Healthworld.com
From The Economic Times

Industry · 4 Min Read

Is India Lacking Healthcare Data Security Guidelines?

If India can establish itself as a HIPAA compliant country, there is more potential for business opportunities from other countries.

ETHealthWorld
Updated On Jan 16, 2022 at 03:08 PM IST

Read by 5286 Industry Professionals

By Ashish Kaushik

Data is being stored and managed in the cloud at what feels like alarming quantities – and the exponential rise is on track to continue. A large proportion of this is sensitive healthcare data (especially with the proliferation of mobile health apps) which should be governed by the most stringent data security regulations. So, when it comes to protected health information (PHI) and data security, what policies come to mind? It's likely HIPAA will feature high on your list. While HIPAA Law is primarily designed for US citizens and healthcare organizations, regardless of where in the world they are located, other countries have also developed HIPAA equivalents for healthcare data protection and privacy. For example, EU General Data Protection Regulation (GDPR), Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, or The Privacy Act 1988 in Australia.

Despite this, India, one of the most populous places on earth generating vast volumes of healthcare data, has yet to define its own guidelines governing the protection and security of healthcare data. Software developers in India, building applications for the healthcare industry, will almost definitely process or manage PHI, which automatically makes them business associates.

The good news is that there is something in the pipeline. But in the meantime, unless Indian Business Associates can demonstrate HIPAA compliance, it could prove a set-back to the Indian IT industry if US organizations are cautious about engaging their services. Therefore, if India can establish itself as a HIPAA compliant country, there is more potential for business opportunities from other countries, including the US.

The Future Looks Bright for Indian PHI

The current legal framework in India, relating to protected health information, is governed by Information Technology Act 2000, along with Information Technology (Reasonable Security Practices and Procedures, and Sensitive Personal Data or Information) Rules 2011. Together, they provide a degree of PHI protection, but with rapidly advancing IT technology there are potential data security 'gaps'.

In view of this, the Indian Government are working to enact the Personal Data Protection Bill, along with the proposed Digital Information Security in Healthcare Act (DISHA). DISHA, being India's HIPAA equivalent, could enforce the implementation of enhanced data security solutions. While this may require additional investment, the need to protect personally identifiable information (PII) and PHI cannot be underestimated.

The Benefits of Being HIPAA Compliant

While the Indian Bills are still under debate in parliament, HIPAA Compliance is mandated for organizations working in healthcare, not just in the US but many globally. Therefore, India can benefit from the direction on data security and privacy rules and regulations derived from this statute:

- HIPAA Security Rule sets out administrative, physical and technical safeguards for electronic PHI in order to ensure digital PHI is secure, reliable, and confidential. It focuses on the protection of data from unauthorized access, internal or external, as well safe storage and transfer

- HIPAA Privacy Rule concentrates on the rights of patients as to how their PHI is used, in strict accordance with confidentiality. Only patients can grant permissions for their PHI to be disclosed with ancillary services or third parties. It also gives patients the right to obtain copies of their health records.

In order for Indian software developers to achieve HIPAA Compliance, there are some overarching factors that need to be addressed:

- Regular self-audits – to assess the strength of admin, physical and technical safeguards. Any identified data security vulnerabilities should be rectified immediately.

- Documented Policies – to demonstrate how an organization complies with the HIPAA Security and Privacy Rules, and states appropriate uses and disclosures of PHI. This includes incident management procedures, in the event of a data breach.

- Staff Training – any employee associated with handling PHI needs to complete annual training to keep them up-to-date with cybersecurity and HIPAA basics, internal policies and procedures, and their individual responsibilities.

- Business Associate Agreements – outsourced service providers that your organization works with must also be HIPAA compliant if they handle any client's PHI on your behalf. For example, cloud platform provider, communication provider, data processors, etc.

Bottom line:

Once the Indian bills, currently in debate, are passed, there will likely be a roll-out timeline, by which time healthcare organizations and healthcare technology solution providers must be compliant. DISHA, the closest thing to Indian HIPAA Compliance, will certainly help set standardized benchmarks. In the meantime, steps taken now to increase responsibility for healthcare data security and compliance will ensure the future of IT technology businesses are not left behind.

Ashish Kaushik, CISO, SourceFuse