides cloud computing and managed hosting solutions. In April 2015, the company launched a HIPAA compliant solution for Amazon Web Services (AWS).

In this Q&A with TechRepublic, Pollard also discussed how the cloud will enhance HIPAA compliance, how AWS users need a partner to manage healthcare workloads, and his firm's track record in providing compliance services.

TechRepublic: What are the risks and pitfalls for healthcare organizations in moving to the cloud? What practical steps can they take?

Connectria's David Pollard
Image: Connectria Hosting

David Pollard: We still receive the occasional call from a C-level executive that thinks that engaging a HIPAA service provider to manage their PHI (Protected Health Information) workloads will essentially offload their liabilities. There are still people out there that believe that a HIPAA cloud provider somehow mitigates their own needs for compliance. Understanding your own risks in your own data center is key to understanding your risks in the cloud.

The BAA (HIPAA business associate agreement) outlines the roles and responsibilities of each member of the partnership. Know how the BAA is written before you sign up for the services. It is also a good idea to perform a HIPAA assessment prior to engaging a provider. This will tell you where your vulnerabilities lie, allowing you to find a provider that will help you cover your gaps.

TechRepublic: What are the main security trends in managed cloud hosting over the next few years?

David Pollard: Customers are becoming more aware of their own threat profiles. More and more customers are hearing about breaches and the impact on businesses from both a financial and image level. They are also evaluating cloud providers at a deeper level to understand where the provider leaves off. As a provider, you can no longer say you have a HIPAA compliant solution and only provide the minimum infrastructure.

TechRepublic: How prepared, in your view, is the healthcare sector for handling the HIPAA compliance and cybersecurity risks of cloud deployments?

David Pollard: If you attend any function related to healthcare and IT, you will see that the common themes are functionality and security. The difficult task is weighing the access to patient records with the need to secure it. What use is an electronic health record if the providers cannot access that record in an emergency? This is something that is continuing to evolve, and there will be stumbling blocks along the way.

TechRepublic: I'll ask you to make some predictions. How will cloud computing affect and disrupt the practice and regulation of HIPAA compliance?

David Pollard: That is difficult to say. I don't think that the adoption of cloud computing will disrupt the practice and regulation, but more likely enhance it. There are some brilliant minds out there in the world and if you look at the Amazon Marketplace, you can buy some very cool products right off the shelf. Encryption products, anonymizers and de-identifiers, security appliances, and more. These readily available tools make the day to day securing of PHI data easier to buy and more simple to implement.

TechRepublic: Since Connectria launched its AWS HIPAA solution this past April, what kind of traction are you seeing in the marketplace?

David Pollard: Frankly, it is our fastest growing segment. AWS has some incredible tools, but there is a lot of work involved to make that HIPAA Compliant. Customers really need a partner that understands HIPAA and how to secure data. At the end of the day, hosting in AWS is no different from hosting in any data center, colo, managed or your own. You just need a partner that can guide you through the steps required to secure it at the highest levels. Having nearly 10 years of HIPAA hosting experience has allowed us to provide a comprehensive solution that is unmatched in the market. As AWS and technology in general evolves, so will our solutions. This is what we have done in our own data centers for 17 years.

TechRepublic: Additionally, what have you learned from speaking with customers and prospects about HIPAA and the cloud since April?

David Pollard: There is a lot of cloudiness out there. Pardon the pun, but the idea that "It's the Cloud...it just works" is still very much the norm. Not until we engage a customer on a call or through their completion of our pre-sales questionnaire do many people realize that High-Availability in multiple AWS Availability Zones requires the purchase of those resources. People think their data is replicated and a hot standby is sitting out there somewhere waiting for them to push the easy button. Again, these things take smart people and a solid plan to implement them successfully.

TechRepublic: What would your quick elevator presentation about the HIPAA solution to an exec at a prospective client focus on?

David Pollard: That is a good question... one I think we are constantly perfecting. The short summary is that this is, at the end of the day, someone's entire life of data in their possession. Many of the companies in the business of securing PHI weren't in business 5 years ago. We have built our solutions on nearly two decades of supporting some of the largest and most heavily regulated environments in the world. It is the core of what we do, and we have done it well for nearly 20 years.

TechRepublic: What are the main benefits of Connectria's AWS HIPAA solution to hosting customers?

David Pollard: The main value we bring is again in our history. You may have seen our "No Jerks Allowed" philosophy prominently displayed on our site. That is a real thing. When our owner started the company his first rule of business was "No Jerks Allowed." This is one of 14 of our Guiding Principles, but the one that resonates most with our customers because they can pick up a phone and call our people 24/7/365.

So many companies in the business of "Securing PHI" are all about the API. They put their API on your AWS instances and it runs, ever vigilant until something doesn't go well. Then what? Does the API call you? Does it look into your logs and use its years of SysAdmin experience to properly diagnose and correct the problem? We have built our solution based on smart people managing and monitoring in a true Enterprise Class environment.

Note: TechRepublic and ZDNet are CBS Interactive properties.

About Brian Taylor

Brian Taylor is a contributing writer for TechRepublic. He covers the tech trends, solutions, risks, and research that IT leaders need to know about, from startups to the enterprise. Technology is creating a new world, and he loves to report on it.