Why Colocation Is More Secure For Healthcare

Today's healthcare organizations rely on their IT infrastructure to handle patients' electronic records, health monitoring and laboratory systems, and standard business operations. Ensuring that all of these different systems operate efficiently and effectively is one of this sector's most daunting challenges.

At the same time, healthcare organizations have extremely rigorous requirements for security and privacy, as well as always-on availability.

Most notably, HIPAA standards are in place to secure protected health information (PHI) and to protect patient's personally identifiable information (PII). According to Forbes, data breaches in healthcare totaled over 112 Million Records In 2015, and as a result, the Office of Civil Rights has been conducting random HIPAA audits. The top four HIPAA rules that must be met include:

- Ensure the company's employees practice compliance.
- Protect against inappropriate information disclosures.
- Identify likely security threats, and establish protected measures against those threats.
- Ensure that all electronic PHI that is created or stored remain confidential.

HIPPA implementations include requirements such as encryption, strong passwords, multi-authentication systems, and a lapse in a single implementation can compromise an organization's entire security posture.

Owning and operating a secure data center requires advanced security measures that most healthcare organizations' in-house data centers are ill-equipped to provide. In addition, having the personnel, technology and processes in place to maintain a highly-secure environment requires advanced technical capabilities and a substantial financial investment.

As a result, many healthcare organizations have turned to colocation to deploy and manage their IT operations, and meet their stringent security and compliance requirements.

Colocation is inherently more secure, and here is why:

Most colocation providers implement a variety of measures to help guarantee security and compliance within their colocation facility including:

1. Physical Security - If physical security is top-of-mind for your organization, you're not alone. With a growing number of potential threats, both digital and physical, it's no wonder. Your valuable IT assets should be safeguarded against both man-made and natural disasters. Physical security measures should include video surveillance, mantraps and biometric readers.

2. Network Security - The massive increase in malicious network traffic and the proliferation of SPAM have caused many businesses to be concerned about the security of their network. To safeguard your network, your colocation provider should provide IDS/IPS (intrusion detection services / intrusion prevention services) and basic firewall services. Additional optional services may include virtual firewall services, VPN services, content filtering, SPAM filtering, virus filtering, spyware removal, real-time traffic analysis using net flow reporting and real-time bandwidth reporting.

3. Compliance - As if IT departments didn't have enough to worry about these days, they also have to ensure that their organization is in compliance with various industry and federal regulations (PCI, HIPAA) which are designed to keep sensitive customer data safe. Your provider should provide as much assurance to their customers as possible, that their practices and methodologies are compliant with various compliance audit and certification requirements including:

- **Type 2 SSAE 16 (SOC 1)** - Validates that the providers organizational and information technology controls related to the services audited are fairly described, suitably designed and are operating effectively.
- **HIPAA** - Typically focused on the healthcare industry, but necessary for any company storing sensitive protected patient information.
- **PCI** - Compliance with the PCI DSS is required for any organization that stores, processes or transmits payment cardholder data.
- **ISO 27001** - International Organization for Standardization (ISO) is an independent non-government organization and has international acceptance as a standards leader for electrical, electronic and related technologies.

4. Reliability - Uptime in a data center is non-negotiable. 100% uptime SLAs will provide you with the confidence in knowing that your most important resources and information will be available when you need them.

Why Colocate with OneNeck?

Security and compliance are essential. By working with a colocation provider like OneNeck, you can ensure that your healthcare applications and data are protected through additional layers of cybersecurity and physical security measures to help mitigate your risk.

We understand the growing security demands on today's healthcare organizations, and our goal is to ensure our nine US-based data centers have exceptional security, redundant connectivity and climate-controlled environments ideal for protecting your data. OneNeck data centers are designed around an extreme availability architecture, and in addition, are built in geographic areas that are safe, secure and have access to reliable, low-cost utilities. And if it's validation you need, they're certified by third-party commissioning engineers and agents, and independently tested and validated.

OneNeck's successful independent examination of its information security program by a CPA provides OneNeck's healthcare customers assurance that their information security program is fairly presented and that it adopts essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 (HIPAA) and the Health Insurance Technology for Economic and Clinical Health Act (HITECH).

So don't settle for anything but 100% peace of mind when deciding to colocate your data with a partner. OneNeck owns and operates our facilities — we aren't selling you someone else's data center. Our data centers house our customers' infrastructure as well as our own. You'll receive the same attention to detail and focus on uptime that we count on too.

Come check out one of our data centers in your area today, and see why with OneNeck, your data's security is our number one priority.

OneNeck®
IT SOLUTIONS
a TDS® Company

Part #1.5.4_ARC_0117_v1

Call 855.ONENECK | Visit OneNeck.com