Privacy And Security Concerns In Electronic Health Records - A Comparative Study Between India And USA

Purvi Nema
& Riya Sinha*

Abstract

With the pandemic hitting hard, the realization that India needs to increase investments and improve healthcare sector in the country is sinking in, each passing day. The induction of Information and Communication Technology (ICT) in healthcare system is revolutionizing the healthcare system across the globe by increasing the availability and accessibility of healthcare to the patients. Electronic Medical Record or Electronic Health Record is a fundamental pre-requisite in using ICT in healthcare. It is a digital record that integrates patients' health data and is used for the purposes of education, research, referral, and management of data. Many developed countries including USA have a well-established system of Electronic Health Records in place. Although with numerous benefits, many concerns are raised regarding the protection of the information and privacy of the individuals as it includes sensitive personal data. The Government have proposed two new legislations namely, the Personal Data Protection Bill, 2018 and the Digital Information Security Healthcare Act, 2018, to tackle the setbacks of current law. The objective of the paper is to discuss the issues related to privacy and security of health data and analyse the lacuna in the existing and proposed legislations in India. Furthermore, the paper provides suggestions for improvement in data protection laws in India and highlights those measures that can be borrowed from the federal legislations related to health privacy in USA (HIPAA, 1996 and HITECH Act, 2009).

Keywords: Electronic Health Records, Health Information Privacy, DISHA, Data Protection Bill, Aarogya Setu

* Law Graduates, NUSRL, Ranchi

I. Introduction

The advancements in technology is revolutionizing the healthcare system across the globe as we experience today. One of the greatest benefits of internet on healthcare is integration of health data of patients into an electronic form that shall be handy, flexible and easy to use and maintain.[1] In May, 2018, the Member States of the World Health Organization met and unanimously approved the World Health Assembly Resolution on Digital Health that recognizes potential contribution of digital technologies in advancement of universal health coverage and the aim of Sustainable Development Goals.[2]

The use of Information Communication Technologies (hereinafter referred as ICTs) in healthcare aims to transform conventional health care data or information system by strengthening collection, exchange and analysis of the data.[3] The significant advancement is the use of Electronic Health Record is a significant advancement in digital healthcare sector, which provides an organized and methodical collection of health data in an electronic form.[4] This collection shall help in creating a life-long health record of an individual that shall help in improving health care of a greater mass at a much lesser cost than the paper records.[5]

The digitization of health data would prove to be an efficient tool in cases of emergency where a medical practitioner can immediately access the health data and learn about the patient's information related to allergies, drug interactions or any pre-existing medical complications. Also, digital healthcare data can be of great help for conducting research and empirical studies.

Undoubtedly, the collection and storage of digital healthcare data is a remarkable step in the healthcare sector. However, it also raises many concerns regarding the breach of security of the

[1]Jodiê Smith & Suresh Sankaranarayana, "Smart Agent-Based Hospital Search, Appointment and Medical Diagnosis" (2012) 3(4) E-Health and Medical Communications <http://www.igi-global.com/article/smart-agent-based-hospital-search/73707> accessed 20 September 2020

[2]World Health Organisation, "WHO Guidelines on Recommendations on Digital Interventions for Health System Strengthening" (2019) <https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1> accessed 20 September 2020

[3] Ajay Goel, "Harnessing ICT in HealthCare Services in India" (*Institute of Public Health*, 21 August 2015) <https://iphindia.org/harnessing-ict-in-health-care-services-in-india> accessed 20 September 2020

[4]Anoop K. Pandey, 'Introduction to Healthcare Information Privacy and Security Concerns', in Sudeep Tanwar et. al. (ed.), *Security and Privacy of Electronics Healthcare Records* (The Institution of Engineering and Technology, London, 2019) 17

[5]M.S. Bexci & Dr. R. Subramani, "Towards Effective use of Information and Communication Technology (ICT) Application in the Healthcare Management: A Descriptive Study of Online Appointment System Services of Hospitals in India" (2013) 1(7) International Journal of Management Science and Technology, 2, 17

information stored and violation of the right to privacy of the individuals. It is critical to note that the digital health care data includes some sensitive personal data, which is likely to be misused by the miscreants. Therefore, it imperative, that such data is collected and stored with outmost safety.

II. Understanding the Concept of Electronic Health Records

A. What constitutes Electronic Health Records?

Electronic Health Records are digital method to store and maintain a database for the health record patients.[6] These records comprise of the medical history of an individual which is longitudinally arranged as a time series starting from the birth.[7] The data contains personal and sensitive personal information of the patients which are available to the stakeholders including all the past, present or future mental as well as physical conditions, diseases, allergies, sexual orientation and so on.[8]

Often the term Electronic Medical Record and Electronic Health Record are used synonymously but there is a slight difference. While EMR is restricted only to the medical history and treatment of a patients, the EHRs presents a broader view by including data collected beyond standard clinical data. It contains information about the overall health of the person.[9] Unlike EMRs, the EHRs are designed to share information with healthcare providers such as the laboratories and specialists.[10]

The transition of paper records to digitisation of patient information has brought about multiple advantages for all stakeholders of healthcare community. The traditional paper-based records were ineffective as well as cumbersome,[11] for instance, a patient with several years of medical condition like cancer has to carry bundles of previous reports, prescriptions each time he consulted a different doctor. EHRs are designed to provide an efficient, reliable and secure way to store and access the

[6]D.A. Handel DA, & J.L. Hackman, *Implementing Electronic Health Records in the Emergency Department*, 38 JOURNAL OF EMERGENCY MEDICINE, 257, 263 (2010).
[7]Ministry of Health and Family Welfare, *Electronic Health Records Standards for India*, December, 2016, https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
[8]S. Acharya, B. Coats, et.al., *Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objectives,* 46 INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 1, 10 (2013).
[9]Peter Garrett & Joshua Seidman, *EMR vs. EHR – What is the Difference?*, HEALTH IT BUZZ, January 4, 2011. https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference.
[10]*Ibid.*
[11]S. Acharya, B. Coats, et.al., *Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objectives*, 46 INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 1, 10 (2013).

medical information of an individual.[12] This would help the doctor to know the medical history, diagnosis of patient with a click and also reduce patient's load and time in making online appointments and accessing other integrated services. Further, EHR can be digitally shared for health education, e-prescriptions, computer-simulated patient encounter, and computer assisted instructions.

B. Development of Electronic Health Records

The early development of EHR began in USA in 1960s and 1970s. Initially, the EHR systems were known as clinical information systems.[13] By 1980s, Institute of Medicine made incessant efforts to increase use of EHR. By 2004, with the creation of office of National coordinator of health information, the importance of EHR was recognised across the nation.[14]

Health Data in USA is used for primary healthcare purposes like by doctors, clinics, dentists etc., or for supporting health services or administrative services or for a broader secondary purpose like public health programmes, research purposes etc.[15] Federal regulations create powerful incentives for hospitals like granting clinical privileges and in return request the health information from it.[16] Apart from the State authorities, many private entities have collected highly sensitive information as part of employee assistance programs or wellness programs. These programmes include approximately half of the workers in USA.[17]

On the other hand, India is slow in adopting nationwide EHR model. Some of the private hospitals have actively implemented electronic health records such as Max Healthcare in Delhi that introduced the concept of EHRs in the year 2009, other hospital includes Apollo group of hospitals

[12]P.C. Tang, J.S. Ash, and D.W. Bates, *Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption*, 13 J. OF THE AMERICAN MEDICAL INFORMATICS ASSN., 121, 126, (2006).
[13]University of Scranton's Online Resource Center, *EMR: The Progress to 100% Electronic Medical Records*, https://elearning.scranton.edu/resource/health-human-services/emr_the-progress-to-100-percent-electronic-medical-records.
[14]Gabby Marquez, *The History of Electronic Health Records (EHRs)*, ELATION HEALTH, August 4, 2017. https://www.elationhealth.com/clinical-ehr-blog/history-ehrs/#:~:text=In%20the%201970s%2C%20the%20federal,the%20AMA%20Journal%20of%20Ethics.
[15]Alan F. Westin, *How the Public Vies Privacy and Health Research*, 20-22 (March 2008), http://www.iomn.edu/Object.File/Master/48/528/ %20Westin%20IOM%2OSrvy%20Rept.
[16]Paul M. Schwartz, *Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 303, (1995).
[17]Ellen E. Schultz, *Open Secrets: Medical Data Gathered by Firms Can Prove Less Than Confidential*, WALL ST. J. AL (May 18, 1994); *Who's Reading Your Medical Records*, CONSUMER REPORTS 628, 632 (1994); Joan Hamilton, *Can Company Counselors Help You Cope?*, BUSINESS WEEK 140, 141 (Nov. 14, 1994).

in Chennai, Ayambakkam, Nandanam, and Jubilee Hills in Hyderabad, Sankara Nethralaya, Fortis etc.[18]

The Ministry of Health and Family Welfare released the Electronic Health Records Standards for India in August, 2013,[19] which were revised in 2016.[20] The MoH&FW called these standards as 'living document' as they shall evolve with time and shall be guided by the recommendations of proposed National Electronic Health Authority that is set to be established under the proposed Digital Information Security Healthcare Act, 2018.[21]

These standards significantly include the use of patient identifiers (i.e. either UIDAI Aadhaar Number or in absence of Aadhaar, any local identifier or central or state government issued photo identity card number). [22] These standards also include electronic data exchange in healthcare environments; information security management; privilege management and access control; data integrity; and digital certificate.[23] Presently, the existing Indian legislations including Information Technology Act, 2000 and the amendments from time to time would apply.

Additionally, NITI Aayog released a discussion paper on Blockchain technology wherein the introduction of Blockchain technology in various government schemes in health sector was emphasised.[24] It is suggested that blockchain powered digital registration infrastructure be developed for vaccination purposes so that health officials can register details of child at the incidence of birth and that can be accessed in any immunization centre at any place in India.[25] Similarly, the use of blockchain in record keeping of medical insurance claims will automate the insurance process.[26]

III. Privacy and Security Concerns of Health Data

[18]Sunil Srivastav, *Adoption of Electronic Health Records: A Roadmap in India*, 22(4) HEALTHCARE INFORMATICS RESEARCH, 263 (2016).
[19]Ministry of Health and Family Welfare, *Electronic Health Records Standards for India*, August 2013, https://www.nhp.gov.in/NHPfiles/ehr_2013.pdf.
[20]Ministry of Health and Family Welfare, *Electronic Health Records Standards for India*, December, 2016, https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf.
[21]*Ibid*.
[22]*Id*. at 10.
[23]*Id*. at 6.
[24] NITI Aayog, *Blockchain: The India Strategy*, THE DRAFT DISCUSSION PAPER, 1-59 (January, 2020).
[25] *Id*. at 43.
[26] *Id*. at 47.

Privacy, in simple words, is a right of persons to choose to whom or whom not to disclose the information personal to them.[27] EHR Standards, 2016 provides that 'the term privacy shall mean that only those person or person(s) including organizations duly authorized by the patient may view the recorded data or part thereof.[28] The right to privacy is susceptible to attempts by individuals to manipulate the world of another person by selectively disclosing facts about them.[29]

On the other hand, the EHR Standards, 2016 provides that security shall mean 'all recorded personally identifiable data will at all times be protected from any unauthorized access, particularly during transport such as from healthcare provider to the patient or any other healthcare provider'.[30] Therefore, security of EHRs can be understood as the protection measures and tools that are used to safeguard the patient information from unauthorized access and abuses, manipulations, deletions and denial to access.[31]

A. Necessity to Secure the Health Data

The former Chairman of UIDAI, Nandan Nilekani described data as 'the fuel of the modern economy that is a valuable commodity that can be bought and sold and is strategic resource for nations'.[32] Health data can be understood as records that contain information describing a person's past and present health status including aetiology, diagnosis, prognosis, or treatment or methods of reimbursement for health services.[33] It also includes medical information of patients, the patient's identification, that is, personal information, bank account and/or credit card number, past medical judgment, nature of treatment from previous doctors, digital representation of medical images, history of drugs, diet habits, hereditary information, psychological summaries, sexual orientation, income and employment history amongst others.[34]

---

[27] S.D. Warren & L.D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review, 193

[28] Ministry of Health and Family Welfare, 'Electronic Health Records Standards for India' (11 December, 2016) <https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf> accessed 20 September 2020

[29] Richard A. Posner, 'The Right of Privacy' (1978) 12 GA. L. REV. 393, 400

[30] Ministry of Health and Family Welfare, 'Electronic Health Records Standards for India' (11 December, 2016) <https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf> accessed 20 September 2020

[31] Anoop K. Pandey, 'Introduction to Healthcare Information Privacy and Security Concerns' in Sudeep Tanwar et. al. (ed.), *Security and Privacy of Electronics Healthcare Records* (The Institution of Engineering and Technology, London, 2019) 27

[32] Nandan Nilekani, 'Data to the People: India's Inclusive Internet' (2018) 97 Foreign Aff. 19

[33] O. Gostin et al., 'Privacy and Security of Personal Information in a New Health Care System' (1993) 270 JAMA 2487, 2488

[34] R.T. Mercuri, 'The HIPPA-potamus in Health Care Data Security' (2004) 47 Communications of the ACM 1, 7

In addition to healthcare providers such as doctors and clinics, the health data is also held by the members of public health system, health insurance system and an expansive array of record holders such as pharmacies, pathological laboratories, researchers and other employers.[35] It may also be recorded or accessed by entities that might have little or no relationship to provision of healthcare such as banks, credit card companies or direct marketers etc.[36] Therefore, the need for privacy and security of health records become all the more important as any misappropriation of patient's health information may have life-threatening consequences.

However, for the fear of breach of privacy of an individual if the systematic collection of identifiable health data is limited, the chances of substantial social good through thoughtful use of health data will be reduced. Alternatively, if the system in place could not ensure absolute or significant levels of privacy then it will open gates for swarm of cyber-crimes. It is, thus, a system is developed in a manner that ensures that informational privacy co-exists with collection of information digitally for development of healthcare infrastructure.

B. Challenges to Security and Privacy while dealing with Electronic Health Records

Medical records contain critical personal information such as surgical history, fertility issues, sexually transmitted diseases, emotional and psychological disorders, which lots of patients are hesitant to share.[37] The collection and storage of health information in electronic format is vulnerable to be accessed by unauthorized entities or misuse and manipulation by authorized entities.[38]

1. Unauthorized access:

Unauthorized access of personal information includes data theft, hacking, sale of data etc. by users who illegally get hold of the sensitive information. The use of smart devices such as smart watches, wearables, mobile phones, and like products have increased exponentially in considerable sections of society, thereby increasing the theft of medical identity in unprotected devices. There is a

[35] *Ibid.*
[36] *Ibid.*
[37] E.R. Weitzman, S. Kelemen, L. Kaci & K.D. Mandl 'Willingness to share personal health record data for care improvement and public health: a survey of experienced personal health record users' (BMC Med Inform DecisMak, May 22, 2012) <https://bmcmedinformdecismak.biomedcentral. com/articles/10.1186/1472-6947-12-39> accessed 20 September 2020
[38] P. Cerrato, 'Medical data breaches: the latest health care epidemic' (2017) GW Public Health Online Blog, Milken Institute School of Public Health, George Washington University <https://public healthonline.gwu.edu/healthcare-data-breaches/> accessed 20 September 2020

constant threat that hackers, network intruders, previous employees or any other miscreant may steal, access, disrupt, damage information or the hardware.[39] The sale of health data to information brokers or marketing firms to make employment and insurance decisions or uncovering sensitive information about famous individuals like information related to history of mental illness or sexually transmitted disease seems profitable business and might be used in malicious defamation or other purposes.[40] Due to unauthorized access, in India, the Health Solutions pathology laboratory, Thane, Mumbai, suffered data leak of over 43,000 patients' electronic medical data including HIV reports in December 2016.[41]

2. Accidental or wrongful intrusion by authorized entities:

It may happen that medical personnel may misuse the given access to patient's health data for personal respite, revenge, profit or other purposes by leaking out or selling the information. Also, since the information may pass several digital entities and healthcare providers, there may be unintentional errors that cause the data to disclose.[42] The issue of violation of privacy security of healthcare data is thought-provoking and challenging in multi-specialist situations or when the EHR system uses the storage space or transfer mechanism of third parties.[43]

IV. Legal Framework related to protection of Digital Healthcare Data in USA

With the emergence of EHR in the USA, the Health Insurance Portability and Accountability Act (hereinafter referred as HIPAA) was introduced in 1996 in response to the growing concerns of violation of privacy and breach of security due to growing healthcare coverage.[44] Later on, EHR was incorporated in the 2009 American Recovery and Reinvestment package during the Obama

[39]A. Le Bris & W. El Asri, 'State of cybersecurity and cyber threats in healthcare organizations: applied cybersecurity strategy for managers' (2017) ESSEC Business School <https://www.beckershospitalreview.com/healthcare-information-technology/top-3-security-threats-to-the-healthcare-industry-tips-to-avoid-them.html> accessed 20 September 2020

[40]'Congressional Office of Technology Assessment, Protecting Privacy in Computerized Medical Information' (1993) OTA-TCT-576, 26

[41]TNN, 'HIV patients' data in 43,000 path lab reports leaked online' *Times of India*, (December 3, 2016) <https://timesofindia. indiatimes.com/city/mumbai/HIV-patients-data-in-43000-path-labreports-leaked online/articleshow/55761372.cms>

[42]R.E. Gliklich, N.A. Dreyer & M.B. Leavy (ed.), 'Registries for Evaluating Patient Outcomes: A User's Guide' in M.D. ROCKVILLE, 11 *Data Collection and Quality Assurance* (Agency for Healthcare Research and Quality, US 2014)

[43]The Office of the National Coordinator for Health Information Technology, 'Guide to Privacy and Security of Electronic Health Information' (2015) <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

[44] Jim Atherton, Development of the Electronic Health Record, 13(3) Journal of Ethics, 186-189 (2011).

presidency as a part of the Health Information Technology for Economic and Clinical Health Act, 2009 (hereinafter referred as HITECH).[45]

A. Health Insurance Portability and Accountability Act, 1996

The basic federal law that regulates the healthcare industry in the USA is HIPAA and it applies only to what the law considers covered entities and their business associates. The covered entity consists of healthcare providers that include doctors, psychologists, clinics, dentists etc.; health plan that include insurance companies, employer-sponsored health programs, government programs etc. and health care clearinghouse that process data content to put it in a standardized format or vice-versa. While a business associate is the one who handles protected health information on behalf of a covered entity to help them carry out healthcare related functions under a contract. In case, the medical information is disclosed to anyone else who does not fall in the above two categories then that information shall not be protected under HIPAA.[46]

The rules only protect information that is known as individually identifiable health information that includes demographic data of patient relating to the individual's past or present physical or mental health or condition or any previous, present or in advance medical treatments or payments and such information is likely to identify the individual or at least creates a reasonable basis to identify the individual.[47] HIPAA required the U.S. Department of Health and Human Services (hereinafter referred as HHS) to develop regulations protecting the privacy and security of health information;[48] and thereof regulations commonly known as HIPAA Privacy Rule and HIPAA Security Rules were published.

1. Privacy rule

The Standards for Privacy of Individually Identifiable Health Information or better known as HIPAA Privacy Rule established a set of national standards for the protection of certain health information. [49] It lays down the rules as well as standards that address the use and disclosure of protected health information by the covered entities and business associates for protection of

[45] *Ibid*.
[46]United States Department of Health & Human Services, *Summary of HIPAA Privacy Rule*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.
[47] 45 C.F.R. § 160.103
[48] PUBLIC LAW 104–191—AUG. 21, 1996.
[49]United States Department of Health & Human Services, *Summary of HIPAA Privacy Rule*, https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

privacy rights of individuals, held or transmitted in any form or media, whether electronic, paper, or oral.[50] Furthermore, the use and disclosure of protected health information by the covered entities and business associates is classified into three heads:

(i) Required disclosures

A covered entity must disclose protected health information only to individuals or their personal representatives when they request access to it or for accounting of disclosures of their protected health information; or HHS when they are undertaking a compliance investigation or review or enforcement action.[51]

(ii) *Permitted uses and disclosures*

A covered entity is permitted and not required to disclose the protected health information without the authorization of individual for the specified purposes only. In this category, information may be disclosed in certain situations that includes disclosure to an individual; for treatment, payment and healthcare operations to any other healthcare providers; for public interest or benefit activities that falls in national priority purposes; incidental uses or disclosures and for the purposes of research, law enforcement, judicial proceedings or health care operations.[52]

(iii) Authorized disclosure

In certain cases, the covered entity must take written authorization of individual for any use or disclosure of protected health information that is not for treatment, payment or healthcare operations but it is otherwise permitted or required under the rules that includes disclosures to an employer for pre-employment medical test or life insurer for coverage of medical bills or to pharmaceutical firms for marketing or other specified purposes.[53]

2. Security rule

Another important rule is the Security Standards for Protection of Electronic Protected Health Information or better known as HIPAA Security Rule that established a national set of security standards for protecting certain health information that is held or transferred in electronic form

[50] 45 C.F.R. § 160.103.
[51] 45 C.F.R. § 164.502(a)(2).
[52] 45 C.F.R. § 164.502(a)(1).
[53] 45 C.F.R. § 164.508.

known as electronic protected health information.[54] It specifies a series of administrative, technical or physical security procedures for covered entities specifically to ensure the confidentiality, integrity and availability of the electronic protected health information. The Rule also requires compliance of security standards by the workforce of the covered entity or business associates; identification and protection against the reasonably anticipated threats to the security or integrity of the information and reasonably anticipated impermissible uses or disclosures.[55]

However, this Rule gives enough room to allow the covered entities or business associates to analyse their own needs by their size, complexity, and capabilities, technical, hardware, and software infrastructure, costs of security measures and likelihood and the possible impact of potential risks to electronic protected health information and implement solutions that are appropriate for their specific environments.[56] The security measures shall be reviewed and modified periodically to ensure protection of electronic protected health information in changing environment.[57]

3. Breach notification rule

One of the important rules is the requirement to notify breach to the affected individuals, HHS and, in some cases, the media of a breach of unsecured health information by the covered entities and business associates. Herein, breach is generally an impermissible use or disclosure under the Privacy and Security Rules that compromises the security or privacy of protected health information.[58] However, the presumption of breach can be rebutted by the demonstration by the defaulted entity that there is a low probability that protected health information that has been compromised based on a risk assessment of at least the following factors: (i)The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification; (ii) The unauthorized person who used the protected health information or to whom the disclosure was made; (iii) Whether the protected health information was actually

[54] 45 C.F.R. § 160.103.
[55] 45 C.F.R. § 164.306(a).
[56] 45 C.F.R. § 164.306(b)(2).
[57] 45 C.F.R. § 164.306(e).
[58] U.S. Department of Health & Human Services, *Breach Notification Rule, Health Information Privacy*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

acquired or viewed; (iv)The extent to which the risk to the protected health information has been mitigated.

B. Health Information Technology for Economic and Clinical Health Act, 2009

The HITECH Act of 2009 presented a new process for certification of EHRs that was sponsored by Office of the National Coordinator for Health Information Technology as well as Certification Commission for Healthcare Information Technology certification. This new certification ensures that the rules of HIPAA for EHRs are complied and further support meaningful use. The certification includes requirements on confidentiality of data through database encryption, transmission mode encryption, access control through authentication, data integrity, audit trail logs, automatic log off, access in case of an emergency and also addressing HIPAA releases of information.[59]

The HITECH Act also helped in fortifying existing breach notifications in HIPAA in addition to HIPAA breach notification rule by enforcing civil and criminal penalties for business associates as well as other covered entities.[60] Civil penalties can be imposed extending up to 1.5million USD. In the case of breach of protected health information, all the affected individuals or organizations must be notified without unreasonable delay within sixty days following the breach discovery. Also, annual submission should be made to HHS notifying all the smaller breaches affecting less than five hundred individuals.

V. Legal Framework related to Protection of Digital Healthcare Data in India

A. Existing Legislation Regarding Data Protection

The collection and storage of digital healthcare data is a remarkable step in the healthcare sector. However, it also raises many concerns regarding the protection of the information and privacy of the individuals. The digital healthcare data is collected and stored by clinical establishments and other entities, so naturally, the control and responsibility to protect the data from any kind of data breach lies with them. Presently, in India, there are legislation to prevent data breach such as the

[59]The Office of the National Coordinator for Health Information Technology, *Guide to Privacy and Security of Electronic Health Information*, (2015), https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

[60]United States Department of Health & Human Services , *HIPAA Breach Notification Rule, 2016*, HHS.gov, https://www.hhs.gov/hipaa/for-professionals/breach-notification/ index.html.

Information Technology Act, 2000 (hereinafter referred as IT Act), the Information technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 framed under IT Act, The Indian Medical Council Act, 1956, The Clinical Establishments Act, 2010, Other Service Providers Regulations under the New Telecom Policy, 1999. [61] The existing legislation regarding digital healthcare and data protection handles the issue of data protection in a piecemeal manner. It merely addresses the tip of the iceberg and fails to address many aspects of data breach. In India, the offence of data breach is dealt under the IT Act. But in the times where new technology is evolving rapidly, twenty-year-old legislation fails to tackle the new challenges posed due to the advent of technology.

The novel and complex nature of digital health data demands a more elaborate and specific legislation to protect the personal data of the individuals. Presently, two new legislations have been proposed to tackle the vices of data breach, namely, draft of the Personal Data Protection Bill, 2019,[62] and the Digital Information Security Healthcare Act (DISHA)[63].

B. Insufficiency in the existing legislation

Some of the failures of the existing legislations can be observed while understanding the scope and application of Section 43A of IT Act that provides for the compensation for failure to protect data.[64]

Firstly, the newly added provision imposes liability on body corporates and also specifies the meaning of the term body corporate. It defines body corporate, as any company and includes a firm, sole proprietorship, or other association of individuals engaged in commercial or professional activities. The section omits to include any government agencies and non-profit organisations or other entities that may collect or store digital health data as body corporates. Therefore, apart from

[61] Dr. Milind Antani, Darren Punnen & Shreya Shenolikar, 'Digital Health in India: Legal, Regulatory and Tax Overview' (Nishith Desai ,April 2020), <http://www.nishithdesai.com/fileadmin/user_upload/pdfs/Research_Papers/Digital_Health_in_India.pdf> accessed 20 September 2020

[62]The Personal Data Protection Bill, 2019, Ministry: Law and Justice, (2019) <https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf> accessed September 15, 2020

[63] *Placing the draft of "Digital Information Security in Healthcare, act (DISHA)" in public domain for comments/views-reg*, (Ministry of Health and Family Welfare, 21 March 2018) <https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf> accessed September 20 2020

[64] Information and Technology Act, 2000 § 42A.

the body corporates, no other entity or agency can be held liable for data breach under the Act. This constricts the scope of the provision and limits its application.[65]

Secondly, the hospitals and clinical establishments are allowed to collect, store, or access digital health data. Such entities are more likely to commit data breach. Therefore, it is imperative that such entities are brought within the purview of the Act. Now, the majority of the hospitals are companies and fall into the category of body corporates. However, an unregistered clinical establishment is not body corporates and fall beyond the purview of Section 43A of the Act. Section 3 of the Clinical Establishments (Registration and Regulation) Act, 2010, lays that Establishments falling under the definition of a 'clinical establishment' under the Clinical Establishments Act would be required to register with the relevant authority and conform to the minimum standards as prescribed under the Act.[66] Therefore, the acts of Clinical establishments that are not incorporated under the Act are not punishable under the IT Act.

Thirdly, under the Act 'sensitive personal data or information'[67] is defined as such personal information as may be prescribed by the Central Government and the term "reasonable security practices and procedures"[68] is defined as those measures which the body corporate has to follow. Such measures are either specified in an agreement between the parties, in any law in force or as prescribed by the central government. The definition provided in the Act clearly indicates a room for further legislation and executive directions. The definitions are not conclusive, instead it demands further elaboration.

C. Introduction to the Data Protection Bill

From the above discussion, it is evident that the existing legislation regarding data protection deals with the issue in a piecemeal manner and there are many gaps in the legislation that needs to be plugged. The failure of the pre-existing legislation to protect personal data has led the way for the

[65] N.S. Nappinai, *Technology Laws Decoded*, (1st ed. 2017)
[66] Asheeta Regidi & Nehaa Chaudhari, 'DISHA and the draft Personal Data Protection Bill, 2018: Looking at the future of governance of health data in India' (Ikigai law, 25 February 2019) <https://www.ikigailaw.com/disha-and-the-draft-personal-data-protection-bill-2018-looking-at-the-future-of-governance-of-health-data-in-india/> accessed 20 September 2020
[67] Information and Technology Act, 2000 § 43A.
[68] *Id.*

introduction of Data Protection Bill which provides a well-built mechanism to thwart the misuse of personal data in the country.

In July 2018, a committee lead by retired Supreme Court Judge, Justice B.N. Srikrishna submitted the draft of the personal data protection bill requesting further feedback from the public, ministers and stakeholders till September 2018. The revised version of the Bill was submitted in the Lok Sabha in 2019. Presently the Bill is still pending and is expected to be enacted as legislation soon.[69]

The Bill establishes a fiduciary relationship between the owner of the data and the entity with whom the data is stored or accessed. An individual is vested with the right to either restrict or prevent the disclosure of his personal information.[70] Furthermore, the Bill also highlights the need for specifying the purpose of collection of the data by the companies and also imposes the responsibility of informing the owner regarding any use[71] or transfer of the data from one provider to another.[72] It also lays down the foundation for the formation of a 'Data Protection Authority of India', which will be work as a watchdog in the matters of data security and data protection. The authority shall ensure the compliance of the measure provided by the Bill and prevent any misuse of personal data or information.[73]

The Bill provides an inclusive definition of sensitive personal data, which is absent in the IT Act, 2000. It categorises personal data into two categories to revamp the data management practices and also provides some clarity on the data localisation. The categories are namely sensitive personal data and critical personal data.[74] Personal data is defined as information which can be used in the identification of the person and any such inferences drawn out of that information.[75] Whereas, sensitive personal data refers to any information related to financial data, health data,

[69]Surabhi Agarwal, 'Justice Srikrishna committee submits report on data protection. Here're its top 10 suggestions' (ET, 28 July 2018) <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-committee-submits-report-on-data-protection-herere-the highlights/articleshow/65164663.cms?from=mdr> accessed 20 September 2020

[70] The Draft of Data Protection Bill, 2019 § 20 Cl. 1.

[71] The Draft of Data Protection Bill, 2019 § 11 Cl. 3.

[72] The Draft of Data Protection Bill, 2019 § 11 57.

[73] The Draft of Data Protection Bill, 2019 § 11 41.

[74] Surbhi Aggarwal & Meghna Mandavia, 'Government localises 'critical' & 'sensitive' personal data' (ET, 05 December 2019) <https://economictimes.indiatimes.com/news/politics-and-nation/government-localises-critical-sensitive-personal-data/articleshow/72376594.cms?from=mdr> accessed 20 September 2020

[75]The Draft of Data Protection Bill, 2019 § 2 Cl. 28.

sex life, sexual orientation, biometric data, genetic data, caste or tribe, religious or political belief or affiliation, etc.[76]

The term critical personal data has been not been defined yet and is left at the discretion of the Central Government to provide meaning to the term.[77] The Bill restricts the cross-border data flow of critical and sensitive data.[78] The storage and processing of critical personal data cannot be outside India. However, the Bill allows the processing of sensitive personal data outside India. The Government is empowered to restrict the storage and processing of any sensitive personal data outside India, by classifying that data as critical personal data.[79]

Another striking feature of the bill is the introduction to right to erasure and right to be forgotten. The inspiration for the same has been derived from Article 17 of the European General Data Protection Regulation which provides for right to be forgotten which falls under the broad heading of right to erasure.[80] However, unlike the right provided in the European GPDR, the bill segregates between the right to erasure and right to be forgotten. Section 18 of the bill provides for right to erasure of personal data which is no longer necessary for the purpose for which it was processed,[81] while Section 20 of the bill provides for right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary.[82]

The bill significantly differs from the provisions GDPR relating to right to be forgotten. Under the GDPR the data principal has to apply to the data fiduciary for the removal of the personal data. The decision as to whether the data has to be removed or not is ultimately taken by the data fiduciary.[83] Therefore, the adjudicating powers are vested with the data fiduciary. However, under the data protection bill the adjudicating power cannot be vested in a private entity and so the data fiduciary has to further apply to government body (democratically elected) for the approval to delete the personal data so requested by the data principle.[84]

[76]The Draft of Data Protection Bill, 2019 § 3 Cl. 36.
[77] The Draft of Data Protection Bill, 2019 § 33 Cl. 2.
[78] The Draft of Data Protection Bill, 2019 § 34.
[79] *Id.*
[80] The European General Data Protection Regulations, Article 17.
[81] The Draft of Data Protection Bill, 2019 § 18(1)(d).
[82] The Draft of Data Protection Bill, 2019 § 20.
[83] The European General Data Protection Regulations, Article 18.
[84] *Ibid.*

D. Overview of the Digital Information Security in Healthcare Act, 2018 (DISHA)

The Ministry of Health & Family Welfare has proposed a new bill in 2018 titled the Digital Information Security in Healthcare Act to govern data security in the healthcare sector. The Purpose of the Act is to provide for electronic health data privacy, confidentiality, security and standardisation.[85] Some of the salient features include the right to ownership of the health data by an individual. The owner has the right to privacy, confidentiality and security over their personal health data.[86] Also, the consent of the owner of the information is of prime importance, the owner can refuse to share the digital health data with the clinical establishment and other entities.[87] Consequently, the owner has the right to refuse or withdraw consent to access or disclosure of the digital health data.[88] In case of data breach, the owner has the right to claim compensation for damages caused.[89]

The Act imposes liability to protect the health data on any entity that collects digital health data and that the digital health data should not be disclosed or used for commercial purposes. It also puts a bar on disclosure of the data to insurance companies, employers, human resource consultants and pharmaceutical companies, or any other entity as maybe specified by the central government.[90]

Furthermore, Section 33 of the draft legislation of DISHA provides guidelines for the transmission of information by the clinical establishment. The provision allows the transmission of the health data by clinical establishment in an encrypted form and for reasonable use. Also, the data can be transmitted only after the data is well informed about his right and gives his consent for such transmission. It further provides that the National Electronic Health Authority of India (NEHA) shall provide standards for physical, technical, administrative measures, keeping in mind the privacy and confidentiality of the data owner.[91]

[85]Digital Information Security in Healthcare Act, 2018, (Government of India, Ministry of Health & Family welfare, 2018) < https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf > accessed 20 September, 2020
[86] Digital Information Security in Healthcare Act, 2018 § 28 Cl. 1
[87]Digital Information Security in Healthcare Act, 2018 § 28, Cl. 2
[88]Digital Information Security in Healthcare Act, 2018 § 28 Cl. 3.
[89]Digital Information Security in Healthcare Act, 2018 § 28 Cl. 8.
[90]Digital Information Security in Healthcare, Act, 2018 § 29 Cl. 5
[91]Digital Information Security in Healthcare, Act, 2018 § 33 Cl. 2.

E. Whether DISHA and Data Protection Bill is the required law?

Evidently, the Data Protection Bill provides a very innovative approach towards data protection. The provision backs the directions provided by the Reserve Bank of India that mandates all the banks to store all information about payments in India.[92] Another notable aspect of the Bill, which catches attention, is that the Bill proposes to repeal section 43A of the IT Act, 2000 because of the overlapping of similar provisions from the Bill as well as the Act.[93] However, it doesn't deal with another parallel provision in IT Act i.e. Section 72A that provides punishment for disclosure of information in breach of lawful contract.[94] Therefore, there can be clashes between the two legislations, when the bill becomes a law.

A stark difference can be observed in the provisions of DISHA and the data protection bill that is DISHA provides for such restrictions that are essential to safeguard the privacy of an individual. In DISHA the information can be accessed without the consent of the owner only for a specific purpose as specified in the Act, the scope of non-consent based processing is narrow and restricted to purposes such as to advance the delivery of patient care or to improve public health facilities.[95] This is opposed to the approach taken in the Data Protection Bill, where the scope of non-consent based processing of information is wide and more liberal. In this aspect, DISHA proves to be a better piece of legislation with lessloopholes, as it provides more efficient and effective provisions for the protection of the personal health data. Both these legislations are similar in essence, as both of them create a trust-based relationship between the individual and the entity storing the information. However, both the legislations differ in their approach to some extent.

Furthermore, according to DISHA,, the government agencies can access the health data from the NEHA established under the Act for only those purposes as mentioned in the Act. This restricts the power of the government agency to access the personal information to a large extent, whereas the only restriction placed in the Data Protection Bill is that the information must be provided for protection of the sovereignty and integrity of India, the security of the state, friendly relations with

[92]Kunal Thakore & Deepa Christopher, 'Data Protected – India' (March 2020) <https://www.linklaters.com/en/insights/data-protected/data-protected---india> accessed 20 September, 2020
[93]*Ibid.*
[94] Information and Technology Act, 2000 § 72A.
[95]Digital Information Security in Healthcare, Act, 2018 § 29.

foreign states, public order.[96] Such terms are extremely subjective and because of such wide interpretation. The government is vested with immense unfettered power to access the data which may have adverse effects. DISHA narrows down the purposes for which the data can be accessible, thereby making it a suitable legislation for protecting the healthcare data.

VI. Current Issues relating to Protection of Health Data in India

The Data Protection Bill provides that the central government may allow any government agencies such as law enforcement agencies or authorized third parties, to access the personal data of the individuals without complying with the legal obligations entailed in the Bill.[97] The exemption offers an advantage to the government in matters relating to protection of sovereignty and integrity of India, the security of the state, friendly relations with foreign states, public order.[98] However, such unfettered power also raises concerns regarding the right to privacy of an individual.

Privacy concerns are the major reason for the delay in passing the Bill, as it is anticipated that the Bill would prove to be a threat to the right to privacy. Similar issues were raised in the Aadhaar case[99], where the biometric data of an individual was accessible by the government as well as the private entities.[100] The constitutionality of the Act was challenged in a writ petition, on the grounds of violation of Article 21 of the Constitution. However, the Supreme Court upheld the constitutionality of the Aadhaar Act but with few riders.

A. The Importance of the Aarogya Setu App

Many concerns have been raised regarding data protection of the health data collected by the *Aarogya Setu* App. The app has brought a revolution in the health sector and the introduction of digital healthcare becomes even more relevant in the time of a global pandemic. The issue at hand has sparked major debates regarding data protection and right to privacy of individuals

The app gained massive popularity after the Prime Minister of India urged its citizens to use the app. *Aarogya setu* is a contact tracing app that provides assistance in preventing the spread of

[96] Draft of Data Protection Bill, 2019 § 35 Cl. 1.
[97] Draft of Data Protection Bill, 2019 § 35 Cl. 2.
[98] *Id.*
[99] Justice K. S. Puttaswamy v. Union of India, (2018) 1 S.C.C. 809.
[100] The Aadhaar Act (repealed) § 57.

coronavirus by tracing the individuals, who come in contact with an infected person.[101] In absence of any vaccine to cure the infection, the only recourse left with the government is to prevent further communication of the disease. In order to assure the same, it is imperative that the government conducts testing and isolates the infected person as well as those who come in contact with the infected ones. It is anticipated that a contact tracing app can prove to be a strong weapon against the virus.

Apart from the contact tracing features, the app also provides access to telemedicine, an e-pharmacy, and diagnostic services. Also, it advises the users for quarantine, caution and testing.[102] However, the major concern surrounding the use of the application is the protection and security of the data shared by the app users.

B. The privacy concerns relating to the Aarogya Setu App

Several times the government as well as private infrastructure have suffered cyber-attacks, like the incidents of hacking into Pune-based Indian Railways Institute of Civil Engineering, targeted attacks on the State-run Nuclear Power Corporation of India; and hacking into servers of Airport Authority of India's Cargo department and breaches in ATC.[103] The app server stores information worth millions and it is highly likely that the hackers might attempt to gain authorised access to the data. In the past, the personal data of 2.9 crore job-seeking Indians was leaked on the dark web for free in one of the hacking forums.[104]

This is the reason that despite the multiple benefits offered by the app, it has attracted huge criticism on grounds of threat to the security and privacy of an individual. Especially when the Indian government made it mandatory for all the employees of any private or public company as well as all the passengers to download the app. However, the latest Ministry of Home Affairs

[101] Ministry of Electronics & Information Technology, 'Aarogya Setu is now open source' (Ministry of Electronics & Information Technology Electronics Niketan, 26 May 2020) < https://static.mygov.in/rest/s3fs-public/mygov_159050700051307401.pdf > accessed 20 September 2020

[102] *Id.*

[103] Manu Kaushik, 'Beware of the Bugs' (Business Today, 17 Feb 2019)<https://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html.> accessed 20 September 2020

[104]Anandi Chandrashekhar & Surabhi Agarwal, 'Mumbai, New Delhi, Bengaluru face maximum cyber attacks: Report' (ET, 06 May 2020), < https://tech.economictimes.indiatimes.com/news/mobile/legal-experts-point-out-liability-concerns-with-the-aarogya-setu-app/75561228 > accessed 20 September 2020

Directive has removed the clause mandating the use of *Aarogya setu* app.[105] This was a necessary step taken by the Indian government considering the security issues and the threat it poses to the privacy of its users. Recently Elliot Alderson, a French hacker and cyber-security expert intimidated the government about some security issues in the app, which may adversely affect the privacy of 90 million Indians.[106] Apart from that, many other such private entities highlighted the privacy issues in the *Aarogya Setu* app. It is alleged that the app lacks transparency, and it poses a threat to the user's security because of the sensitive personal data collected through it.[107]

Furthermore, the computer emergency response team under the ministry of information and technology released an advisory raising security concerns relating to *Aarogya Setu* app, highlighting the phishing attacks related to the app. It also reported that the criminals are sending fake phishing emails in the name of WHO, which are originating from World Health Organisation domain name.[108] The advisory warned against such mails for having various malicious files or URLs (Universal Resource Locator).[109]

C. Liability of the government in case of any Data breach

Another concern regarding the app is the liability of the government in case of any data breach. The app stores sensitive personal data of all the users. The troublesome aspect is that the user of the app is unaware as to who has access to the data. The government has the discretion to allow the access of the data to any third party.[110] As per the data sharing protocol released by the Ministry of Information and Technology, the Government may share the data with third parties if it finds it

[105]Rahul Tripathi, 'MHA dilutes provision on use of Aarogya Setu app' (ET, 26 May 2020) <https://economictimes.indiatimes.com/news/politics-and-nation/aarogya-setu-not-mandatory-for nris/articleshow/75983344.cms?from=mdr> accessed 20 September 2020

[106]Revathi Krishnan, 'Govt Thanks French ethical hacker who flagged Aarogya Setu, but dismisses security concern' (The Print, 6 May 2020) <https://theprint.in/india/govt-thanks-french-ethical-hacker-who-flagged-aarogya-setu-but-dismisses-security-concern/415348/> accessed 20 September 2020.

[107] Saurabh Singh, 'Government of India makes Aarogya Setu app open source; here is what it means' (The financial Express, 26 May 2020) <https://www.financialexpress.com/industry/technology/government-of-india-just-made-aarogya-setu-app-open-source-here-is-what-it-means/ > accessed 20 September 2020

[108] Hemani Seth, 'Covid-19, Aarogya Setu related phishing scams see a massive spike in May: Report' (The Hindu Bussinessline, 13 May 2020) <https://www.thehindubusinessline.com/info-tech/covid-19-aarogya-setu-related-phishing-scams-see-a-massive-spike-in-may-report/article31573109.ece> accessed 20 September 2020

[109]'Phishing attacks in name of Aarogya Setu app increasing: Cyber agency' (ET, 18 May 2020) <https://ciso.economictimes.indiatimes.com/news/phishing-attacks-in-name-of-aarogya-setu-app-increasing-cyber-agency/75797051> accessed 20 September 2020

[110] *Ibid.*

necessary for directly formulating or implementing appropriate health responses.[111] This means that personal data can be shared with anyone on the directions of the government. Additionally, the terms and conditions of the app absolve the government from any liability.

The terms and conditions of the app include an indemnity clause that limits the government's liability towards the user. The clause states that the user agrees and acknowledges that the government of India will not be liable for any unauthorized access. In that scenario, legal actions in the court will be the only alternative left at the disposal of the affected users.[112]

The clause also falls in violation of the Information Technology Act and the proposed Personal Data Protection Bill, as both these legislations imposes liability on the intermediary for any data breach.[113] The IT Act clearly mentions that the person who receives stores or transmits that record or provides any service concerning that record will be an intermediary under the Act.[114] On the other hand, the Data Protection Bill coins a new term i.e. social media intermediary, which essentially means any individual who primarily or solely enables online interaction between the users and allows them to create, upload, share, disseminate, modify or access information using its services.[115] The app service provider falls within the ambit of the definition of intermediary and will be obligated to ensure the security of the data and would incur liabilities in case of data breach. Therefore, the indemnity clause falls in strict violation of the existing as well as the proposed legislation regarding data protection.

From the above discussion, it is clear that the *Aarogya Setu* app on the face of it appears to be a threat to the security of the user and it lacks legislative backing, In a country where the legislative framework for data protection is already out-dated, any kind of data breach can cause massive damage to the government and the users of the app.

VII. Considerations for Securing Digital Health Data- USA or India Way

[111] The Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020, Protocol 7(b) <https://meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf> accessed 20 September 2020
[112] *Supra* note 27.
[113] Information Technology Act, 2000 § 67C.
[114] Information Technology Act, 2000 § 2 Cl. w
[115] Data Protection Bill, 2019 § 26.

A patient provides his health information in trust to the health care system in the electronic format for the better facilities and the development in scientific research. It is very important that the patient is assured of the protection of his privacy as well as data against any risk associated with EHRs.[116] The health data is shared by the patient on the trust developed through the medical relationship and it shall be protected and secured at all costs as it contains information that is confidential,[117] and such information shall only be disclosed as per law or with authorization from the patient.

In India, the development of a pan India EHR model is at a very nascent stage in terms of technology, infrastructure, implementation and law. The USA model of EHR and the related laws have existed for more than two decades and sets an exemplary digital healthcare system for considerations in India. Undoubtedly, the provisions of the Information Technology Act, 2000 are insufficient to deter the breach of health data. The other related legislations that are Personal Data Protection Bill and Digital Information Security of Healthcare Data Act are yet to be enacted by the Parliament. In the meanwhile, the following are the suggested considerations for safe and secure transmissions in light of HIPAA and HITECH:

A. Access Control and Verification of Users

In addition, to encryption of data as provided under DISHA and EHR Standards 2016, a set of persons could be identified as to who shall have the authorization to access the health information. Access Control means that the authorized access shall be controlled i.e. depending on the role and duties performed by the authorized persons the access of data should be limited. For instance, in case of healthcare providers, the doctor and the nurse have different work and responsibilities, so they can't have the same rights to access the same information.

HITECH Act requires the certificate of compliance for which the entity needs to show evidence of access control through authentication.[118] For facilitating access control an identity management system can be established that is composed of users, systems or applications, and policies; which

[116]J. Vora, P. Italiya, S. Tanwar et al., 'Ensuring privacy and security in E-health records' (2018) Int'l Con. on Computer, Information and Telecommunication Systems, France, 192, 196

[117]L.A. Rinehart-Thompson & L.B. Harman, 'Privacy and Confidentiality' in L.B. Harman (ed.), *Ethical Challenges in the Management of Health Information* (2nd ed. Sudbury, MA: Jones and Bartlett, 2006) 53

[118] The Office of the National Coordinator for Health Information Technology, 'Guide to Privacy and Security of Electronic Health Information' (2015) <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf> accessed 20 September 2020

is based on the privilege and rights of each practitioner authorized by the patient or trusted third parties.[119] In a non-secure remote connection, it is tough to identify a user who is retrieving the data,[120] and there use of authentication systems such as token-based and biometric-based authentication systems can provide assurance to the users for authorized access to healthcare records.[121]

B. Stringent Data security policies

Under the HIPAA Privacy and Security Rules, liability can be imposed on the employers for the breach committed by their employees. One such case took place in USA in 2011, wherein the employees of the UCLA health department accessed the records of famous celebrities without authorization. Consequently, UCLA was held accountable for this breach for not being able to implement enough security measures so as to mitigate the risk of unauthorized access to protected electronic health information and had to pay a fine to HHS amounting to USD 865,000.[122]

A similar rule can be imposed on the organizations collecting health data herein India through DISHA that they make stringent rules and processes to ensure inhibition of loss or theft of data or portable devices. There should be a regular security update of EHR system to block or track the access of important medical information like lab reports, encrypt entries, manage security levels.[123] The entities can conduct periodical training programs security standards or mock drills of to avoid probable threat for instance hacking, alteration, or damage of data by internal or external users.[124]

C. Data Breach and Mandatory Disclosure

Breach of a medical data is an intentional or unintentional unauthorized disclosure of health information from EHR or billing records from any entity holding such information.[125] HIPAA

[119]Arjun Khera et.al., 'Application design for privacy and security' in Sudeep Tanwar et. al. (ed.), *Security and Privacy of Electronics Healthcare Records* (The Institution of Engineering and Technology, London, 2019) 100
[120]M.N. Huda, N. Sonehara & S. Yamada, 'A Privacy Management Architecture for Patient-Controlled Personal Health Record System' (2009) 4(2) Journal of Engineering, Science and Technology
[121]Y. Han & B. Deng, 'A Smart-Card-Enabled Privacy Preserving E-Prescriptions System' (2004) 8(1) IEEE Transaction on Information Technology in Biomedicine, 47–58
[122]Health and Human Services, 'University of California settles HIPAA privacy and security case involving UCLA Health System facilities' (2011) HHS gov. 7
[123]Sudeep Tanwar et. al. (ed.), *Security and Privacy of Electronics Healthcare Records* (The Institution of Engineering and Technology, London, 2019) 12
[124]*Id*. at 11.
[125]Anoop K. Pandey, 'Introduction to Healthcare Information Privacy and Security Concerns' in Sudeep Tanwar et. al. (ed.), *Security and Privacy of Electronics Healthcare Records* (The Institution of Engineering and Technology, London, 2019) 32

breach notification rules and HITECH make stringent provisions of mandatory disclosure of breach of protected health information to the affected individuals or organisations and the US Health Department i.e. HHS and media houses in certain cases. Under DISHA, the probable Section 35 provides that a clinical establishment or a health information exchange shall provide notice immediately, in all circumstances, in a prescribed format, to the owner of data within three days in case of breach of such digital data.[126]

DISHA provides only three days' time limit to disclose a breach of information to the owner of data, HHS and in some cases to the media within sixty days' time span from the date of breach discovery under HIPAA. The provision of DISHA requires more clarity regarding a hyper optimistic time limit and the date of commencement of this time period and that will only be clear once the rules are prescribed under DISHA regarding the manner of disclosure.

D. Audit Trail

The Audit trail requires maintenance of record to check who had accessed the patient's data. While HIPAA mandates to main the audit log records for a minimum of 6 years,[127] DISHA has no such mandatory requirement. Audit trails log all activities of addition, modification and deletion of entries in an EHR along with the date and time stamp in addition to access logs, authentication logs and any other related system activity logs.[128] It thus facilitates to spot errors, to indict the individual who committed a breach or for evidence in legal proceedings.

E. Certificate of Compliance

The main objective of HITECH Act, 2009 is to mandate certificate of compliance of HIPAA rules regarding requirements on confidentiality of data through database encryption, transmission mode encryption, access control through authentication, data integrity, audit trail logs, automatic log-off, access in case of an emergency and also addressing HIPAA releases of information.[129]

[126] Digital Information Security in Healthcare, Act, 2018 § 35 Cl. 5.
[127]L. Washington, 'Managing health information in mobile devices' (2012) 83(7) Journal of AHIMA 58–60
[128]Gelzer R, Hall T, Liette E, et al., 'Copy Functionality Toolkit: A Practical Guide: Information Management and Governance of Copy Functions in Electronic Health Record Systems' (2012) Int'l J. of AHIMA
[129] The Office of the National Coordinator for Health Information Technology, 'Guide to Privacy and Security of Electronic Health Information' (2015) <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>

Presently, there is no such mandatory provision in DISHA and it seems that it is an important inclusion that needs to be deliberated upon.

F. Disclosure to other entities

In the USA, HIPAA is applicable to covered entities as well as business associates that include a wide range of entities other than healthcare providers like HHS, government, employees, pharmaceutical firms, insurance providers etc. However, DISHA strictly prohibits access, use or disclosure of digital health data whether identifiable or not to any person for a commercial purpose and under no conditions to insurance companies, employees, human resource consultants and pharmaceutical companies.[130] Even the government departments including Ministry of Health will have to request access to the National Electronic Health authority for specified purposes.[131]

The restrictive approach of the Indian legislators is cautious and thoughtful considering the nascent stage of development of EHRs in the country. It not only controls private but government surveillance on digital information as well. But with the usage of EHRs for a considerable time, DISHA might require amendments on this avenue considering the intricate role of insurance companies and development of e-commerce and e-business possibilities in healthcare sector.

VIII. Conclusion- Moving Ahead

The digitisation of healthcare will empower wellbeing of citizens by improving connectivity and better accessibility not only within India but also across the globe. It is undeniable that health related information is perhaps the most personal, intimate and sensitive information about an individual. The threat to cyber security will not outweigh the whopping benefits of electronic health records if cyber law is strengthened.

The digital model is based on patient's trust and its success is possible only by ensuring informational privacy by the State and other organisations. There shall be a uniform standard that should be mandatorily followed across the country and any violation shall entail strict action. We can adopt the rules of mandatory disclosure of breach and audit trails from the USA Model. Additionally, the breach of data security entails breach of privacy which is breach of fundamental right and should be heavily penalised.

[130] Digital Information Security in Healthcare, Act, 2018 § 29 Cl. 5.
[131] Digital Information Security in Healthcare, Act, 2018 § 34 Cl. 3.

Moreover, on the issue relating to the *Aarogya Setu* app, it has been observed that currently the country lacks a legislative framework to protect the adversities that might occur by the use of a contact tracing app. The failure of the pre-existing legislation to protect personal data has lead the way for introduction of Personal Data Protection Bill which provides a well-built mechanism to prevent the misuse of personal data in the country, by establishing a fiduciary relationship between the data owner and the entity with whom the data is stored or accessed. Furthermore, it categorises personal data in two, to revamp the data management practices and also provides some clarity on the data localization. Unlike the Personal Data Protection Bill, the Digital Information Security in Healthcare Act that specifically deals with the protection and security of digital health data and it narrows down the purposes for which the data can be accessible to the Government, thereby making it a suitable legislation for protecting the healthcare data.