Central University of Kashmir Law Review
Online First
eISSN: 2583-6935
pp. xxx-xxx

Digital Healthcare and Data Protection: Human Rights Perspectives in Context

Jyoti Bhakare*
Vipasha Chirmulayǂ

Abstract

The development of digital technology led to rapid progress and innovation in the field of healthcare across the world, particularly during the Covid-19 pandemic. Data-driven technologies provide benefits such as diagnostic accuracy, operational efficiencies, etc. In India, the healthcare sector is seeing advancements in infrastructure and technology, supported by state policies and initiatives. While these offer great potential for access to healthcare, they also raise human rights concerns about privacy and discrimination, and necessitate strong data protection measures.

Considering such potential human rights violations in digital healthcare, the authors felt it necessary to analyse the ethico-legal implications which digitalisation raises for the healthcare system and its stakeholders. This paper explores the critical issues at the intersection of digital healthcare, data protection, and human rights. It examines how the use of digital infrastructure and the collection of sensitive health data can raise ethical concerns about confidentiality, discrimination, and autonomy for the beneficiaries.

The first part of the paper would provide an overview of the recent advancements in digital healthcare. The second part would then analyse the human rights concerns and corresponding legal measures associated with this area. The final part would propose recommendations to navigate such concerns, emphasizing the importance of human rights-based approaches to develop and implement digital health technologies.

Keywords: *Digital Healthcare, Data Protection, Human Rights, Ethics, Regulation*

1. Introduction

Digital healthcare has become an increasingly significant phenomenon in today's digital age. This transformation has resulted

* Professor, Department of Law, Savitribai Phule Pune University, Maharashtra, India. email: jyotibhakare@gmail.com

ǂ Department of Law, Savitribai Phule Pune University, Maharashtra, India.

from efforts to meet the Sustainable Development Goal 3 and improve health infrastructure and health outcomes. The World Health Organization (WHO) has defined digital health as "the field of knowledge and practice associated with the development and use of digital technologies to improve health."[1] Advanced medical technologies and digital communication are being adopted in healthcare systems around the world. During the Covid-19 pandemic, the adoption of technology innovations in the system transformed the way in which the patients could be able to access healthcare. Emerging technologies such as artificial intelligence (AI), machine learning, Blockchain, Internet of Things (IoT), Internet of Medical Things (IoMT), and Big Data analytics have aided in transforming the digital healthcare market. The digital health market in India is predicted to grow at the rate of 20.40% from 2023 to 2027, resulting in a market volume of 25.64 billion dollars by 2027.[2]

Technologies such as artificial intelligence, telemedicine can have a disruptive impact on the delivery of healthcare. They enable patients to actively participate in their treatment, and collaborate on decision making with their physicians. A survey (2024) found that such technologies provide patients with a better sense of control over their health management, since these provide personalized experiences.[3] Medical data, electronic health records form the basis for healthcare data analytics. Healthcare can be of value if it produces better health outcomes for the patients. The development of such health outcomes depends on the health literacy level of the patients. They have to be

---

[1] World Health Organization, *Global Strategy on Digital Health* (2021) *available at:* https://iris.who.int/bitstream/handle/10665/344249/9789240020924-eng.pdf?sequence=1. (last visited on April 5, 2025).

[2] CIO News, 'Digital healthcare platform Nirvasa surpasses Rs 100 Cr ARR' (3 August 2023) *available at:* https://cionews.co.in/digital-healthcare-firm-nirvasa-surpasses-100-cr-arr/ (lasted visited on June 15, 2024).

[3] EY Health Pulse Survey: Health payers report that digital healthcare tech investments are showing promise for members, PR Newswire (17 June 2024) *available at:* https://www.prnewswire.com/news-releases/ey-health-pulse-survey-health-payers-report-that-digital-health-care-tech-investments-are-showing-promise-for-members-302171117.html (last visited on June 24, 2024).

safely integrated into healthcare, in order to monitor their impact on data protection and healthcare disparities.

Health disparities are the disadvantages which certain populations face in their opportunities to achieve ideal health. They are caused by health inequities, or the unjust social positions held by different communities. These inequities are a result of social determinants of health ('SDOH'), or the factors which affect the life of people, such as their housing, education, income, exposure to pollution, etc., and which are distributed unequally among communities. The concepts of human rights, distributive justice are a part of the framework to reduce health disparities. Considering fairness in healthcare access when creating digital health tools can ensure that they are designed and built in a way that benefits everyone equally. The paper has sought to shed light on the impact of such digitalisation of healthcare on human rights.

2. Developments in Digital Healthcare in India

India has adopted many national and state level policies to improve access to healthcare. In India, the Ayushman Bharat Pradhan Mantri Jan Arogya Yojana ('ABPM-JAY') was launched in 2018, as a step towards achieving Universal Health Coverage ('UHC') for all segments of the population by the year 2030. This means that all people should be able to access quality health services without financial burden.[4] Recently, Union Minister of Health and Family Welfare Jagat Prakash Nadda advised the officials of National Health Authority to use smart technology tools to connect directly with beneficiaries regarding their healthcare experience.[5]

India still ranks low on effective UHC coverage on the UHC service index, due to its socio-economic and geographical inequities. A study

---

[4] 'Concept Note on Roadmap for Universal Health Coverage in India: Arogya Manthan 2022' (Ministry of Health and Family Welfare, 2022) *available at:* https://abdm.gov.in/static/media/Session%201%20Note%20-%20Universal%20Health%20Coverage.da4d39535a6227916c18.pdf (last visited on July 17, 2024).

[5] 'Health Minister Nadda reviews Ayushman Bharat PMJAY and Ayushman Bharat Digital Mission', INDIAN PHARMA POST, July 14, 2024, *available at*: https://www.indianpharmapost.com/policy/health-minister-nadda-reviews-ayushman-bharat-pmjay-and-ayushman-bharat-digital-mission-15875 (last visited July on 16, 2024).

reported that failure to record public and private participation in the funding and delivery of healthcare was considered to be a hurdle in India's UHC. It recommended the use of digital technologies as a strategy to address inefficient resource allocation by adopting a nationally linked health record system across states, between public and private sectors, and throughout different levels of care. However, this could raise issues of inequitable access to technologies for disadvantaged communities.[6] The Union Budget (July 2024) has increased expenditure for the National Health Mission (NHM) from Rs 31,550 crore to Rs 36,000 crore for the year 2024-25.[7]

During the COVID-19 pandemic, digital health innovations such as telemedicine were rapidly implemented across the healthcare system in India. In 2021, the National Health Authority ('NHA') of the Government of India, launched a digital health program, Ayushman Bharat Digital Mission ('ABDM'), to integrate digital health records of patients and to enable telemedicine. The National Medical Commission has directed all hospitals attached to medical colleges to make ABHA digital accounts mandatory for patients, as a prerequisite for availing OPD/IPD/emergency services.[8] At present, over 3 crore tokens have been generated for out-patient department registrations, especially in government hospitals, through the Ayushman Bharat Health Account ('ABHA') service.[9]

---

[6] Anuska Kalita, Noah Carton-Rossen, Linju Joseph, Deepshikha Chhetri & Vikram Patel, 'The Barriers to Universal Health Coverage in India and the Strategies to Address Them: A Key Informant Study' (2023) 89(1) *Annals of Global Health* 1.

[7] Sarkaritel, 'Budget increases expenditure for National Health Mission, proposes digital public infra' (24 July 2024) *available at:* https://www.sarkaritel.com/budget-increases-expenditure-for-national-health-mission-proposes-digital-public-infra/ accessed 22 May 2025.

[8] Priyanka Sharma, 'Medical education regulator tells med schools to mandate ABHA IDs for patients', Mint (6 June 2024) *available at:* https://www.livemint.com/news/india/medical-education-regulator-tells-med-schools-to-mandate-abha-ids-for-patients-11717651323182.html accessed 7 June 2024.

[9] 'ABHA's Scan and Share Service Facilitates 3 Crore OPD Registrations Nationwide' (Ministry of Health and Family Welfare, 2024) *available at:* https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2023289 accessed 8 June 2024.

The Digital Health Incentive Scheme ('DHIS') of the Government seeks to pay Rs 20 to healthcare facilities such as hospitals, diagnostic labs, pharmacies, and to digital solution companies ('DSCs') which create digital health records, for every record they digitise and link to the ABHA account, above the threshold of 100 transactions per month, in order to reimburse the costs associated with digitizing of facilities.[10] Further, the Health Ministry is now planning to repurpose Co-WIN, India's Covid vaccination portal, into U-WIN, a national vaccination portal, to register and link records of pregnant women, delivery outcomes, vaccination and immunisation status.[11]

3. Human Rights Concerns and Regulatory Governance

3.1 Human Rights Concerns

Safeguarding health data is essential to protect fundamental rights like privacy, autonomy, and non-discrimination. Misuse of health information can lead to stigmatization, discrimination, and even physical harm. Strong data protection measures can empower individuals by giving them control over their health information, fostering trust in healthcare systems, and enabling advancements in public health without compromising individual rights.

(a) Confidentiality and Data breach

Technological innovations in healthcare offer radical possibilities such as remote patient monitoring, personalized medicine, and improved access to care. However, they also involve the inherent collection of vast amounts of sensitive health data. It is a breach of security that results in destruction, loss, alteration, disclosure of or access to personal data. Health systems must invest in information

[10] 'Digital Health Incentive Scheme' (NammaKPSC, 17 June 2024) *available at:* <https://nammakpsc.com/affairs/digital-health-incentive-scheme/> accessed 19 June 2024.

[11] Sarasvati NT, 'From Co-WIN to U-WIN: Indian Govt Plans to Digitise Immunisation Programme Amid Unaddressed Privacy Risks to Health Data' (MediaNama, 30 May 2024) *available at:* <https://www.medianama.com/2024/05/223-cowin-uwin-indian-govt-digitise-immunisation-programme-privacy-risks/> accessed 2 June 2024.

security and data protection, but not all health systems may have the resources for the same.[12]

10 Bed ICU, a public-private collaboration that seeks to set up ICUs in India's rural government hospitals, has developed AI tools to transcribe doctor-patient interactions into electronic medical records. However, the organization has not specified what kind of personally identifying information of citizens it will exclude while developing its products.[13] In 2023, a healthcare system server breach at the Indian Council of Medical Research gave unauthorised access to data of about 81 crore vaccinated citizens, which enabled the hackers to auction it. While India's digital public goods are accessible to the public and private collaborators, the government must be kept accountable for any security breaches.[14]

Digital public health surveillance can identify real time data and trends, in order to find methods of intervention. In this case, informed consent must be taken for data which is not sourced from medical institutions, such as from online platforms, and which presents personal attributes. Such use of non-health data in algorithms may misattribute stigma to certain groups or behavior, and may affect public trust.[15]

(b) Function Creep and Commercialization

Patients' health data should be collected and used for limited purposes, with their informed consent. When data collected for a

---

[12] Nina Sun, K. Esom, M. Dhaliwal & Joseph Amon, 'Human Rights and Digital Health Technologies', (2020) 22(2) *Health and Human Rights* 1, *available at:* <https://www.jstor.org/stable/27039994> accessed 5 June 2024.

[13] Vallari Sanzgiri, '10BedICU Leverages OpenAI's API, Creates AI Tools for Medical record entry', MediaNama, June 7, 2024, *available at:* https://www.medianama.com/2024/06/223-10bedicu-openais-api-creates-ai-tools-medical/ (last visited June 10, 2024).

[14] 'Thieves & servers' Times of India (2 November 2023) *available at:* <https://timesofindia.indiatimes.com/blogs/toi-editorials/thieves-servers-healthcare-data-taken-out-of-icmr-points-to-gaps-in-digital-architecture-risk-of-wide-exemptions-for-governments/> accessed 5 June 2024.

[15] Allison E Aiello, Audrey Renson and Paul Zivich, 'Social media- and internet-based disease surveillance for public health' (2020) 41 *Annu Rev Public Health* *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7959655/ accessed 5 June 2024.

specific purpose (for instance, medical information, location, business information) are used for another purpose (for surveillance, commercial purposes), it results in a phenomenon called 'function creep'. This means that systems or technologies process the data to expand beyond the initial scope for which they are deployed. Biometric data collected for digital health purposes could be used for forensics or criminal proceedings, which may affect stigmatized or criminalized groups.[16] This becomes a concern when such secondary use of the data is not communicated to the individual at the time of using their data.

A World Bank study reported that health insurers, being a part of the health data system, can access patient data and can use it to hike their premiums.[17] Devices that make data accessible to both stakeholders and patients may enable third parties to acquire sensitive information.[18]

Developer companies help synthesize patient data for pharmaceutical companies, hospitals. If these companies purchase pharmacy companies, they get access to patient data and may distribute it inappropriately to misuse it for marketing purposes. Social media platforms and pharmaceutical companies can use patient browsing history, age, gender, and locations to find an individual's health issues and market for medicines.[19]

(c) Disparities and Equitable access

---

[16] Nina Sun, K. Esom, M. Dhaliwal & Joseph Amon, 'Human Rights and Digital Health Technologies', (2020) 22(2) *Health and Human Rights* 1, *available at:* <https://www.jstor.org/stable/27039994> accessed 5 June 2024.

[17] 'Thieves & servers' Times of India (2 November 2023) *available at:* <https://timesofindia.indiatimes.com/blogs/toi-editorials/thieves-servers-healthcare-data-taken-out-of-icmr-points-to-gaps-in-digital-architecture-risk-of-wide-exemptions-for-governments/> accessed 5 June 2024.

[18] Bertalan Meskó, Zsófia Drobni, Éva Bényei, Bence Gergely & Zsuzsanna Győrffy, 'Digital Health is a Cultural Transformation of Traditional Healthcare' (2017) 3(38) Mhealth, *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5682364/ (last visited on June 6, 2024.

[19] Varsha Chiruvella & Achuta Kumar Guddati, *Ethical Issues in Patient Data Ownership*, 10(2) Interactive Journal of Medical Research (2021). Available at https://doi.org/10.2196/22269

Digital healthcare has the potential to expand access to care, especially in remote areas. But if privacy concerns or data discrimination limit who feels comfortable using these tools, it can actually exacerbate existing health disparities. Apart from minimizing harmful effects, technologies should also maximize benefits for humanity, by improving accuracy, access for marginalized communities.[20]

Digital health technologies may have unintended consequences for socially disadvantaged populations, and may contribute to health disparities. Digital divide refers to the gaps between individuals, communities who cannot access critical technologies, such as smart-phone usage, access to broadband, owing to affordability, digital literacy etc. In healthcare, digital determinants of health, such as digital literacy, healthcare delivery outcomes, infrastructural outcomes, affect healthcare experiences of people. Data solidarity is an approach that emphasizes data justice and equity for those who may be disadvantaged by health data and technology use.[21] Quality digital technologies must be acceptable and be made available to all communities through proper digital infrastructure and digital literacy training.[22]

(d) Discrimination based on Health Information

Health information is personal and can be used to make critical decisions about people's lives. Without strong human rights protections, digital healthcare could lead to discrimination in areas like employment, insurance, or even legal issues. Training AI on biased datasets can create inequities in healthcare software. Because of algorithmic biases in AI, there may be discrimination in criminal procedures or in employment as to which patient shows healthcare risk, all because of inaccurate predictions of health

---

[20] Nina Sun, K. Esom, M. Dhaliwal & Joseph Amon, 'Human Rights and Digital Health Technologies', (2020) 22(2) *Health and Human Rights* 1, *available at:* <https://www.jstor.org/stable/27039994> accessed 5 June 2024.

[21] Katharine Lawrence, 'Digital Health Equity' in Simon Lin Linwood (ed), *Digital Health* (Exon Publications 2022) *available at:* https://www.ncbi.nlm.nih.gov/books/NBK580635/ accessed 24 May 2025.

[22] Nina Sun, K. Esom, M. Dhaliwal & Joseph Amon, 'Human Rights and Digital Health Technologies', (2020) 22(2) *Health and Human Rights* 1, *available at:* <https://www.jstor.org/stable/27039994> accessed 5 June 2024.

outcomes across race, gender, or socio-economic status. Inclusiveness and participation involves developers and government authorities to ensure that end users are engaged in the development of digital technologies, through public feedback, monitoring, and consultation. Businesses should take input, identify and redress any discriminatory outcomes.[23] Medical information may be used to discriminate in a recruitment process or against employees, especially those with disabilities or medical conditions. The use of such data to unlawfully discriminate against a person violates his right to privacy (if consent is not obtained) and the right to be free from discrimination.

(e) Loss of Patient Autonomy

Any personal information collected should be done with fully informed consent. A rights-based approach to informed consent would consider inequalities such as economic status, digital access, and relationships with health care providers so that patients can make decisions regarding the use of their personal data.[24] MNCs who gain access to the databases may use the data for defrauding vulnerable populations or for sharing data with commercial entities. Legal regulation must monitor data exploitation for profit.[25]

The aim of informed consent procedures is to enable autonomous choice by disclosing information about the recommended interventions and to let the patient consent or refuse without any undue influence. However, the patient may also have doubts originating from sources that the doctor may not consider relevant such as internet sources, blogs, and videos. The patient may not have

---

[23] Nina Sun, K. Esom, M. Dhaliwal & Joseph Amon, 'Human Rights and Digital Health Technologies', (2020) 22(2) *Health and Human Rights* 1, *available at:* <https://www.jstor.org/stable/27039994> accessed 5 June 2024.

[24] Deekshitha Ganesan, 'Human Rights Implications of the Digital Revolution in Health Care in India' (2022) 24(1) *Health Hum Rights*. *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9212836/. Accessed on: 5 June 2024.

[25] Vijayaprasad Gopichandran, Parasuraman Ganeshkumar, Sambit Dash & Aarthy Ramasamy, *Ethical Challenges of Digital Health Technologies: Aadhaar, India*, 98(4) BULL. WORLD HEALTH ORGAN. (2020), *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7133485/. Accessed on: 5 June 2024.

the critical skills to determine whether the data available is research-based or personal.

In clinical research, researchers should ensure that participants give adequate informed consent regarding all aspects of use of their information when seeking consent for data extraction. They should also enable continuous involvement and communication between participants and the users of their data.[26]

3.2 Legal framework and Limitations in the Digital Age

Human rights law requires that digital initiatives should comply with the users' rights of privacy, autonomy, and non-discrimination. The legal framework to govern digital health technologies in India is not comprehensive, and increasing developments and business models have resulted in the law becoming ambiguous.

Law must define the legal process specifically for the collection, storage, and use of health data. The present legal framework for data protection is governed by the Information Technology Act, 2000. This Act does not specifically address concerns of data privacy, or health data in particular, but focuses more on information security. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 governs the exchange of information between a patient and his service provider. The Rules includes physical, psychological, and mental health conditions, medical records, and biometric data in the definition of 'Sensitive Personal Data or Information'. They require companies to inform patients of the collection of their data, purpose of use, and any transfer to third parties.

The draft Digital Information Security in Healthcare Bill 2018 ('DISHA') provided for security, privacy, and confidentiality standards for electronic health data. Although it specified 'Digital Health Data' (which is derived from electronic records related to a clinical establishment) and 'Personally Identifiable Information', it separately defined 'Sensitive health-related information' as information that could result in substantial harm to a person's physical or mental

[26] Varsha Chiruvella & Achuta Kumar Guddati, *Ethical Issues in Patient Data Ownership*, 10(2) *Interact J Med Res* (2021), *available at:* https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8178732/#:~:text=The%20increasing%20interest%20of%20for,and%20even%20target%20vulnerable%20populations (last visited June 5, 2024).

health condition, if it is compromised. The Bill did not require 'explicit' consent from the owner of any data concerning health, for its processing. Also, the Bill did not specify third party controllers of health data such as technology developers, who can have access to biomarker data, which can be used commercially. Neither did it address the right of the data subject to be forgotten or the erasure of data.[27]

DISHA was eventually subsumed under the Personal Data Protection Bill 2019, which was re-introduced and enacted as the Digital Personal Data Protection Act 2023. This Act does not specifically address protection of health data, nor does it distinguish between personal data and sensitive personal data. This implies that public and private entities dealing with health data (unless they are designated to be significant data fiduciaries) will not be required to audit their data security practices. Users must be provided data portability, whereby they can reuse their health data for their own purposes across various platforms.[28] The entity is also required to have a privacy policy and reasonable security practices in place alongside additional compliances such as adopting privacy by design, maintenance of records, auditing etc. Data protection becomes a challenge when such data is being collected on a real-time basis. With the advent of a new digital public infrastructure in India, the use of health data and control of data flow should be regulated.

Institutions and agencies that are not mandated to access health data must not be enabled to do so. There has to be a check on how health related applications comply with legislation requirements for encryption, privacy, data security measures. Their terms and conditions of use must be scrutinized, so as to ensure that these are

---

[27] Vanshika Arora, 'Protection of User Healthcare Data in India Vis-a-Vis the DISHA Bill: Substantive Takeaways from GDPR' (*NUALS Law Journal,* 1 October 2022) *available at:* <https://nualslawjournal.com/2022/10/01/protection-of-user-healthcare-data-in-india-vis-a-vis-the-disha-bill-substantive-takeaways-from-gdpr/> accessed 14 June 2024.

[28] Shivangi Rai & Shefali Malhotra, 'India is piloting ambitious digital health initiatives while neglecting data safeguards' (31 October 2023) *available at:* https://amp.scroll.in/article/1057716/india-is-piloting-ambitious-digital-health-initiatives-while-neglecting-data-safeguard (lasted vistied on June 04, 2024).

inclusive and do not violate the rights of users. The design management practices of applications should not compromise user safety. Data usage policies should be transparent and clearly presented, which aligns with the informed consent approach.[29]
Data collection applications for medical data should comply with Good Clinical Practices (GCP) as issued by the NMC. The data collection tools ought to protect the data subjects' rights of integrity and confidentiality. Providing users access to their data can also enable them to check whether advertising companies use their data. Government digital health policy initiatives like the NDHB should aim to have maximum reach to all beneficiaries, to address their needs, to find resources and provide a solution to their problems, all after planning for financial coverage, budgeting, strategising and consulting all stakeholders.

Conclusion

A robust human rights framework which is implemented in legislation will be effective to navigate the ethical complexities of digital healthcare. The regulatory framework must specifically target the risks and shortcomings of healthcare technologies, to protect sensitive information, and to promote transparency and patient control over health data. Developers and government authorities should ensure that the end users are engaged in the development of digital technologies, through public feedback, monitoring, and consultation. Effective non-digital options should be accessible to all as an alternative to digital healthcare technologies.
If human rights norms and standards based on ethical principles are implemented into laws, they can improve enforceability and accountability. According to the WHO, digital healthcare should benefit people in a way that is ethical, secure, equitable and reliable. This is possible if development of such technologies is carried out with transparency, accessibility, interoperability, privacy, security and confidentiality. To achieve these, ethical frameworks, such as the Trustworthy and Ethical Assurance of Digital Healthcare (created by

[29] Jitamanyu Sahoo & Mujtaba Hussain, 'Bridging the Digital Divide: Ensuring Health Apps Uphold Health Rights', Rising Kashmir, July 3, 2024, *available at*: https://risingkashmir.com/bridging-the-digital-divide-ensuring-health-apps-uphold-health-rights/ (last visited July 5, 2024).

the University of York and the Alan Turing Institute) can offer guidance on how ethical principles can be applied to handle specific risks and benefits of digital technologies. Closing the gap in health equity requires further research on the impact of digital health technology. This research can guide the development of strategies to ensure everyone benefits from these tools.