ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

PRESERVING PRIVACY: A CORNERSTONE FOR ACHIEVING UNIVERSAL HEALTH COVERAGE IN INDIA'S DIGITAL ERA

Niharika Raizada[1*] and Prof. (Dr.) Mamata Biswal[2]
[1]Research Scholar and Gujarat National Law University, Gandhinagar, Gujarat
[1]niharikaphd202030@gnlu.ac.in and [2]mbiswal@gnlu.ac.in

ABSTRACT
This article aims to assess the dynamic landscape of digital health systems in India, with a particular focus on the Ayushman Bharat Digital Mission. The analysis conducted in this piece not only delves into the ongoing discourse surrounding health data privacy and security but also underscores the pivotal role privacy plays in attaining Universal Health Coverage (UHC), a sustainable development goal slated for accomplishment by 2030. The core of the article introduces and expounds upon India's evolving digital health systems, centering on the Ayushman Bharat Digital Mission. It elucidates how these systems play a crucial role in realizing universal healthcare objectives, emphasizing the twin pillars of affordability and accessibility to healthcare services. The comprehensive digital health system's operational facets are detailed, shedding light on its integral components, while acknowledging the inherent challenges associated with safeguarding privacy. Integral to the discussion are the major legislations governing health data in India, which the authors critically analyze within the context of the regulatory and legal framework. This scrutiny is conducted through the lens of privacy concerns surrounding health data. The article takes into account the nuanced complexities of data protection in the health sector and highlights the need for a robust legal and regulatory framework to ensure the secure handling of digital health information. Upon a meticulous examination of the existing literature, the authors arrive at a compelling conclusion. They emphasize that beyond the imperative of physical infrastructure development and the digitization of health systems, ensuring the protection of digital data stands as a paramount requirement for the realization of Universal Health Coverage. The article accentuates that striking a balance between technological advancement and robust privacy measures is indispensable for achieving comprehensive and equitable healthcare access across the nation.

Keywords: National digital health mission, Ayushman Bharat digital mission, Universal health Coverage, electronic health records, privacy.

1. INTRODUCTION
The term “digital health” is characterized by the World Health Organization (WHO) as a comprehensive concept that encompasses eHealth, including mHealth, along with emerging fields like the utilization of advanced computing sciences in “big data,” genomics, and artificial intelligence[1]. Over time, the definition of digital health has expanded to encompass many digital technologies used for remote consultations, and electronic record-keeping, including telemedicine, digital health records, clinical decision support systems (CDSS), and web-based health services. Digital health services have played a crucial role in enhancing support for different services like successful cancer screening, managing post-treatment symptoms, and facilitating communication between patients and healthcare providers. Undoubtedly, medical sciences have made commendable progress in treating terminal diseases like cancer, but the case is not similar in low and medium income countries like India. India, although made considerable growth in medical field but a large segment of the population remains underserved and untreated. Digital health systems offer numerous benefits in healthcare. Firstly, they improve access to healthcare services, especially for individuals in hard-to-reach areas[2]. This is particularly important in ensuring that everyone has equal opportunities to receive necessary medical care. Additionally, digital health technologies enhance the safety and quality of healthcare services and products. By utilizing digital tools, healthcare providers can streamline processes, reduce errors, and improve patient outcomes. Moreover, digital health systems provide better knowledge and access to health information for healthcare workers and communities, leading to increased productivity and improved decision-making. These technologies also facilitate the rapid transmission of public

health information, enabling timely decision-making and monitoring of program performance. They improve quality of research studies, protect patient privacy and confidentiality and possess the capability to change the delivery of healthcare services[3]. However, data privacy and security of health information is an integral part of universal health coverage. Significant benefits related to data privacy and security follow adoption of digital health system. However, the rapid adoption of digital health services and big data, it is extremely difficult to achieve universal health coverage and preserve privacy simultaneously. The article explains functioning of newly developed digital framework in India, Ayushman Bharat Digital Mission and analyzes relevant provisions of the corresponding policies and laws. Furthermore, the why preserving privacy is of utmost significance to achieve universal health coverage, particularly in India.

2. DIGITAL HEALTH AND UNIVERSAL HEALTH COVERAGE

Digital health systems have revolutionized the healthcare industry, enabling individuals to have access to quality healthcare services and promote universal health coverage. In today's interconnected world, the adoption of digital health systems has emerged as a catalyst for ensuring that everyone has access to affordable and effective healthcare.

Ayushman Bharat Digital Mission (ABDM) is a digital health program launched as a part of an overarching initiative, Ayushman Bharat Mission (ABM), formulated by Government of India in 2018. Ayushman Bharat Mission aimed to provide two major components[4]:

a. Establishment of 1,50,000 health and wellness centers by 2022 at primary level of health system which substitutes primary centers and sub-centers.

b. To evaluate the implementation of National Protection Health Scheme providing government- funded insurance cover of Rs. 5,00,000 to Socio-Economic and Caste C census.

The ABM aims to further the progress towards attainment of Universal Health Coverage by 2030 as a part of Sustainable Development Goals (SDGs)[5]. In India, universal health coverage finds its roots in National Health Policy, 2017 under clause 2.3.1. Universal health coverage signifies equitable access to every citizen of the country irrespective of their caste, gender, status, religion, place of residence, etc. to affordable and accessible quality of health care services. Subsequently after National Health Policy, 2017 the Government of India determined the need of establishing a comprehensive digital system for healthcare service delivery. With the consultation of NITI Aayog, National Health Stack[3] was published in 2018, delineating the significance and functioning of building blocks constituting the health stack. Based on the recommendatory document by NITI Aayog, National Digital Health Blueprint (NHDB)[6] was developed which enables interoperability in digital health system. Subsequently in 2020, National Digital Health Mission was established as an entity for proper implementation of NHDB. The Blueprint provides for governing structure of NDHM and its development to National Digital Health Authority. Subsequently, NDHM was implemented as Ayushman Bharat Digital Mission (ABDM) in 2021[7] in six union territories as pilot project and later launched in whole country in 2022. ABDM provides for necessary building elements for digital health infrastructure.

One of the primary concerns of the ABM was ensuring that benefits of the scheme was received by beneficiaries and healthcare facilities is accessible to everyone. Following this concern and the outbreak of COVID-19, the need for establishment of comprehensive digital system for delivery of healthcare facilities was realized. ABDM is based on Model of India Stack known as National Health Stack published by NITI Aayog in 2018, which proposed federated health information model. ABDM is a federated health information repository comprising health information of an individual across the different health providers, consisting of medical history, details of prescription, vaccination status, results of laboratory tests, radiology or MRI images, vital signs, stats of an individual like age and weight, demographics and information on the other digital health applications[8]. The ABDM framework not only improves accessibility for patients but also enable them to store their medical records in health locker and provides longitudinal view of their medical history. ABDM is based on building blocks like

ABHA Number, Registries (ABHA Registry, Health Facility Registry and Health Service Provider Registry), Consent Manager and Gateway (HIE-CM) and Unified Health Interface (UHI)[9].

3. PRIVACY CHALLENGES IN THE HEALTH DATA LANDSCAPE

The paradigm shift in the healthcare industry can be observed with the adoption of ABDM framework across the country. More than 23 crores of ABHA numbers (unique health identifiers) have been created by July 2022 in India. In ABDM, a centralized database is created using ABHA numbers of the registrants. It also enables them to link their personal health records like medical prescriptions, consultations with medical practitioners, X-Ray, MRI scans, etc. altogether for the ease and convenience of the registered people. It is important to understand that storing sensitive data in a centralized and one single database makes it susceptible to data breach and other forms of risks against confidentiality, availability and integrity of information stored. Data breach at Indian Council for Medical Research, CoWIN data breach and ransomware attack on All India Institute of Medical Sciences, New Delhi are few examples demonstrating the urgency for preserving privacy of medical information. The inevitability of privacy and security threats against the health data stored in different information systems cannot be refuted. As much as significant is attainment of Universal Health Coverage, so is ensuring of privacy and security of medical data. De-identification is a one of the methods used to camouflage some parts of health data. There are other techniques such as privacy by design, data augmentation, cryptography, end-to-end encryption etc. incorporated to ensure that sensitive health information is secure.

Working of AI algorithms based on big data is not a mystery anymore and re-identification of aggregated health data is not irreversible now. In the age of big data and AI, misuse is a more likely consequence of medical data in absence of adequate measures and mechanisms to preserve and protect such information. Keeping this in mind, the most important element of universal healthcare, “health for all” will apparently not be achievable on account of several reasons like stigmatization and discrimination[10]. For the sake of determining the gravity of the problem and the anticipated effect of a data breach on the owners of data, it would not wrong to assume that health information of an individual is not only extremely sensitive but rather personal in nature as well. There is an existing risk in utilizing data for purposes different from its intended use. Reference can be placed on the Google-NHS incident where health information collected by the hospitals was shared with Google with the objective of developing new AI Technology. Acquiring and using of data in such manner might lead to illegal or dubious use of such data[11]. In some instances, as a consequence of such illegal use of data, might lead to exclusion of several members of protected classes as desirable candidates and later condemns certain groups in entirety or composed of members of protected classes to less favorable management and treatment[12].

For instance, if the information relating to an individual’s sexuality or information about a person suffering from HIV/AIDS or any other such disease is disclosed without the individual’s explicit consent, the same will not just be a reason of embarrassment but may also adversely affect the possibilities of being employed, or risk of being discriminated. Such consequence will also adversely affect everyone in a group instead of just those people who have consented to share their medical information. Therefore, to achieve Universal Health Coverage, ensuring privacy is significant.

4. REGULATION AND HANDLING OF HEALTH DATA

Ayushman Bharat Digital Mission enforces an interoperable infrastructure and regulates exchange of data between health information providers, patient and health information users. Health information providers are doctors and/or diagnostic laboratories, which generate medical reports, health information users are the medical practitioners who require viewing the medical records of the patient after obtaining consent from the patient[13]. There are certain building blocks of ABDM required to coordinate to uphold efficient functioning of digital health system. They are:

a. **Health ID**- Health ID is a unique set of alphanumeric characters provided to registrant upon registration as a patient with ABDM. It can be obtained via registering at any nearest health service provider registered with

ABDM, or through any Personal Health Records application (like DocPrime, PayTM, etc.) or registering himself or herself through official website.

b. Health Lockers- These are software service providers who provide for longitudinal storage of medical records of registered individuals. They act like HIUs when they are on the receiving end of medical records transaction and act as HIPs when the user of health locker shares his records from the same.

c. Consent Manager & Gateway- Interoperability of health information is ensured by consent manager and gateway. Consent manager is responsible for permitting, denying or revoking requests for accessing medical records by any individual.

d. DigiDoctor- DigiDoctor is a national directory of all the medical practitioners and facilitates their participation in the digital health ecosystem by permitting them to eSign prescriptions, summaries for discharge of patients, notes, etc. Registration of doctors with DigiDoctor participating in ABDM is mandatory.

e. Health Facilities Registry (HFR)

HFR is national directory of all healthcare facilities. Every healthcare facility interested in participation in ABDM is required to register as HFR at the official website. Registration of the same ensures that they are properly authorized to provide health records to patients.

4.1. Entities under ABDM

a. Health Information User (HIU) - Health information user is an entity requesting access of health records of individual.

b. Health Information Provider (HIP) - Health information provider is an entity which creates health information with respect to providing services to patients related to healthcare and assents to agree the same digitally with patient's consent.

c. Health Repository Provider (HRP) - HRP are software service providers which enable long-term storage of personal health records for healthcare service providers like hospitals, diagnostic centers, etc. HRP permits different HIPs and HIUs to securely share and maintain health records digitally. HRPs offer longitudinal storage and maintenance of health records of HIPs.

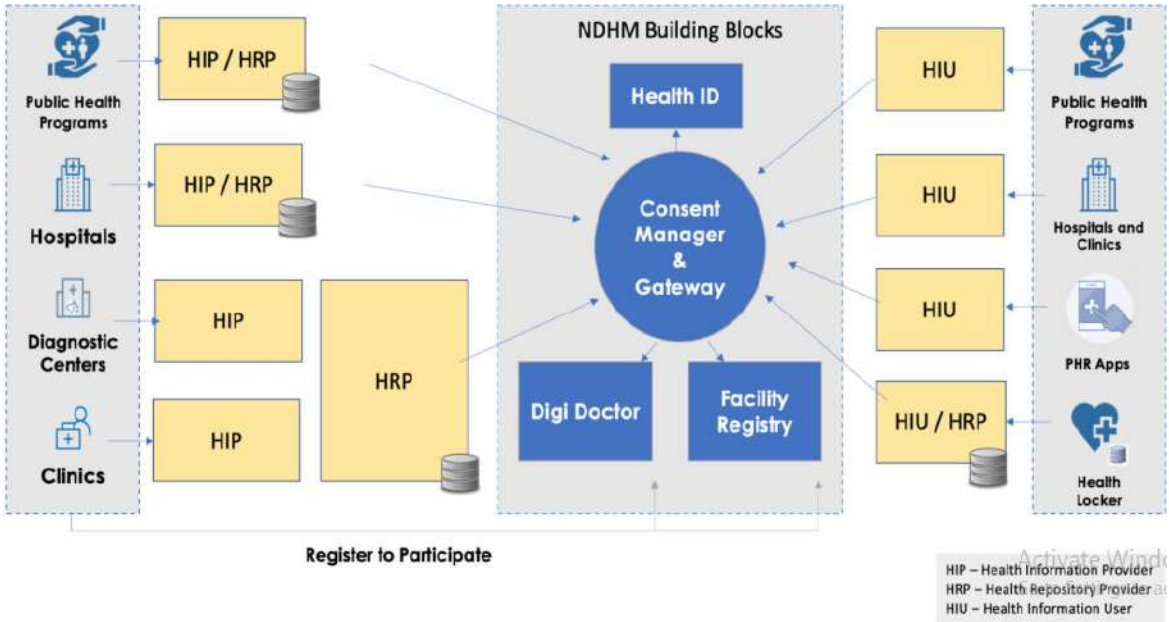

Fig. 1 Working of Ayushman Bharat Digital Mission

The data is exchanged through consent manager (HIE-CM), which is one of the essential building blocks of ABDM infrastructure. HIE-CM is a gateway, which enables sharing of information linked to ABHA account of the individual, from HIP to HIU, upon receiving consent.

4.2. Regulatory Frameworks and Laws in India

Currently The Digital Data Protection Act, 2023 and Information Technology Act, 2000 are the major legislations governing data privacy and protection in India. However, Ayushman Bharat Digital Mission provides for corresponding policies like Health Data Management Policy, Data Retention Policy, Health Information Provider and Health Information User Policy for the holistic governance of the framework. It is here important to take into consideration that these policies are regulatory and not obligatory in nature. The laws and policies will be discussed in relation to privacy of health information.

4.2.1. Health Data Management Policy

Storing, sharing and interoperability of data is governed through Health Data Management Policy 2.0[14] (HDMP) and is a significant step towards ensuring 'security and privacy by design' for preserving patients' personal and sensitive data. This policy upholds the importance of data protection and acts as the guiding document with minimum standards for an optimal-cum-advanced National Digital Health Ecosystem. HDMP is the guiding document and acts as the minimum standard for data privacy. The policy is based on principles of federated architecture, which enables interoperability between different stakeholders of ABDM and decentralized information systems. HDMP provides for seven different privacy principles under Art 26 of "Chapter V: Accountability, Transparency, Privacy by Design, Consent and choice based sharing, limitation on data retention, empowering data principal, enhancing data quality and reasonable practices.[14]" Art. 26 obligates data fiduciaries to ensure that these principles are complied. Besides the HDMP 2.0, there are other legislations, which obligate data fiduciaries to protect sensitive and personal data.

4.2.2. Information Technology Act, 2000

Information Technology Act, 2000 is a comprehensive legislation focused on governance of several different electronic transactions and interchange electronic data. The Act came into force on June 9, 2000 and specified in its Preamble "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as ―electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies[15]" IT Act provides for several offences[16] under Chapter IX however, the Act does not specifically deal with data breach or cyber-attack. The Act however provides for compensation on part of the body corporate on account of failure to protect sensitive data from being stolen or unlawfully accessed. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011is one of the corresponding rules which aim at explicit protection of sensitive personal data and information and these Rules are supposed to be read with section 43A.

Rule 3 of the IT Rules, 2011[17] defines Sensitive Personal Data and information comprising of information relating to:

i. "password;
ii. financial information such as Bank account or credit card or debit card or
iii. other payment instrument details;
iv. physical, physiological and mental health condition;
v. sexual orientation;
vi. medical records and history;
vii. Biometric information;

viii. any detail relating to the above clauses as provided to body corporate for providing service; and

ix. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise."

The Rules although provide for umbrella provisions for protection of sensitive data and information but it does not provide for specific provisions and classification of health and medical data and as to what kinds of data constitute as health data. Furthermore, the Rules have major application over body corporate only and not on other organizations or individuals. Consequently, there won't be any imposition of compensation on individuals or other organizations which are not within the ambit of 'body corporate'.

4.2.3. Electronic Health Records Standards, 2016

Electronic Health Records Standards, 2016 (EHR Standards, 2016) provides for extensive standards which specifically apply on healthcare institutions or anybody which lead to creation of medical history and record. In a way, EHR Standards, 2016 fill the gaps with respect to terminologies, protection, and prevention from unlawful access and in relation to health data primarily. The Standards specify International Standards for not only protection of sensitive data but also focuses upon maintenance, sharing or enhance interoperability of electronic health records as well. In addition to this, the Standards also lay down guidelines with respect to network connectivity, interoperability and data ownership as well. Most importantly, they also define and differentiate in an elaborate manner between 'Electronic Health Record (EHR)', 'Electronic Medical Records' (EMR), Electronic Personal Health Information' and 'Personal Health Record' (EPR)[18].

a. Electronic Health Record

EHR has been defined as "one or more repositories of information in computer processable form, relevant to the wellness, health and healthcare of an individual, capable of being stored and communicated securely and of being accessible by multiple authorized users, represented according to a standardized or commonly agreed logical information model."[19]

b. Electronic Medical Record

EMR has been defined as a varied form of EHR ", restricted in scope to the medical domain or at least very much medically focused".

c. Electronic Personal Health Information

E-PHI has been defined as any protected health information which has been 'created, stored, transmitted, or received electronically'. The data created, recorded, sent, transmitted or received through any electronic medium is covered under this term.

d. Personal Health Record

A PHR has been defined as documentation of any form of patient information including medical history, vaccinations or even medicines prescribed and purchased.

The EHR Standards, 2016 is though a comprehensive document but lacks enforceable character due to unavailability of such provision. Subsequently, due to lack of enforceability, the application and the norms so provided within the same, act as mere recommendations or guidelines for health service providers and hence there is no imposition of penalty or fine on lack of implementation of such standards by the service providers.

4.2.4. Digital Personal Data Protection Act, 2023

The Act lays down "for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health"[20]. In addition to this, the Act also provides for penalties specified under Schedule I to be imposed on data fiduciaries because of failure to comply with obligations stated in section 8 and section 10 of the Act. However, it is important to note that relevant provisions of the Act do not provide for privacy, security and confidentiality of health data specifically and most importantly, it does not define sensitive personal data and differentiate between sensitive and non-sensitive personal data. Consequently, there are no provisions for regulation of the same.

5. COMMITTING TO UNIVERSAL HEALTH COVERAGE AND PRIVACY TOGETHER

It is noteworthy that HDMP although provides for an extensive governance of storage and exchange of health data across the ABDM architecture, but the said policy does not possess *ex ante* character unlike European Union's General Data Protection Regulation or U.S. Health Information Privacy and Accountability Act. As comprehensive as HDMP is, the policy will enhance data privacy and security of health data across all the electronic registries associated with ABDM, if it is enacted on similar lines as other data privacy laws in the country. Furthermore, ABDM is mentioned as a mere framework, and enables voluntary adoption on the part of private or even government entities; thereby rendering the resilient efforts made towards management and preservation of privacy of health information as inadequate. It is important to ensure that stakeholders in the in a federated architecture are obligated to incorporate certain measures. Some of these include, mandating audits (both internal and external) of Information Security Management Systems as under ISO/IEC 27000 family, and other relevant international standards like NIST Framework Version 1.1, anonymization of information in accordance with the relevant anonymity standards, utilization of blockchain technology, determining the liability of third-party service providers, etc.

Furthermore, it is significant to consider ABDM is a complex digital ecosystem involving front-line workers and other stakeholders. It is important to understand all the skills and knowledge essential to utilize the technology and ensure that it is easier and convenient for users to navigate and use the services rendered through ABDM such as telemedicine. Education and training here plays an important role. Privacy and security of health information is a significant subject about which both healthcare service providers and patients should be educated separately and equally. Awareness and education help mitigate the risks around health information by explaining the actions taken to protect patient data and informing them about their rights and duties while availing services from healthcare service providers in the digital ecosystem.

ABDM has the potential to transform the healthcare delivery system and ascertain high quality and affordable healthcare services to everyone, elements underscoring Universal Health Coverage, is delivered. Incorporation of every single measure to avoid a data breach will still not guarantee the absolute safety of data but such efforts and measures will reduce the probability of unauthorized disclosure of health information. Subsequently, it will also aid in universalizing healthcare. Promotion of inclusive healthcare through digital means is not the only prong for achieving Universal Health Coverage but ensuring that such health information is inaccessible and confidential to tackle discrimination also holds equal significance.

REFERENCES

[1] Doolan M, 'Using Technology to Support Collaborative Learning Through Assessment Design' (2011) <https://www.semanticscholar.org/paper/Using-Technology-to-Support-Collaborative-Learning-Doolan/5d3baa50c707ea764420501561c9201c86c19f5d> accessed 15 September 2023

[2] Biggs JS and others, 'Digital Health Benefits Evaluation Frameworks: Building the Evidence to Support Australia's National Digital Health Strategy' (2019) 210 Medical Journal of Australia <https://onlinelibrary.wiley.com/doi/abs/10.5694/mja2.50034> accessed 26 September 2023

[3] Ibid

[4] Budd J and others, 'Digital Technologies in the Public-Health Response to COVID-19' (2020) 26 Nature Medicine 1183 <https://www.nature.com/articles/s41591-020-1011-4> accessed 26 September 2023

[5] National Health Authority, "Ayushman Bharat Comprehensive Primary Health Care through Health and Wellness Centers - Operational Guidelines", (2018)

[6] Lahariya C. 'Ayushman bharat' program and universal health coverage in india. Indian Pediatr [Internet]. 2018 Jun [cited 2024 Feb 1];55(6):495–506. Available from: http://link.springer.com/10.1007/s13312-018-1341-1

[7] Kant A, Paul K V. National Health Stack Strategy and Approach [Internet]. NITI Aayog; 2018. Available from: http://abdm.gov.in:8081/uploads/NHS_Strategy_and_Approach_1_89e2dd8f87.pdf

[8] Satyanarayana J. National Digital Health Blueprint [Internet]. New Delhi: Ministry of Health and Family Welfare; 2018. Available from: https://abdm.gov.in:8081/uploads/ndhb_1_56ec695bc8.pdf

[9] Dastidar BG, Suri S, Nagaraja VH, Jani A. A virtual bridge to universal healthcare in india. Commun Med [Internet]. 2022 Nov 16 [cited 2024 Feb 2];2(1):145. Available from: https://www.nature.com/articles/s43856-022-00211-7

[10] Ram TS. Ayush grid: Digital health platform. International Journal of Ayurveda Research [Internet]. 2023 Jun [cited 2024 Feb 2];4(2):61. Available from: https://journals.lww.com/ijar/fulltext/2023/04000/ayush_grid__digital_health_platform.2.aspx

[11] Rai S, Malhotra S, Divan V. Digital technology, health & the law implications for universal health coverage. Centre for Health Equity, Law and Policy (C-HELP)2023 [cited 2024 Feb 2]; Available from: https://www.ssrn.com/abstract=4501893; Shrivastava, Swapnil, and T K Srikanth. 'A Framework for Secure and Privacy Preserving Health Data Exchange across Health Information Systems Using a Digital Identity System'. In 15th International Conference on Theory and Practice of Electronic Governance, 41–49. Guimarães Portugal: ACM, 2022. https://doi.org/10.1145/3560107.3560115.s

[12] Véliz C, 'Medical Privacy and Big Data: A Further Reason in Favour of Public Universal Healthcare Coverage' in Thana C de Campos, Jonathan Herring and Andelka M Phillips (eds), Philosophical Foundations of Medical Law (Oxford University Press 2019) (http://www.ncbi.nlm.nih.gov/books/NBK550264/)

[13] NHA | Official website Ayushman Bharat Digital Mission. [Cited 2024 Feb 2]. Available from: https://abdm.gov.in/abdm

[14] Jain A. NHA releases new and revised health data management policy, MediaNama. 2022 [cited 2024 Feb 2]. Available from: https://www.medianama.com/2022/06/223-new-health-data-management-policy/

[15] Information Technology Act, 2000, Act No. 21 OF 2000 Jun 9, 2000. Available from: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[16] Information Technology Act, 2000, Act No. 21 OF 2000. Sect. 45 Jun 9, 2000. Available from: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[17] Information Technology Act, 2000, Act 21 of 2000. Sect. 43A - Explanation June 9, 2000. Available from: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

[18] Arora J. Electronic Health Records Standards for India, Q-11011/3/2015 –eGov, Glossary Dec 30, 2016 p. 33. Available from: https://main.mohfw.gov.in/sites/default/files/EMREHR_Standards_for_India_as_notified_by_MOHFW_2016_0.pdf

[19] Ibid

ABOUT THE AUTHORS

Niharika Raizada: Niharika Raizada is currently enrolled as a Ph.D. candidate at Gujarat National Law University, Gandhinagar, Gujarat. Her area of research lies in understanding the intersection between cybersecurity in healthcare infrastructure and law. She has completed her Masters in Criminal Law from Sardar Patel University of Police, Security and Criminal Justice, Jodhpur. Her primary interests lies in criminal law and jurisprudence and data protection and privacy laws.

Prof. (Dr.) Mamata Biswal: Prof. Mamata Biswal is a senior Professor in Gujarat National Law University, Gandhinagar, Gujarat. She has been ICSSR senior research fellow and has extensive research and academic experience in Corporate Law. She is currently a visiting faculty at different reputed institutions.