# HIPAA: Opportunity Rather than an Encumbrance

February 4, 2015

*Guest post by Roman Foeckl, CEO and founder, CoSoSys.*

Roman Foeckl

Since HIPAA was enacted in 1996, IT security specialists in the healthcare industry have often been confused by the complex regulations the U.S. government has put in place to carry out the law. Even for experts that were already used to untangling complicated IT security practices, HIPAA regulations have remained a bit of a mystery. What may not be appreciated is that the great work being done by these patient and hardworking industry professionals is setting a new standard for enterprise security that the rest of us can follow.

When we began working on a HIPAA component of our data loss prevention solution we began view it as an opportunity rather than an encumbrance. Here are four reasons why:

**Addressing the Previously Unaddressed:** Thanks to HIPAA, the healthcare industry is now more aware of the need for a strong data security program. For example, who would have thought that protecting healthcare information should include IPs or postal addresses? Finding the ways to protect this type of data has now become much more critical, and an area of potential risk and huge legal and regulatory costs is now contained. This level of detail and control is something the rest of the industry can learn a great deal from.

**Paving the Way:** Regulations like HIPAA are essential to protect one of the most private aspects of our lives — information about our health and well-being. This is an opportunity for organizations to position themselves as industry leaders in information security that view patient privacy protection as absolutely equal with patient health. This level of care will reflect very highly on the institution as a whole.

**Adding Value:** This is an opportunity for all healthcare information security professionals to rise up and demonstrate that the most critical data of patients can, and will, be protected. HIPAA came about because many felt that healthcare organizations were being lax and not protecting our most critical and personal data. An organization can be perceived as cutting edge in an area that is understood by the public at large. By having a best practice obligation to provide patients with an industry leading protection you are reinforcing your commitment to patient advocacy and care.

**Staying Ahead of the Threat** : By being on the forefront of data protection, you are demonstrating to the industry and public at large that you are not simply filing their information away and hoping for the best. Rather, you are actively monitoring their most intimate details and are making sure you are aware of any potential breach before it becomes an issue of concern to the patient. You are following an industry best practice that is well ahead of the retail and banking organizations patients deal with on a regular basis. You can tell them this is due to this information being more intimate and vital which explains this extra vigilance.

Organizations that fall under the regulations of HIPAA carry the huge obligation of protecting patients' records and personal information to avoid massive fines and lawsuits, as well as the burdens of patient-doctor confidentiality. Starting with solutions like antivirus, data backup, firewalls, etc. to avoid corruption of data and external attacks, and continuing with data loss prevention and mobile device management solutions to address the internal threats, data security specialists must consider human behavior when creating personalized policies for their organization. For that reason, employees have to be trained on the changes and best practices for data security, so that an innocent error or the lax attention to a detail doesn't become a major financial, and reputational, hit to the organization.

The healthcare profession has as one of its cores the concept of confidentiality. Retailers, financial institutions and

others get do-overs when they have data loss events. Healthcare organizations have a legal and moral obligation to protect patient privacy and that’s why you need to make sure your HIPAA regulations are closely tied to data security operations.