BioSpectrum the business of Bio & Health Sciences

Enable fair use of data to usher innovation

10 November 2020 | Views

The health data is sensitive, and hackers look to exploit a weak link in the system

A potential transformational moment arrived in the healthcare scenario of the country with the launch of the National Digital Health Mission. According to a Lancelet study, India ranks 145 among 195 countries in Healthcare Access and Quality (HAQ) Index, below its neighbors like China, Bangladesh, Sri Lanka, and Bhutan. The need for an overhaul in healthcare infrastructure and delivery systems was therefore always there, and the pandemic made us wary about it again.

While the healthcare system strives to transform telemedicine and bring in digital maintenance of health records and information systems, challenges with data privacy need a discussion. To realize the full potential of the transformation, addressing issues with regards to the protection of patient records and safe use of data are issues that need to be addressed. We have witnessed that Health information systems and Electronic Medical Records (EMRs) can be prone to cyber-attacks globally. The data breach exposes a patient's confidential data with severe consequences on their lives. The health data is sensitive, and hackers look to exploit a weak link in the system.

Preventing such attacks thus requires a foolproof system across the players in the sector. Establishing standards mandating requirements for the transmission and electronic maintenance of health information reduces vulnerability to attacks. However, as of today, many healthcare institutions that include both the public and private players may not have the necessary wherewithal to follow those standards. Adhering to such norms brings cost implications and, organisations who may have scant resources may find it daunting to comply with the norms.

Access to EMR is a sensitive policy and has to be understood in the light of multi-disciplinary clinical teams providing holistic care to patients. Access rights of clinicians and support staff and read-only or editing rights should be predefined. Similarly, we need stricter norms to govern the usage of Cloud computing systems. To further safeguard patient data, access rights given to third-party apps that will use the Hospital database should be covered by the Institutional policy.

Healthcare today constitute a wide and fragmented number of healthcare institutions. These institutions have varied resource capability and their ability to revamp their current infrastructure to venture into digital health-tech could be limited. Public health infrastructure in India remains poor and the transformation to digital healthcare while ensuring data privacy will depend on boosting the current health expenditure. Portability of data without compromising with data privacy is a critical component of telemedicine to unlock an 'open' health data eco-system. These will entail investments to bring changes in the required

hardware and software system.

As these changes are implemented, training the workforce and making them aware of the various aspects of maintaining data privacy and handling digital records will be necessary. To prevent any accidental leakage, institutions must also encrypt the data. Already starved of resources, many Public and private healthcare institutions will find it difficult to allocate their resources.

The Personal Data Protection Bill, tabled in the Parliament, defined measures to protect the health data of the patients. In light of this, health institutions must ready themselves for internal and external threats while handling health data. Setting accountability while handing health data is necessary and the organization must bring changes in terms of security safeguards, carry proper risk assessment, and understand supply chain risk. Informed consent is a critical dimension to data privacy and it should be strictly adopted when patient data is used for research purposes.

There should be robust debate governing the monetization of patient data even after obtaining informed consent. The medico-legal ramifications of a breach of such policies and the resultant penal provisions need more spotlight. The NDHM principles should also be co-opted by the Clinical Establishment Act passed by various State Govts. NABH should improve upon the existing standards and train the assessors based on NDHM guidelines.

In a country with a population of over 1.3 billion with inadequate health standards and fragment players, integration of health-tech is undeniably a humongous task. The synergies developed as a result of such implementation will be transformational. Given we are still at the early phase of the transformation, protecting data privacy right at the onset is an essential component in building trust and encourage adoption among the patients. At the same time, while keeping data privacy concerns in the centre of things, it will be crucial to create balance and enable fair use of data to usher innovation and better health treatments. A lot will depend on how sensitive we are towards protecting data in the successful implementation of telemedicine.

Dr Harish Pillai, CEO – Aster India, Aster DM Healthcare