BioSpectrum
the business of Bi
24 years of leveraging the business of Bio
www.biospectrumindia.co

Embedding privacy in Indiaâ??s MedTech ecosystem

01 June 2026 | Views | By S Chandrasekhar, MD & CEO, K&S Digiprotect Services

Indiaâ??s MedTech ecosystem now extends beyond physical devices to include connected systems, diagnostics, IoT, and AI-driven solutions. However, regulation remains fragmented. While medical devices are governed by the Central Drugs Standard Control Organisation (CDSCO) through the Medical Devices Rules, 2017, software and IoT-based technologies are not. With the Digital Personal Data Protection Act (DPDPA) coming into force, this gap is no longer sustainable. MedTech solutions increasingly process sensitive health data, often across borders. Almost 70 per cent of Indian medical devices are imported from foreign suppliers. This creates a need for system-level data-flow governance across the entire MedTech ecosystem. This includes hospitals, device manufacturers, software developers, and AI deployers. Just as strong regulatory standards exist for clinical evidence, similar standards are now required for data and AI governance. Embedding Privacy by Design and adopting global standards such as IS/ISO 27701, IS/ISO 42001, and ABHA (Ayushman Bharat Health Account) will be key to ensuring compliant and future-ready MedTech systems.

The medical devices sector in India is an essential and integral constituent of the Indian healthcare sector, particularly for the prevention, diagnosis, treatment, and management of all medical conditions, diseases, illnesses, and disabilities. The terms MedTech and medical devices are used interchangeably. While the medical devices industry is often understood to be limited to physical products, the broader MedTech industry also encompasses digital solutions such as telemedicine platforms, home diagnostic devices, AI-enabled software for disease detection embedded within products, and specialised medical equipment, including ocular implants.

In India, the medical devices industry is regulated by the Central Drugs Standard Control Organisation (CDSCO), which also regulates the pharmaceutical industry. Unlike in other countries where drugs/pharmaceutical products are regulated separately from medical devices, in India, medical devices are regulated under the Drugs and Cosmetics Act, 1940 (Act) and more specifically Medical Device Rules, 2017. Medical devices in India are defined as ‘drugs’ under Section 3(b) of the Act.

The Indian MedTech market will expand to about $12 billion by 2030, according to an EY report. Due to changing lifestyles and technology, medical devices are no longer simple, standalone equipment. They now have operating systems and are connected to networks and other devices. Earlier, monitoring heart rate was done by standalone ECG machines in hospitals and nursing homes.

Today, IoT devices such as the Apple Watch monitor heart rate efficiently. Due to the growth in technology and shift in nature of medical devices from freestanding to Internet of Things (IoT), health data (categorised as ‘personal data’ under India’s data privacy law) generation and processing volume have increased exponentially. The digitisation of healthcare has given caregivers the power to access, analyse, manage, and share patient data, helping to transform care and lower costs. But millions of connected medical devices, systems, and networks make hospital and patient data highly vulnerable to cyber-attacks, and consequently, data privacy issues also emerge. As the medical devices are connected to networks and transmit data, the threat of cyberattacks looms large.

As per a report of Philips, EMR systems are increasingly connecting to hospital networks and are constantly feeding EMR systems with patient physiological data. The multitude of vendors, legacy networks, and devices in any given hospital provides attractive access points for bad actors to extract volumes of valuable patient data. Moreover, currently, the medical devices sector is 70-80 per cent dependent on imports.

DPDPA in the MedTech sector

In this regard, it's important to examine the privacy compliance imposed by the Digital Personal Data Protection Act, 2023. This is because the DPDPA has a fine of up to Rs 250 crore. The DPDPA requires significant efforts by the MedTech sector for compliance, like, for instance:

- **Notice and consent** – Taking consent from patients before processing their health data or transferring their health data to other stakeholders. If MedTech device operators or manufacturers aren't directly processing patients' personal data, then they must enter into a formal data processing agreement with hospitals. A typical data processing agreement should state clauses such as cross-border data transfers, data principal rights management, grievance redressal, data retention, etc.
- **Reasonable security safeguards** – MedTech manufacturers must implement robust information security measures within medical devices. These measures should include encryption, obfuscation, masking, and tokenisation of personal data. Strong access control systems should also be implemented. Manufacturers should also maintain secure data backup and recovery processes. Audit Overall, appropriate technical and organisational measures must be adopted to ensure the protection, integrity, availability, and confidentiality of personal data.
- **Data Protection Impact Assessment (DPIA)** –This is an assessment of risks based on the necessity and proportionality of processing of personal data. It also contains a description of processing operations. Under DPDPA, DPIAs are mandatory for significant data fiduciaries. Given that MedTech sector devices are processing sensitive health data of patients, they must conduct DPIAs. Given that nearly 80 per cent of medical devices are imported, it is imperative for entities operating such devices to conduct a DPIA and ensure that any transfer of personal data outside India is carried out lawfully and subject to appropriate safeguards.
- **Privacy by design (PbD)** – Embedding PbD involves embedding data privacy into the core architecture of medical devices, software, and health applications from the development phase. It is essential in managing significant privacy risks associated with connected devices, wearable technology, and AI in healthcare. For example, A heart rate monitor analyses ECG data on the device itself and only sends processed, aggregated insights (e.g., 'normal sinus rhythm' or 'one anomaly detected') to the cloud, rather than storing and transmitting continuous, raw, identifiable physiological data.

As per the Central government notification dated November 14, 2025, all entities, including the MedTech manufacturers and operators, will need to be compliant with the DPDPA by May 14, 2027.

Adopting voluntary standards

There are several voluntary standards that are available; the adoption of which by the MedTech manufacturer or the hospital that is operating the MedTech device can lead to heightened security. Some of these standards are –

- **IS/ISO 27701:2025 Privacy Information Management System** – ISO 27701 is a standard that specifies requirements for establishing, implementing, maintaining, and continually improving a privacy information management system. It is applicable for all types and sizes of MedTech manufacturers, as well as hospitals or medical practitioners who are using the medical devices.
- **ISO 42001:2023 – Artificial Intelligence Management System** – AI is being increasingly applied in the MedTech ecosystem, utilising information technology, and is expected to be one of the main economic drivers. Adoption of this standard will help organisations responsibly perform their role with respect to AI systems (e.g., to use, develop, monitor, or provide products or services that utilise AI systems).

Targeting structured DPDPA

The MedTech industry is becoming increasingly connected. Software, medical devices, and health data are now constantly exchanged across multiple stakeholders in the ecosystem.

With the Digital Personal Data Protection Act, 2023, being enforced from November 14, 2025, and compliance timelines extending till May,14 2027, participants across the MedTech sector must prepare for compliance. This includes manufacturers, hospitals, software providers, platform operators, and white-labelling entities.

Given the volume and sensitivity of health-related personal data involved, undertaking a structured DPDPA implementation exercise is essential for the sector.

S Chandrasekhar, MD & CEO, K&S Digiprotect Services

(with inputs from Aman Varma, Senior Manager – Legal and Regulatory Affairs, K&S Digiprotect Services)