Point of view on the Health Data Management Policy-2020

Overview

The health care, life sciences, and pharmaceutical industry continues to grow across the globe and solidify its foothold in India. The current pandemic has increased the focus on the health care sector. The involvement of the sector has become the key driver in developing a robust digital health care data management system. In order to set up this digital system, the Ministry of Health and Family Welfare (MoHFW) launched the National Digital Health Mission (NDHM). This Government of India project stems from the National Health Policy, 2017 and intends to digitise the entire healthcare ecosystem of India towards a single source of truth about the health status of the nation.

The objective of this mission is to create digital health records, as well as to set up and maintain registries for healthcare professionals and health facilities in order to ensure a smooth interoperable framework for the multiple partners associated with healthcare delivery. This mission will enable individuals and health care providers to benefit from the opportunities that would arise from progressive digitalisation of health records. This policy acts as a guidance document for the National Digital Health Ecosystem (NDHE) and outlines the new standards for data privacy and protection.

The MoHFW has focused, specifically, on India's interests in the health care sector. Government of India has approved the Health Data Management Policy, after addressing all the privacy and security concerns received from various stakeholders. As healthcare companies in India capitalise on the data-driven ecosystem, this policy attempts to streamline the protection of personal data, sensitive personal and health-related data and provide full control to an individual over the data they generate. This policy overlaps with the Personal Data Protection bill with respect to its Privacy principles, focusing on the principle Security and Privacy by Design for the protection of individuals' data privacy, throughout the life cycle of the data processing.

The objective of this policy is:

- to provide adequate guidance and to set out a framework for the secure processing of personal and sensitive personal data
- to implement adequate technical and organisational measures across the ecosystem
- to create a system of personal and medical health records which is easily accessible to individuals and health service providers
- to create awareness of the importance of the data privacy and embed or build the privacy mindset
- to ensure the national portability in the provision of health services
- to establish appropriate institutional mechanism for auditing of the NDHE, Draft Personal Data Protection Bill-2019 has categorised health data as sensitive personal data.

It would be interesting and thought-provoking to see if the Personal Data Protection Bill-2019 and the Health Data Management Policy-2020 will be able to achieve such a high level of harmonisation.

Key Highlights:

Roles in the Health Data Management Policy:

- **Data principal:** The person/ individual to whom the collected data pertains
- **Data Fiduciary:** The entity that determines the purpose and means of collection and processing of personal data
- **Data Processor:** The entity which processes the personal data on behalf of a data fiduciary
- **Health information Users (HIU):** HIUs are entities that are permitted to request access to the personal data of a data principal with the appropriate consent of the data principal
- **NDHM DPO:** National Digital Health Management Data Protection Officer
- **NDHM CISO:** National Digital Health Management Chief Information Security Officer.

Classification of Records:

- **Electronic Health Records (EHR):** EHR (similar to the Protected Health Information -Health Insurance Portability and Accountability Act) is a collection of various medical records that get generated during any clinical encounter or events.
- **Electronic Medical Records (EMR):** EMR refers to a repository of records that are stored and used by the Health Information Provider (HIP) generating such records to support patient diagnosis and treatment. EMR may be considered as a special case of EHR, limited in scope to the medical domain, or is focused on the medical transaction.
- **Personal Health Identifier (PHI):** PHI is the data that could potentially identify a specific data principal and can be used to differentiate such data principal from another.
- **Personal Health Records (PHR):** PHR is a health record that is initiated and maintained by an individual.

Consent Mechanism: Data principals should be given complete control and decision-making power over the manner in which personal or sensitive personal data associated with them is collected and processed further; data fiduciaries would be required to obtain an explicit consent from the data principal to process the data.

Privacy Notice: All data fiduciaries must provide a clear privacy notice to all data principals:

a) Prior to collection of personal and sensitive personal data or further processing it for new or previously unidentified purpose

b) At the time of change in the privacy policies and procedure

Security of data: All the data fiduciaries will implement the International Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System - Requirements as well as any other standard as may be applicable to them.

Monitoring: All the data fiduciaries/processors are required to maintain the audit trail of all the activities related to the processing of personal and sensitive personal data. However, the updated personal data with a new version number should be considered active. The advisory standard for audit trail /log in the health record system is ISO 27789:2013 Health informatics - Audit Trails for Electronic Health Records.

Data Sharing: Data fiduciaries may share processed personal data of data principal with a HIU only when the data principal provides consent. Data fiduciary should maintain the record of all the shared data in accordance with the data principal's consent for audit purposes. Further, according to this policy any personal or sensitive personal data of data principal should not be published or displayed/ posted publically.

Regulatory Comparison: PDPB-2019 v/s HDMP-2020

Domains	Similarities	Differences
Scope	Applicable to any entity processing personal data of any individual in India.	Personal data protection bill is industry and sector agnostic, whereas Health Data Management Policy is specifically applicable to Health care and its relevant sectors
Grounds of Processing	Data Principals freely given consent is defined as primary grounds of processing under PDPB and Health data management policy	Participation of the data principal in the NDHE as set out under this policy should be on a voluntary basis and data can be processed on the basis of consent.
Sensitive Personal Data	Financial information, such as bank account or credit card or debit card or other payment instrument details, is considered as part of sensitive personal data along with health data under PDPB and Health data management policy	-NA-
Rights of Individual/ Data Principal	Common Data Principal rights under PDPB and HDMP are :- • Rights to confirmation and access, • Right to correction and erasure, • Right to data portability	Right to be forgotten under PDPB has been named as Right to restrict or object to disclosure in Health Data Management Policy
Data Security	Personal Data Protection bill and Health Data Management Policy include that the data fiduciary and the data processor should secure all personal data that they have processed by reasonable security practices and procedures including— a) use of methods such as de-identification and encryption; b) steps necessary to protect the integrity of personal data; and c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data	According to HDMP data fiduciaries will implement the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" as well as any other standard as may be applicable to them.
Data Sharing	Organisations are required to obtain individual's consent prior to transfer of personal data under PDPB and Health data management policy.	-NA-
Data Storage and Retention	Organisations are required to store the personal data only as long as it is required to satisfy the purpose for which it is processed and store a copy of personal data on servers or data centres located in India.	-NA-

Key take aways from Policy:

1. All data fiduciaries are required to perform a detailed data protection impact assessment before undertaking any processing which carries a risk of significant harm to data principals
2. Data fiduciaries should maintain accurate and up to date records to document operations of the data lifecycle i.e. collection, transfers, storage, and erasure of personal data and sensitive personal data
3. Data fiduciaries should conduct periodic audits to verify whether their employees and data processors are appropriately in compliance with privacy notices, confidentiality agreements. Data fiduciaries are required to maintain the original personal data and an audit trail of the changes to the data principal
4. This policy has introduced Consent Manager (similar to the Personal Data Protection Bill). Consent manager would be responsible for obtaining, withdrawing, reviewing and managing the consent collected from data principals
5. The timeline for compliance with the policy has not been defined in the current version of the policy. To ensure seriousness and define a starting point of enforcement, this policy should be implemented within 18-24 months from the date it gets passed
6. All data fiduciaries should have a strong automated system to maintain the records to track and respond to in case of breaches or incidents
7. The National Health Agency should provide notification of cybersecurity incidents to Indian Computer Emergency Response Team (Cert-In) and entities should follow the incident reporting guidelines from Cert-In
8. In case of the violation of any provisions of this policy, then an ID issued to such entity/individual may be suspended or cancelled, and during such time of suspension or cancellation, such entity/individual should not be permitted to participate in the NDHE. The procedures involved in such suspension/ cancellation and the details of the consequences thereof may be further set out by the NHA.

Q1: Is this Policy applicable to you?

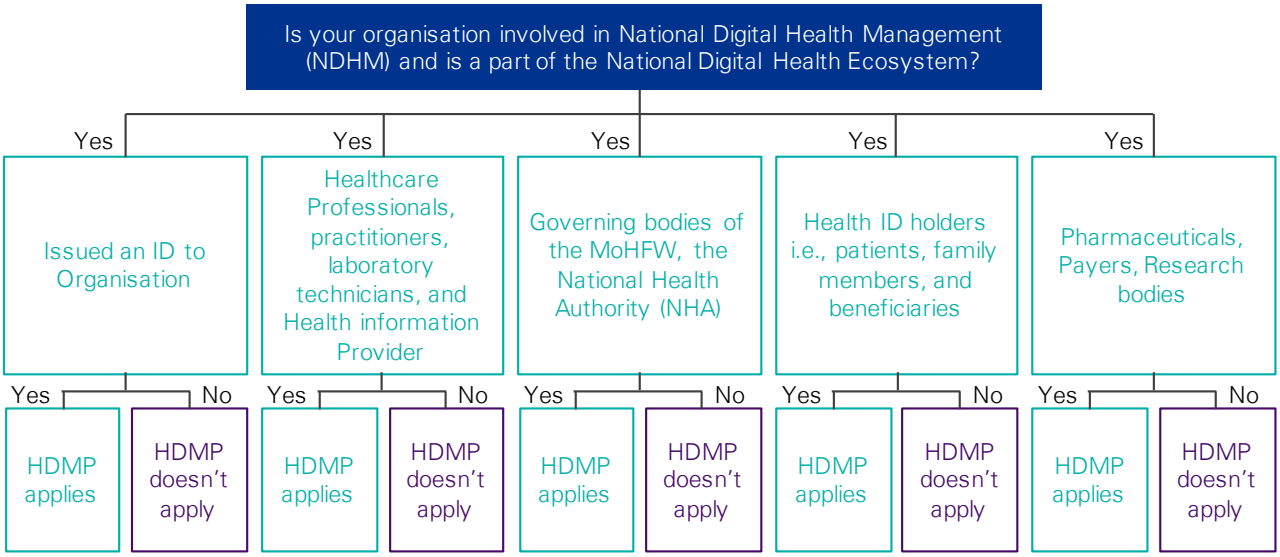
Q2: Do you collect, process, use and store personal and sensitive personal data?

Q3: Identify the applicable role for your organisation role under this policy.

Way Forward:

As Government of India has approved the Health data management policy, organisations and government agencies across India need to kickstart their journey. It is critical to have a robust framework that safeguards the privacy of confidential health data collected from individuals in India. This will be crucial in shaping trust as well as ensuring that the personal and health data of all individuals in India is adequately protected.

Applicability



If your answers to above questions are "Yes", you may require to take an action to understand the importance and implications of being in the healthcare sector and the competitive advantage to comply with Health Data Management Policy. Some key points to create an implementation roadmap are listed below:

- Establishment of Governance structure
- Perform Risk Assessment
- Incorporate Privacy and Security by design
- Design health data management policies, procedures and develop data inventories
- Establish a mechanism to handle data principal requests and grievances
- Training and Awareness

KPMG in India Contacts:

Akhilesh Tuteja
Partner and Head
Digital Consulting
Co-Leader Global Cyber Security
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory
India Cybersecurity Lead
E: atulgupta@kpmg.com

Mayuran Palanisamy
Director - IT Advisory
India Lead - Data privacy
E: mpalanisamy@kpmg.com

home.kpmg/in

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia