The road to HIPAA compliance

on 13 October 2015 at 3:28 pm

Egor Kobelev, DataArt

On the road to becoming HIPAA compliant very few of the challenges are related to technology. It's more than just having compliant software; the real trick is understanding that HIPAA compliance is not a destination, but a long journey of continuous improvements to company operations and procedures. Having been a companion in such a journey for many healthcare companies for nine years now, I wanted to share some observations of what I've seen along the way.

HIPAA compliance implementation is not a straightforward exercise, and a larger portion of its complexity resides in the very first step – planning. There are as many approaches to the process as the number of companies moving towards HIPAA compliance. Each plan is rather unique and heavily depends on the type of company (Hospital, Health Plan, Insurance Company, Clearing House, 3rd Party Administrators, etc.), as well as its specific needs and goals. Through helping our customers we've built a solid knowledgebase around specific types of HIPAA compliance implementation and have come up with our own unique approach to it.

When it comes to planning, I would roughly define three specific areas to be affected by HIPAA compliance: the process, infrastructure, and technology.

PROCESS

The cornerstone of HIPAA compliance is all about the process and paperwork. Not only should business processes in an organization be in line with HIPAA law, they also have to be properly documented as HIPAA Standard Operating Procedures (SOP). Processes and SOP are certainly interconnected, as SOP should reflect the company's operations,

while operations should comply with the SOP. There are a number of ways to get this documentation in place; the typical one is to engage a specialized consultancy for process review and documentation. The downside of such an approach is the cost; a budget of hundreds of thousands it is not something unheard of here. At DataArt we help our clients avoid these costs by putting together all the appropriate documents and making sure all the critical procedures have been properly introduced.

INFRASTRUCTURE

HIPAA compliance heavily depends on a company's IT and infrastructure. It is quite a rare case nowadays that a company decides to build and run their own data center. It usually requires a fair amount of upfront investments as well as maintenance costs. In some situations, it makes sense to go this way, as it gives the company total control over PHI data. However, it requires that the infrastructure is built in such a way that none of the components violates HIPAA.

The dawn of cloud technologies and cloud hosting offerings came with a security concern. Going cloud means decreased control over data, access to it, and even the physical location of data. Early cloud offerings did not support HIPAA requirements. Some of them still don't. Choosing a hosting partner in line with HIPAA and following through with the execution of Business Associate agreements require a lot of thought put into it.

TECHNOLOGY

In comparison, this one is the easiest; you need your software developed in accordance with the HIPAA Privacy and Security Rules. It is as simple as that. Or is it? All HIPAA requirements have technical implications that one has to be aware of. To achieve this we maintain internal technical guidelines and facilitate training sessions for the engineers and management involved into healthcare projects. A useful trait in a vendor is being capable not just to develop HIPAA complaint solutions from scratch, but to take over an existing solution from the client, establish a technical review, modernize the solution and fine-tune it so it becomes HIPAA compliant.

The path to reaching and maintaining HIPAA compliance might seem long and rough, and in a way it is. But when you have a loyal companion, a reliable guide to show you the way, the journey won't nearly be as hard.

By Egor Kobelev, Engagement Manager at DataArt

Original article — http://pixelhealth.net/2015/10/13/the-road-to-hipaa-compliance/