A Critical Analysis on Health Data Management Policy

Archita Tiwari

Shri Ram Institute of Law

Abstract: *The researcher in this paper analyses different circumstances due to which the health management data policy is a big challenge in India. Today in this digital era health issues are raising in a very rapid rate. Data management is essential for healthcare organizations to ensure patient records are safe and securely handled. With an increasing amount of data being collected and stored in digital formats, it's more crucial than ever for healthcare providers to manage their data more efficiently. Health data management, also called clinical data management or health information management, is the management of the collection, storage, and analysis of patient data. This data includes demographic information (name, age, address, gender), medical history and treatments (family history, doctor visits), and administrative information (billing, scheduling, insurance, Medicare coding). There is a huge potential to harness the power of big data to generate insights to address the four big challenges of health care in India – availability, accessibility, affordability, and acceptability.*

Keywords: Health Data Management, Technological Era, Challenges, Health Care Policy, Legal Remedies

1. Introduction

Health is the primary concern of every individual and today with the increasing level of pollution people are getting more aware regarding their health but due to lack of proper management of health data and legal policies people are facing so many issues because every health institution is not technically good and they don't even understand its proper working and therefore it could be sometimes very risky regarding data privacy issues.

Health Data Management (HDM), also known as Health Information Management (HIM) is the systematic organization of health data in digital form. This can be anything from Electronic Medical Records (EMR) generated as a result of doctor visits, to Electronic Health Records (EHR), to handwritten medical notes scanned to a digital repository.

Health Data Management is tasked not only with organizing medical data but also integrating it and enabling its analysis to make patient care more efficient, and derive insights that can improve medical outcomes, while protecting the privacy and security of the data.

[1]Data are being generated exponentially on who we were, who we are, and where we need to be. A data point is a discrete unit of information. It is generated from various sources such as the internet, financial sector, health care, mobile data, and others.

Healthcare data is sensitive, and organizations must handle it with extreme care. Practitioners must adhere to rigorous standards of security set forth by federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) compliance.

To ensure protection from cyber threats, healthcare organizations can employ multiple layers of defence. Here are some of them:
- Firewalls
- Antivirus software
- Encryption technology
- Authentication methods
- User access controls.

On 26 August, the government released the draft health data management policy of the National Digital Health Mission (NDHM), which seeks to digitize the health ecosystem in India and introduce a unique health ID for every citizen. The National Health Authority (NHA) had initially asked for public feedback on the policy by 3 September, which was then extended by a week, giving citizens a total of 2 weeks for their comments.

2. Elements of Healthcare Data Management

1) Data Standardization
Data standardization is a crucial element of healthcare data management. It ensures that all data within the organization are consistent and accurately represented, making it easier to analyze and use. Without standardized data, organizations may deal with multiple datasets from different sources, leading to discrepancies in analysis or interpretation. A plan is vital for standardizing the format of all incoming data and any existing data sets. It should include developing definitions for each type of data field and setting up processes. These factors can guide them to follow the standards consistently.

Meanwhile, the community healthcare network may consider using software tools to automate processes. These may include merging duplicate records and converting file formats into one unified system. Organizations can improve their operations through faster access to information by developing an effective strategy for standardizing data.

---

[1] Lei J, Kong L. *Big Data in Astronomy.* Elsevier; 2020. 2-Fundamentals of big data in radio astronomy; pp. 29–58.

2) Develop A Broad Perspective of the Patient

Healthcare data management is essential for providing effective healthcare services. Hence, organizations must collect and analyse all relevant health information from multiple sources to form a broad patient perspective.

Here are some examples of information that can help you create a patient perspective:
- Medical records
- Lab results
- Clinical documentation
- Pharmacy data
- Billing statements
- Patient portals

Generally, considering structured and unstructured data is essential when forming a comprehensive view. You can store structured data in databases and collect unstructured data manually or with specialized software solutions.

After forming an expansive view, it should inform decisions about care delivery. For example, patients may be at risk for certain conditions based on their medical history, lifestyle habits, and genetic makeup. Hence, preventive measures or early interventions may help prevent those conditions from occurring.

3) Adapt Technology

Healthcare data management has dramatically improved through the use of technology. Electronic health records (EHR) have become increasingly popular due to their ability to store and share patient information easily, securely, and quickly.

Below are some benefits of EHR for healthcare providers:
- Providing access to comprehensive patient histories
- Tracking treatments more effectively
- Improving communication between care teams

Technology can support analytics that provides critical insights into various topics. These include clinical outcomes, operational performance, financial trends, quality assurance measures, and regulatory compliance issues. With these tools at their disposal, healthcare organizations can better understand patterns in data to make informed decisions.

4) Safeguard Sensitive Information

You can use technology to protect sensitive healthcare data. Organizations must ensure their systems are secure and have the necessary safeguards.

Here are a few ways to secure your data:
- Access control measures like encryption of files containing confidential patient information
- User authentication protocols for logging into systems
- Firewalls to block unauthorized connections from outside networks
- Regular scans for any malicious software or viruses

Healthcare organizations must establish policies and procedures to maintain the confidentiality of medical records and other related information.

Here's how to improve the security of your records:
- Control access to certain types of data
- Set limits on how long you can retain data before eliminating it from the system
- Train staff members in proper handling techniques of sensitive information
- Provide clear guidelines regarding the acceptable use of health - related technologies

Meanwhile, physical security is also critical when dealing with sensitive medical records. It's essential to store paper documents in locked cabinets. You can also keep the computer equipment in a secure room with CCTV cameras.

5) Enhance the Exchange Of Information

Healthcare data management requires exchanging information between providers and organizations to ensure patient safety, operational efficiency, and continuity of care.
To enable seamless information exchange, here are three critical practices you can follow:
- **Streamline Processes**: Healthcare organizations should streamline their internal information - gathering and transmission processes. It includes investing in communication tools like secure email services or messaging platforms to facilitate collaboration among staff members.
- **Ensure Data Security**: Data security is paramount when exchanging healthcare information. Organizations must adhere to regulations to protect sensitive patient data from unauthorized access. They should also implement multi - factor authentication measures on all devices accessing medical records or transmitting confidential data.
- **Leverage Analytics**: You can use advanced analytics techniques like predictive modelling and machine learning algorithms to improve how you exchange information. Healthcare organizations can gain deeper insights into their operations and identify areas where improvements are necessary.
- By following these practices, healthcare organizations can create an effective environment for exchanging critical patient information. Consequently, it can improve patient outcomes and attain greater operational efficiencies for the organization.

Five Health Data Management Benefits

Health Data Management can have significant benefits for healthcare organizations, medical staff and patients:
- **Create a comprehensive view of patients, households, and patient groups**—composite profiles that provide status and enable predictions.
- **Improve patient engagement**—target patients with reminders and care suggestions that can be relevant for them, based on predictive modeling.
- **Improve health outcomes**—track health trends in certain areas or among specific populations, predict new **trends and suggest proactive measures to counter rising health issues.**
- **Business decision making**—help healthcare providers make better data - driven decisions, such as which types of medical professionals to recruit, what equipment to

invest in, or which types of patients to focus on in marketing efforts.

- **Analyze physician activity**—analyze data on medical practitioners such as success rates, time invested in different treatments and medical decisions, and aligning physicians with the goals of the healthcare organization.

3. Legal Regulations

In India, digital health is governed by a few laws, guidelines, and standards. Several regulations apply universally to digital health technology, despite the fact that each digital health tool or business model is independently governed. Relevant legislation includes the IT Act, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data and Information) Rules of 2011 (SPDI Rules), and the Information Technology (Intermediaries Guidelines) Rules of 2011 (Intermediaries Guidelines). The IT Act, SPDI Rules, and Intermediary Guidelines comprise India's general data protection framework. Online transactions and the transfer of electronic data are now permitted owing to the better security provisions of the IT Act. The IT Act governs a vast array of online activities, including the authentication of digital signatures and the legal standing of electronic records. The IT Act addresses various types of cybercrime, including hacking and denial - of - service attacks.

India's current legal framework for e - health protection is governed by the IT Act and the SPDI Rules, which provide some protection for the collection, disclosure, and transfer of sensitive personal data such as medical records and histories. In contrast, legislation has lagged behind technological advances and failed to address a number of crucial issues. Thus, medical institutions and healthcare providers in India are increasingly storing patient data in electronic medical records (EMRs) and EHRs. According to the Clinical Establishments (Registration and Regulation) Act of 2010, each clinical institution is required to maintain an EMR for each patient, whose registration must be maintained. The MoHFW put out the EHR Standards for the first time in 2013. In December 2016, they were updated and made public.

[2]The EHR Standards are a set of global standards that can be used by healthcare providers to create and manage EHRs. Some of the key ongoing digital health initiatives being implemented by the MoHFW include: Reproductive Child Healthcare (RCH); Integrated Disease Surveillance Program (IDSP); Integrated Health Information System (IHIS); e - Hospital; e - Sushrut; Electronic Vaccine Intelligence Network (eVIN); Central Government Health Scheme (CGHS); Integrated Health Information Platform (IHIP); National Health Portal (NHP); National Identification Number (NIN); and Online Registration System.

These programmes are well established in the medical field and continue to generate vast quantities of data that can be utilised for the public's benefit. As health is a state responsibility, the National Health Mission (NHM) subsidises states for connected services such as telemedicine, teleradiology, tele - oncology, tele - ophthalmology, and hospital information systems.

The enforcement of standards that maintain the security, confidentiality, and privacy of patients' health and medical records is crucial. Due to the fact that private health information and records are kept under lock and key and are only used for data interpretation for market analysis, marketing, and regulatory sharing, it is very important to keep track of data protection and violations.

Regarding the use and implementation of personal data, data privacy is of paramount importance. In 2013, India's first EHR Standards were proposed. In consideration of their applicability in India, they were chosen from the best available, previously implemented international EHR standards. As a result, the 2016 EHR Standards document was alerted and made available in national IT systems for adoption by healthcare institutions and providers. [3]The MoHFW aided in its adoption by making standards like the Systematized Nomenclature of Medicine Clinical Terminology (SNOMED CT) free to use in India and by appointing an interim National Release Centre to manage the clinical terminology standard, which is gaining global acceptance among healthcare IT stakeholder communities. The MoHFW has also proposed a new bill, the DISHA, to regulate data security in the healthcare industry. This Act is intended to protect the privacy, confidentiality, security, and standardisation of EHRs. The MoHFW plans to establish the DISHA in order to promote and adopt e - health standards, enforce privacy and security measures for electronic health data, and regulate the storage and exchange of EHRs.

4. Conclusion

The draft policy looks to "set out a framework for the secure processing of personal and sensitive personal data of individuals" who will be part of the digital health ecosystem. "Sensitive personal information", according to the policy, means "such personal data, which may reveal or be related to, but shall not be limited to… financial information such as bank account or credit card or debit card or other payment instrument details; physical, physiological and mental health data; sex life; sexual orientation; medical records and history; biometric data; and genetic data".

In the backdrop of issues related to the limited time given for feedback as well as transparency and other issues—India does not have a data protection law yet.
The Union government should be focused on enacting a strong, horizontally applicable data protection law and creating an effective independent regulator— a data protection authority or privacy commission—that oversees further sectoral regulation making on data and provides

---

[2] Das AV, Kammari P, Guizie EB, Varada R, Singh G. Prevalence of ocular disorders in Liberia: A retrospective study using the eyeSmart electronic medical record system. *J Glob Health Rep.* 2019;3: e2019033. [Google Scholar]

[3]Manyika J, Chui M, Brown B, Bughin J, Dobbs R, Roxburgh C, et al. Big Data: The Next Frontier for Innovation, Competition, and Productivity. 2011. Available from: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation .

Indian residents redress and remedy if their rights are harmed.

Healthcare data management is a complex process that requires careful consideration. Standardizing the data and forming a comprehensive view is essential to maximize efficiency. At the same time, protecting sensitive data is equally vital.

Using technology can make these tasks more manageable. Also, implementing best practices can ensure the safe use of healthcare records and enhance the patient's experience.