WinMagic provides healthcare information security and privacy

29 August 2018 | Interviews

Healthcare globally has been a key business segment for us led by the US. Emerging Geographies like India have started contributing and WinMagic sees this segment as a key growth vector

Established since 1997, WinMagic Inc. provides the world's most secure, manageable and easy-to–use data security solutions. WinMagic's SecureDoc™ Environment is an award-winning enterprise disk encryption solution and key management product that is trusted by thousands of enterprises and government organizations worldwide.It is ideal

for healthcare information security

Mr. Rahul Kumar- Country Manager, India & APAC, WinMagic Corp *in a conversation* **with** *BioSpectrum about Importance of data protection in Healthcare sector of India.*

1) How will GDPR specifically affect healthcare?

Technology—more than infrastructure—makes healthcare affordable, accessible and available to a large, disparate population. Private organizations are filling the last mile gap in healthcare service delivery, and they require ready access to data for building solutions. They have experience and expertise, and they are ready to enter developed markets where healthcare schemes are borne by the government. These organizations thrive on direct link to welfare schemes, insurance, data, etc., for their operations, predictive analytics and other routine processing.GDPR has changed the way these businesses operate because they no longer have ownership over the data.

2) How can healthcare organizations comply with GDPR?

GDPR prohibits unnecessary collection of personal data. Moreover, certain personal data—known as genetic data, data concerning health, and biometric data—can't be processed unless it falls into certain categories. In any case, exceptions do exist and allow for data collection—for instance, when data is provided with the owner's consent, when data benefits the owner, when data is used for public good, etc.

3) What are the penalties for non-compliance?

The cost of noncompliance is very high. In case of a compliance failure or a data breach, fines are calculated based on a number of factors. It varies between the standard four percent of global income and 20 million Euros, whichever is higher.

4) What options are there to protect privacy/anonymity?

Privacy is not an end in itself; in fact, encryption is a given when it comes to GDPR. There are also obligations relating to accountability, protection, and transparency among other things, which all come together to ensure the individual's right to data and security. This also includes the requirement for organizations to identify the person responsible for data protection, policies and procedure.

5) What will be the impact of EUGDPR on the global market and how equipped are the Indian healthcare companies today?

Prior to GDPR, personal data was viewed as the property of the businesses that collected and stored the information. It is now the individual's property. This is a radical shift, and it influences how businesses behave. On the issue of Indian healthcare companies looking to do business in Europe, I think the cost of noncompliance is a major deterrent. Secondly, there is still some grey areas relating to understanding various data processing requirements and the legal basis for carrying them out. The dust needs to settle firstand that's going to take some more time.

6) What is the right way to handle a data breach?

A breach is not the issue here; noncompliance to GDPR is. Breaches have become a part of the modern business landscape! Therefore, effective governance and adherence to standards is very important in today's world of business. In GDPR framework, a series of steps should be initiated within 72 hours of identifying a breach. In any case, this poses a serious financial and reputational risk if noncompliance to norms is found lacking. One way to ensure that a breach would not likely result in a risk to EU resident data owners is to encrypt all collected personal data. Organizations need to consider their ability to support large amounts of encrypted traffic in transit and at rest.

7) Why is it necessary to create a Data Breach Preparedness Plan for healthcare organizations?

Healthcare organizations have a unique set of higher standards to adhere to. For instance, these organizations cannot process certain personal data categories until they meet the parameters set by GDPR. These data are categorised as genetic data, data concerning health and biometric data. It is therefore important that healthcare providers and their supply chain

must identify and test incident response management plans to protect their core business functions. This will ensure cyber resilience and business continuity in the event of a data breach.

8) How does WinMagic play an important role in Indian pharma sector to protect data breaching?

Information security management is critical in the pharmaceutical industry. It includes providing protection to not just patient information, but also monitoring the supply chain security, providing patent protection, and mitigating insider threats. WinMagic'ssolutions provide the necessary security layers that are proactive, intuitive, and built to last.

9) What are your business expansion plans in the Indian and global healthcare sector?

Healthcare globally has been a key business segment for us led by the US. Emerging Geographies like India have started contributing and WinMagic sees this segment as a key growth vector. Global compliances like HIPAA and now Disha which is aimed at being Indian healthcare security regulations poses to bring in significant growth driver for adoption for encryption as a technology.