Cloud & Managed Server Hosting for Healthcare Professionals

ATLANTIC.NET

Secure Cloud Services
Managed & Compliant Infrastructure

888.618.DATA
sales@atlantic.net
www.atlantic.net

Table of Contents

Important Healthcare Standards

Three critical standards or forms of compliance of concern to healthcare companies are HIPAA (Health Insurance Portability and Accountability Act), HITECH (Health Information Technology for Economic and Clinical Health Act) and SSAE 18 (Statements on Standards for Attestation Engagements No. 18), the update of SSAE 16.

Beyond finding hosting that is compliant with those standards, you also have to figure out the extent to which you want to include cloud in your architecture. How can you become compliant, and how should you approach decisions on cloud and server management?

HIPAA, HITECH, and SSAE 18: Integrated Objectives

HIPAA's Title II, with its Security and Privacy Rules, is of special concern related to data systems and the safeguarding of sensitive patient data – called electronic protected health information (ePHI). The parameters of the Security Rule are particularly important – establishing reasonable measures to keep information from being compromised, through implementation of administrative (think training), technical (think encryption), and physical safeguards (think physical access control, biometrics authentication, and 24/7 staff monitoring). HITECH was focused more on increasing adoption of technology; however, there are important aspects of it related to compliance of your infrastructure – particularly its introduction of the Breach Notification Rule[1] (as additionally indicated within the HIPAA Omnibus Final Rule). Finally, SSAE 18 is a set of guidelines developed by the American Institute of Certified Public Accountants (AICPA) – a standard that may seem extraneous to healthcare law but that is a reliable way to gauge security protocols more strictly (in some ways) than is required by HIPAA, since it was developed to generally control service provision.

When you work with a provider any type of hosting – managed or unmanaged, cloud or dedicated – it's important to make sure that they meet all these various compliance standards. You must ensure

that you are protecting your patient information within a next-generation data center; that is still true following the above-mentioned Final Rule, which also assigned compliance responsibility to hosting services and other business associates.

These forms of compliance tell you that the web host adheres to industry best practices that are particularly critical for the healthcare field – an operation that leverages a standard contingency plan, data backup plan, disaster recovery plan, emergency mode operation plan, systemic testing procedures, and ongoing data criticality assessment. SSAE 18 compliance lets you know that security is a priority for the host above and beyond the stipulations of HIPAA, helping you exceed rather than simply "meet" the law. It generally serves as a redundancy both as a separate audit and separate set of parameters.

Hallmarks of Compliant Healthcare hosting

First, it should of course have the infrastructural design and technologies in place that are understood within the industry to properly protect data when it is stored or in transit. Those elements include a fully managed firewall, encrypted VPN, encrypted backup, a log management system, and an anti-malware system. (While HIPAA guidelines do not list specific technologies as required, they make it clear that reasonable steps should be taken for protection – and those aforementioned tools would be considered reasonable steps.)

Beyond those "things," you also need to think about a couple other major factors: the people (training of the hosting company's staff) and the space (think cooling and power). To focus specifically on that second element, a next-generation data center will deliver both of these elements efficiently and seamlessly so that you do not experience a failure. The facility will also dynamically allocate resources – which offers additional benefits when those resources are leveraged within the coolest parts of the data center.

Next-generation data centers, i.e. ones

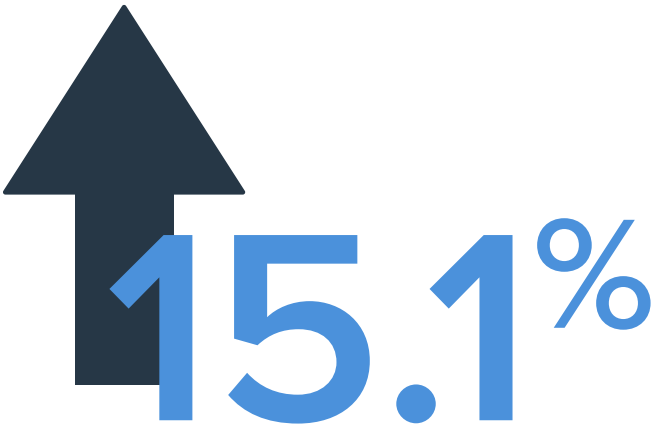
that are prepared to meet the current and ongoing needs of healthcare firms and other highly regulated industries, position themselves more aggressively toward security – making it (as Sean Ellis would say) the "true north" of the organization. It is important to keep in mind the way in which these providers are necessarily putting themselves at risk in order to work with healthcare firms, so a company positioning itself in terms of this expertise must have confidence that it is compliant – for its own sake, beyond its responsibilities to its clients.

It should be clear that meeting the guidelines of HIPAA must be approached at the higher level of the facility and personnel before you start looking into the details of the system and actions at the software or process level. Again, bear in mind that administrative and physical defenses must be established along with technical ones.

Who is Responsible for HIPAA?

In terms of liability, it helps to think about the individual role that each entity plays. In that sense you and the hosting company, and any of your other service providers that handle ePHI (or PHI), must separately meet the HIPAA rules. You will be effectively protected by performing due diligence; you obviously cannot be expected to have full control over an infrastructure that is externalized. However, compliance is about partnership; you need an agreement – a business associate agreement (BAA), specifically. The BAA protects you and sets clear expectations in terms of what exactly is being provided by the vendor – the data center environment, managed hosting, tech support, etc.

The short answer to this question, then, is "Both you and the host, as outlined in the BAA."



Virtualization security growth forecast[2]

Cloud Computing for Healthcare

Through virtualization, cloud computing allows you to deliver resources to users and tasks that need them as efficiently as possible – and, of course, efficiency and performance are two key secondary concerns to security. Despite the complex and distributed nature of virtualization, cloud is not antithetical to HIPAA, HITECH, or SSAE 18 compliance. Virtualization has introduced new opportunities for building healthcare systems. In fact, today, virtualization is an area of specialty within healthcare IT. As seen with the concern over cloud, virtualization may concern experts related to risk. However, virtualization security is growing rapidly – with Mordor Intelligence[2] forecasting it to expand at a 15.1% compound annual growth rate (CAGR) from 2018 to 2023.

Private, public, and hybrid cloud are the three basic models that are used by organizations and widely available through hosts:

Private Cloud

A cloud hosting solution set up by a host that has expertise in healthcare data systems delivers security while distributing your system across various servers. Because you are using private resources contained within the cloud structure, you can easily maintain your environment and customize as needed, as your situation develops. You can customize configurations however you want. There is no debate over the fact that private cloud (whether internal or external) offers you a higher degree of control. The private cloud allows you to benefit from the structure of cloud – and do something about underutilization of resources that can occur in a dedicated setting. As with public cloud, resources are allocated based on demand within a private cloud. Unlike public cloud, private cloud certainly has a stronger security model than public "out of the box."

Public Cloud

Public cloud is the same basic setup as private cloud, with the exception that the physical servers hosting the virtual machines are not discretely allocated to a single customer. While public cloud is officially approved for compliant healthcare systems (per the HHS Department[3]), storing healthcare via this technology will require additional safeguards simply because you are in a setting used by multiple organizations. However, it is worth noting that cloud security is generally seen as strong by computing experts, with David Linthicum[4] stating, "The public cloud is more secure than your data center." While Linthicum's language was particularly bold, it is aligned with common sentiment that public cloud systems now have a baseline security that is stronger than what many organizations have. Along similar lines, New York Times deputy technology editor Quentin Hardy[5] pointed out the degree of on-staff security expertise at credible cloud providers. The HHS has itself noted specifically that any cloud system can qualify as HIPAA-compliant – public, private, hybrid, or otherwise – with the right BAA and additional safeguards in place.

Hybrid Cloud

Hybrid cloud is an integrated combination of on-premise (colocated), private cloud, and public cloud servers. Hybrid cloud allows greater flexibility by enabling organizations to move resources dependent on their needs, cost requirements, and security concerns.

Cloud is typically appreciated for offering a "sliding scale" of IT resources. You don't have to bring in or retire physical servers. You simply click a button. In other words, just like the servers are virtual, the process of adding new ones is virtual too. A private cloud will not give you access to nearly as many machines as you would get in a public cloud; however, there are substantial multiple redundancies built into a well-designed cloud whether it is private, public, or hybrid. Also with any cloud model, new machines can easily be brought onto your network as your demand expands.

How to Select a Strong Healthcare Host

Due diligence is key to selecting your hosting provider; even though your business associates are held responsible for meeting the law's guidelines, you still have to confirm claims made by the provider to whatever extent you can. Read reviews or get recommendations from your colleagues.

Here are a few questions to ask your potential host:

- How long have you been in operation?
- How long have you been specializing in HIPAA-compliant hosting?
- How much flexibility will I have to change my system?
- What makes up your physical and logical network security?
- Are you HIPAA certified?
- Are you HITECH certified?
- Are you SOC 2 and SOC 3 certified?

The first two questions will give you a sense of expertise. The third question will help determine what ability a provider has to offer custom treatment and whether they are able to adapt any system to meet individual client needs.

As discussed in the prior "hallmarks" section, you can benefit from the space of a host – and not only in terms of power and cooling, but also in terms of physical security. Plus, related to staff expertise, data centers also employ experts on logical network (a virtual network typically with pieces of numerous physical networks and supporting various physical devices) security, so that the portion of the network that is used for your server is safeguarded with especially strong protections (i.e., the extra measures necessary for healthcare compliance).

Data Centers: Economies of Scale

Healthcare used to typically be handled internally – because it took time for HIPAA hosting to develop as data centers have adopted models for delivering the custom systems necessary to address compliance. Now, though, once the issue of security is addressed, a key plus of

third-party data centers is the economies of scale: you can take advantage of the volume (resources, equipment, network traffic, etc.) that exists naturally within a thriving data center.

Certainly you want to conduct a risk assessment when working with any third-party data center or other business associate. When you are thinking of going the on-premises approach, though, you need to ask hard questions too. Those should include:

- How much will training cost?
- How much will it cost to maintain your hardware?
- Do you want to bear the full burden of administrative, technical, and physical safeguards, with no business associate agreement to establish specific responsibilities?
- How much will HIPPA, HITECH, and SOC 2 audits cost in man hours and third-party auditors?
- How many man hours will it take to keep up with firewalling, intrusion prevention, vulnerability scanning, patching, physical security, physical server patching and maintenance, and maintenance contracts?

Data centers operate a vast sea of machines; even if your system is isolated from other users, you still take advantage of the purchasing power, infrastructural ecosystem, and support model offered by the hosting form. From a cost perspective, if you are comfortable with the security precautions, it will make sense to work with a healthcare-compliant host. Keep in mind that third-party hosting is not just about cloud, although that is often at least part of the package.

Launching Your Compliant Healthcare System

Deciding on the system that you need for healthcare hosting can be confusing and complicated. Generally, you will want to incorporate cloud computing since its efficiency is revolutionary to IT budgets (and since everything can be isolated for your sole use within a private cloud, if desired).

When you work with a hosting provider, make sure that it has the track record needed for you so that you are afforded ePHI peace-of-mind. In business for more than two decades (since 1994), Atlantic.Net has increasingly focused on meeting the needs of healthcare – offering expertise in hosting, security, server virtualization, and compliance, all within a carrier-neutrality setting.

Multiple-practice data management is rife with challenges, risks, and potential setbacks. Cloud hosting of a HIPAA system allows your infrastructure to grow with you. It gives you the ideal mix of reliability, flexibility, and cost-effectiveness. Just make sure that your chosen host has the expertise you need to feel confident in their services.

To speak with a sales representative on how Atlantic.Net can provide you with a HIPAA-Compliant Solution, please contact sales@atlantic.net.

References

1 - https://www.hhs.gov/hipaa/for-professionals/breach-notification/laws-regulations/final-rule-update/hitech/index.html

2 - https://www.mordorintelligence.com/industry-reports/virtualization-security-market

3 - https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

4 - https://www.infoworld.com/article/3010006/data-security/sorry-it-the-public-cloud-is-more-secure-than-your-data-center.html

5 - https://www.nytimes.com/2017/01/23/insider/where-does-cloud-storage-really-reside-and-is-it-secure.html