HIPAA Security and Patient Data

High-profile data breaches continue to push healthcare toward an increased focus on security. Experts predict that within five years there will be nearly 50 billion smart connected devices in the world. All will have the ability to collect, analyze and share data. According to a study published in the Journal of Medical Internet Research, “75 percent of adults will use a Personal Health Record by 2020, exceeding the adoption targets initiated with Meaningful Use Stages 2 and 3”. Our challenge becomes the ability to protect these large stores of data ([ePHI](http://searchhealthit.techtarget.com/definition/electronic-protected-health-information-ePHI)). Add to this the interoperability and interconnectivity of multiple EHRs, PHRs and HIE systems, and our ability to secure patient information becomes even more complex.

Security measures such as firewalls, antivirus software, and intrusion detection software can be conducted to protect data integrity. There are data loss prevention tools, anti-malware, identity management and authentication programs, and even role-based access and data security solutions. These strategies reduce the risk and help protect patient health information, yet at what cost? There are over 70 different requirements that fall under the HIPAA Security umbrella. It’s critical to ensure **ALL** systems where [ePHI](http://www.hhs.gov/answers/hipaa/what-is-phi/index.html) resides. EHRs are just one piece of the vast [HIPAA compliance](https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/) puzzle.

According to Zack Whittaker in an article published in ZDNet "A hacker who claims to have obtained more than ten million health records is selling the data to the highest bidder on the dark web. A non-technically-proficient cyber thief criminal can purchase tools to exploit a vulnerable healthcare organization, through the use of a little free technical support, extracting 1,000 patient records that could net him about over 15k”. Cybercrime is escalating. The need to secure patient health information becomes more urgent with each passing day.

Fogo Data Centers CEO Bill Esslinger, prior Vice President, General Counsel, Secretary & Chief Privacy Officer at Greenway Health, says “the more extensive our healthcare systems becomes the more time and effort is required to provide optimal protection”. CIO’s are experiencing digital overload. “The average global cost of a data breach per every lost or stolen record is $158. Healthcare organizations, however, had an average cost of $355 per record”, according to the new survey conducted by Ponemon.

Most healthcare organizations are not adequately prepared to protect sensitive data from data breaches, since most of their IT investment is spent on patient care and not data security. Understanding the risks and responsibilities associated with managing ePHI is the first step in protecting patient information. Put safety and compliance first in designing your strategy. Seek partners who understand HIPAA compliance and data security and share your organizations best practice guidelines.

Data breaches, malware and ransomware attacks are not only increasing, they are becoming more sophisticated. #KnowYourCloud is not merely a hashtag for [Fogo Data Centers](http://fogodatacenters.com/). It means know the people involved in the data management solutions you choose, know their experience, and their years of practice in healthcare and Health IT. More than 40 million people have had their protected health information compromised in HIPAA privacy and security breaches. Know who you’re doing business with today, to improve patient and provider security in our era of value based care and increased connectivity. As we accelerate the shift to a higher-performing healthcare delivery system we must examine our ability to protect it.