Data Centers and HIPAA Compliance: What You Should Know

2016-03-16 - Tom Collins - Comments (0) - Blog Posts



Are you exposed to the risk of a Health Insurance Portability and Accountability Act (HIPAA) violation? For organizations that manage protected consumer health information, HIPAA violations are very serious and can result in serious consequences. Violations of a single HIPAA provision can include fines of up to $1.5 million, criminal charges, and jail time. Federal law concerning the protection of private health information covers information in all common forms, including paper assets, oral communication, and electronically stored data. For organizations with a high volume of electronic health information, finding a data center, cloud, or colocation vendor that is HIPAA-compliant is crucial to avoiding costly fines and a loss of public image.

Ultimately, the responsibility to protect electronic protected health information (ePHI) includes hiring appropriate vendors. Information technology teams and leadership must ensure their data center and cloud vendors have the right policies and safeguards to comply with regulatory requirements. In the case of Target's recent high-profile data breach, the attack was executed through a vulnerability in the company's HVAC vendor. While the vendor was reportedly at fault, the media and customers held Target responsible.

Screening and managing vendors is a critical part of information security risk mitigation. In this blog post, you'll learn an overview of a HIPAA-compliant data center, how to assess prospective vendors, and common options.

What Is a HIPAA-Compliant Data Center?

In order to store electronic protected health information (ePHI) offsite, a hosting or colocation provider must meet all standards set forth by HIPAA. This is typically verified and measured by independent auditors, who can measure a hosting environment against the HIPAA audit protocol. Data centers must follow all necessary policies and procedures before claiming to offer HIPAA-compliant hosting and colocation solutions.

How to Assess HIPAA-Compliant Data Centers

Prior to hiring a vendor, you should request and review a hosting client's most recent HIPAA report on compliance (HROC), which is the result of a 3rd-party audit on their data center. It is also important to familiarize yourself with The U.S. Dept. of Health and Human Services' official guidelines for ePHI. The entirety of the HIPAA Security Series: Security Standards: Basics of Risk Analysis and Risk Management can be viewed

online.

Vendors should provide a copy of HROC upon request to prospective clients. Per the Cornell Law School analysis of the HIPAA Security Standards, the following aspects are considered crucial to protecting ePHI in a data center environment:

- Assigned Security Responsibility [section 164.308(a)(2)], which designates that one individual employed by a hosting vendor be held responsible for the implementation of appropriate security policies and procedures.
- Workforce Security [section 164.308(a)(3)], which requires data center vendors to ensure that all data center employees and members of the workforce have access to the appropriate level of information.
- Information Access Management [section 164.308(a)(4)], which requires hosting or colocation providers to create appropriate policies and procedures for managing employee access controls.
- Security Awareness and Training [section 164.308(a)(5)], which designates a requirement for robust security best practice awareness and training programs for data center management and all other employees.
- Security Incident Procedures [section 164.308(a)(6)], which outlines the need to document appropriate policies and procedures for protocol if a security breach occurs.
- Contingency Plan [section 164.308(a)(7)], which includes business continuity planning in case of emergency, such as a natural disaster or physical security breaches
- Evaluation [section 164.308(a)(8)], which requires the scheduling and execution of periodic evaluations of both technical and non-technical security measures.
- Business Associate Contracts and Other Arrangements [section 164.308(b)(1)], which include contracts to designate access to business associates.
- Physical safeguards, which include things like keycard security, security footage, and 24/7 staffing.
- Technical safeguards, including a vendor commitment to continually utilizE best practices to protect against technical attacks.

Common Approaches to Utilizing HIPAA Compliant Data Centers

If you are selecting a vendor that is HIPAA compliant, they may offer more than one-size-fits-all hosting options. Your company's internal talent resources, business requirements, and budget can allow you to choose the right option for ePHI storage with the right HIPAA-compliant hosting vendor.

Depending on your businesses needs, you may opt for:

- HIPAA-compliant colocation, in which you own and maintain your own equiment in a compliant environment.
- HIPAA-compliant private clouds, which is fully managed data hosting services by a compliant vendor.

For more information on whether colocation or private cloud is the right option for you, we recommend Colocation vs. Cloud Services: Which Is Best?

Security and Compliance

No business can afford to weather the costly fines, criminal charges, or loss of revenue associated with a HIPAA violation. By hiring a HIPAA-compliant data center or colocation vendor, you can mitigate your risks and place adequate safeguards around electronic protected health information. Information security isn't simple, but it's a critical component for managing risk in the modern world.

To learn more about how to improve your company's information security with HIPAA-compliant colocation or data center services, click here to learn about Atlantech Online's leading options for compliant ePHI hosting.