Article

DOI: 10.17803/2713-0533.2024.3.29.452-490

Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India

Niharika Raizada[1], **Pranjal Srivastava**[2]

[1] *CHRIST University, Bengaluru, India*

[2] *Rashtriya Raksha University, Gandhinagar, India*

Abstract: 2021 and 2022 have been the years of frequent cyber-attacks. India remains in the top 25 countries severely affected by the continuous cyber-attacks and tops the list. The healthcare department is amongst the most affected area. In 2020, the healthcare department suffered a severe impact with around 348K cyber-attacks alone on Indian healthcare infrastructure. The recent occurrence of cyber-attack on AIIMS hospital in December 2022 followed by several other incidences of data breaches have made the concerned authorities pro-active on exercising vigilance and reforming the legal and technical system to protect the health infrastructure. This paper has been developed on extensive literature and focuses on describing the nature of electronic health records, the risks they are exposed to along with as to why they are so susceptible to these cyber-risks. Furthermore, the paper also deals with different kinds of threats affecting the privacy and security of electronic health records specifically. The paper analyzes Indian legal framework, briefly compares it with international legal framework (specifically US & EU) and highlights the shortcomings in Indian legislative framework followed by laying down certain recommendations primarily highlighting the possible changes required in Indian legal framework and practices that can be adopted at organizational level to overcome and mitigate such risks.

Keywords*:* cybersecurity; electronic health records (EHR); healthcare; personal health information; cyber-threats

Cite as: Raizada, N. and Srivastava, P., (2024). Cyber-Threat Landscape in Healthcare Industry and Legal Framework Governing Personal Health Information in India. *Kutafin Law Review*, 11(3), pp. 452–490, doi: 10.17803/2713-0533.2024.3.29.452-490

Contents

I. Introduction

With the gradual development of technology and its impact on different kinds of infrastructure in various departments and services, the risks have also gradually increased. The technological progress has led to a constant redefining of daily life. The healthcare department is no exception to this. A dramatic shift from paper records to electronic health records has undoubtedly reduced the workload of the front-line

workers, but it has nevertheless increased the risk of unlawful access to such records. Electronic health records are electronic versions of the medical records stored and organized by the healthcare service providers like hospitals, clinics and the internet of medical things (IoMT). They are the patients' history that can be referred to or interoperate between hospitals (Keshta and Odeh, 2021, p. 177). These include essential administrative as well as the clinical data that basically include the care and services given to an individual by a health provider. These are inclusive of details such as demographics, progress reports, problems, medications, important signs, MRI and CTC scans, medical history, immunization reports, laboratory data, radiology reports, etc. (Keshta and Odeh, 2021, p. 178). These electronic medical records are prone to risks and threats of a number of cybersecurity issues. The report published by QuickHeal Report in 2021[1] highlighted that India has suffered most cyber-attacks along with 24 other countries. The most of the attacks were targeted at hospitals, government and defense bodies. Most of them were malware and ransomware attacks. The malware, often also called as malicious software like Advanced Persistent Threats (APT), often targeted the departments and led to data theft.[2] One of such malware is APT10 that targeted at food processing industries, hospitals, banks, automobile industries. APT10 misled the security community in believing that this was a Transparent Tribe.

Ransomware is a variant of malware itself (Reshmi, 2021). Ransomwares attacks are generally financially motivated (Alder, 2021). This malware gives threat actors a large payout in a matter of days after conducting an attack and ransoms are often paid to allow files to be restored or to prevent the release or sale of stolen sensitive data. Ransomware usually either aims encodes the important file or prevent the users from using the devices by locking them and further demanding the organization to pay ransom in order to retrieve the access (Tully et al., 2020).

The cyber-attacks shot up during the Covid-19 period with several number of cyber-incidents covering areas like spyware attacks (Hakak

[1] Seqrite Annual Threat Report 2021. Available at: https://www.seqrite.com/seqrite-annual-threat-report-2021#dflip-df_book_full/1/ [Accessed 23.03.2024].

[2] Seqrite Annual Threat Report 2021.

et al., 2020), DDOS, ransomware (Muthuppalaniappan and Stevenson, 2021), digital fraud (Škiljić, 2020, p. 52), panic, disinformation, etc. The cyber-incidents levered an approximate cost around in millions and exposing the critical data to the illegal assessors. The data of patients and users of various medical services were accessed without consent and sold to various third parties. However, primary questions here are why would they target the medical data that happens to be a sensitive data (Blessing et al., 2022) and what would hackers do with our data?[3] The answer in brief is the medical infrastructure has an issue of weak cybersecurity and it makes it easier for hackers to commit data theft (Pal et al., 2024). Also, the stolen data is either sold on the deep dark online market which can enable the buyer on the market commit felony cases like tax evasion, identity theft, etc. The importance and the utter necessity of cybersecurity comes into play when the very fact is highlighted that the patient's data stored and compiled as EHRs are often stolen and utilized in identity thefts or more serious offences like tax evasion (Coventry and Branley, 2018, pp. 48–52). There are thousands of malware attacks infecting the databases of the hospitals, laboratories, devices, etc. and gaining the access to our personal data stored, illegally.[4]

This particular research article provides for a detailed explanation on the nature and importance of storing and utilization of health data; highlights the major reasons as to why EHRs serve as honeypot for cybercriminals; explores the different elements involved in cybersecurity and underlying explanations for developing a resilient cybersecurity framework for EHRs; provides thorough analyses of the literature available identifying various forms of cyber-threats that severely affect the privacy and security of the EHRs; encompasses the present cybersecurity measures or laws in India protecting the EHRs succeeded by recommendations that can help in strengthening the overall cyber-infrastructure of the system of healthcare.

[3] Once Stolen, What Do Hackers Do with Your Data? *Secplicity — Security Simplified*. May 18. Available at: https://www.secplicity.org/2017/05/18/stolen-hackers-data/ [Accessed 21.09.2024].

[4] BBC News, (2016). Wiggins and Froome Medical Records Released by "Russian Hackers." *BBC News*. 2016. September 15. Available at: //www.bbc.com/news/world-37369705 [Accessed 23.03.2024].

II. Nature of Electronic Health Records

An EHR can be defined as the electronic version of a medical data of a patient that is stored and maintained by a particular health care provider for a certain period. It includes all the essential administrative and clinical data of the treatment, care and facilities given to an individual, e.g., demographics, progress reports, problems, medications, important signs, medical history, immunization reports, laboratory data and radiology reports. In simpler language, an EHR is an enhanced database prepared with respect to health and healthcare of a patient where all data and essential information is kept on electronic media (Negro-Calduch et al., 2021). EHR has capability of storing sensitive personal data relating to our health and care.

The medical records of a person comprise of the simple demographic records, the chronology of the ailments, any type of medical images, problems, medications, etc. The records of a patient stored in hospitals are essential for the purpose of quick reference and finding remedies for the ailments. The paper records cannot sometimes extensively trace data related to a particular person (Keshta and Odeh, 2021, p. 179), which has led most of the organizations shift their policies of preparing, storing and maintaining of paper medical records to electronic health records. An EHR is an electronic version of a medical data of a patient stored and maintained by a particular health care provider for a certain period. It includes all the essential administrative and clinical data regarding the treatment, care and facilities given to an individual. An EHR is an enhanced database prepared with respect to health and healthcare of a patient where all data and essential information is kept on electronic media (Negro-Calduch et al., 2021). It has a peculiar capability of storing sensitive personal data relating to the patient's health and care.

The EHR was introduced in 1960 (Gajwani, 2020) and it is defined as an electronic record keeping system which not only maintains the records but also enables interoperability and various secondary uses as well. For the first time, the guidelines were introduced in 2013 by Ministry of Health and Family Welfare. The guidelines were amended and developed further in 2016. The document set for EHR Guidelines

was stated to be a *"living document"* on account of reason that *"...These standards cannot be considered either in isolation or as 'etched in stone for all eternity.' These will need to undergo periodic review and update as necessary*."[5]

EHRs have played significant role in making access and sharing of health information easier and accessible. The EHR system is apparently providing better benefits, enhanced productivity in contrast to the traditional paper-based record storing system. The EHR is not limited to the electronic records maintained by the hospitals comprising information only regarding ailment along with the demographic and financial details of the patient; it also extends its area over health records obtained via Internet of medical things, wearable body area network, telemedicine, etc., which makes it easier for the general practitioners to derive a specific conclusion with the help of all relevant information at one place. The digitization of the personal health information has also played a significant role in making the records interoperable, i.e., the records are easily accessible to other departments as well. Interoperability is essential to attain better patient care, better prediction for health of populations and lower costs for healthcare services.

The EHR has a peculiar characteristic as it creates a paradox; health records cannot be shared due to their sensitive nature and it is also required to be shared to enable better results and cheaper costs.[6] Lack of interoperability might lead to restricted comprehension of patient and also collective health of population and will consequently result in higher costs and poor outcomes (Kawu et al., 2023). Interoperability is not just limited to records from the hospitals and clinics. With the advancement of The Internet of medical things and wearable body area network are also connected with the primary EHR/EMR to monitor diseases like hypertension, blood sugar, etc. However, there are certain issues on account of which interoperability of electronic records is not a trend. The records of a patient stored in hospitals are essential for

[5] Electronic Health Records (HER) Standards for India, (2016). Available at: https://bahmni.atlassian.net/wiki/spaces/BAH/pages/2983165963/EHR+Standards+across+various+countries [Accessed 21/09/2024].

[6] What is Interoperability in Healthcare? IBM Report. Available at: https://www.ibm.com/topics/interoperability-in-healthcare [Accessed 23.03.2024].

the purpose of quick reference and finding remedies for the ailments. However, the paper records stored have led to an extensive trail of the data related to particular person (Keshta and Odeh, 2021, p. 180), which has led most of the organizations shift their policies of preparing, storing and maintaining paper medical records to electronic health records.

III. Why Electronic Health Records are being Targeted?

With the enhanced use and advantages of EHR, they are now primary targets for advanced cyber-attacks. Besides, financial institutions and healthcare institutions are now the primary focus for data extortion and theft. Lack of stringent legislation and weak healthcare infrastructure are two chief reasons why healthcare institutions have been lately targeted to launch a cyber-attack. There is no set legal framework to govern compliance with the above-mentioned standards. However, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, were enacted under Information Technology Act, 2000. The rules apply to every "body corporate" concerned with holding and maintaining sensitive records. Besides the above stated rules, there have been several attempts at framing laws that primarily deal with sensitive personal data;[7] however, the solid framework for governing the digital personal and sensitive data is yet to come in force.

The lack of a concrete law makes the electronic health records vulnerable and prone to several issues relating to cyber security like data extortion, identity theft, malware attacks, selling of sensitive records in black market, etc.

The vital question in focus, however, is why anyone would want to steal any health record and what is the significance of a mere record comprising of demographic and health information. Indian healthcare institutions have been subject to nearly 1.9 million cyber-attacks in

[7] Several bills precede the current bill in motion in the Parliament. Bills like Personal Data Protection Bill, 2018; Digital Information in Healthcare Security Act, 2018 and Data Protection Bill, 2019 were prior attempt at making flawless framework for governing of digital health data specifically.

year of 2022 (Ang, 2022) and around millions of records comprising of extremely sensitive information of patients were leaked. The primary motivation behind these cyber-attacks can be outlined around financial gain, political or military advantage (Coventry and Branley, 2018, p. 48). Politically motivated cyber-threats amount to approximately 26 % of the global cyber-attacks (Desjardins, 2018) and such motivation preceded by initiation of any form of threat for spreading propaganda or posing serious threat to national security (Han and Dongre, 2014), e.g., NHS website's control was taken over by cyber-terrorists and pictures of gruesome ongoing civil war in Syria were posted (Sengupta, 2017).

Each electronic health record is sold on dark web for around 1,000 $ USD (Sudhanshu, 2022). A social security number is worth $ 3, while credit card details are worth 15–20 $ (Ibarra et al., 2019, pp. 115–137). On a rough estimate, a particular EHR is sold for over hundreds of dollars over dark web. The electronic records can apparently be (mis) used to either extort money from the victim whose record has been sold illicitly or expose it to public embarrassment and/or political assassination (Ibarra et al., 2019, pp. 115–137). In other scenario, there are also several secondary uses of EHRs; they are also generated and developed in a clinical trial.

A clinical data is generated in the form of in-effect patient diagnostics and consists of extremely private information. It is used for purposes other than medical treatment like medical research, preventive campaigns, establishing national and international statistics, allocation of resources, study epistemological trends (Richter and Thielscher, 2023; Shah and Khan, 2020). Earlier, the diagnosis from any particular clinical trial were stored and maintained in paper records but to enable accessibility and promote better maintenance of all the records, the EHR system was adopted.

Induction of health records into EHR system enables medical researchers to keep track after a drug has been introduced in a drug trial (Shah and Khan, 2020; Adebayo and AbdulAziz, 2014) for the purpose of scientific discovery, for the purpose of conducting observational studies (Hoffman and Podgurski, 2013), to track the effects and focus on quality improvement with the aim of rendering better treatments, (Hoffman and Podgurski, 2013) and also in cases where, if any sensitive or de-

anonymized information of a patient(s) gets public, the EHRs can prove to be rather a fatal legal injury against the person/entity/organization responsible for storing such health records (Howden, 2023, p. 23).

IV. Cybersecurity for Electronic Health Records

Cybersecurity guarantees safety of computer systems and networks against data breach, data theft, information leak or any form of harm to the hardware, software or any form of electronic data and any form of disruption of services. Cybersecurity is one of the most persistent challenges that every corporation working with digital information encounters. Unfortunately, healthcare industry faces several kinds of cyber-threats leading to disruption in functioning of health delivery services. There are several factors in play for such threats like lack of cybersecurity policy, lack of management of proper record, minimal training, education and awareness of staff and personnel about the procedures, etc. (Paliwal et al., 2023, p. 388).

Because of these factors, healthcare cybersecurity is threatened (Pears and Konstantinidis, 2021, p. 1675). Healthcare industry functions as a supply-chain network involving different stakeholders interconnected and exchange data amongst themselves. This data is in form of electronic health record (EHRs) that consists of tons of valuable information of a patient. Any particular EHR comprises of following information:

— Personal information (Name, contact details, details of relatives).

— Demographic details of the patient (residential, permanent address and office address).

— Social security number of the individual (like AADHAR, driving license number).

— Financial details (credit card, bank account details, ATM numbers).

— Medical history or details of ailments or information related to diseases suffered by the individual.

Cybersecurity revolves around three pillars of information security: confidentiality, integrity and availability also known as CIA

Triad (Langer, 2017, pp. 117–125). However, this model of information security (CIA Triad) has been extended to include Accountability as a non-repudiated pillar (Warkentin and Orgeron, 2020). Electronic health records (EHRs) are vulnerable to various cyber-risks that can compromise the confidentiality, integrity, and availability of patient information. Confidentiality refers to protecting the privacy of patient data, ensuring that only authorized individuals have access to it. Integrity involves maintaining the accuracy and trustworthiness of the data, preventing unauthorized modifications or tampering. Availability ensures that the data is accessible to authorized users when needed (Almaghrabi and Bugis, 2022, pp. 126–128). One significant cyber risk to EHRs is the potential for unauthorized access and data breaches. The importance of confidentiality is one of the key security requirements for IoT-based healthcare systems (Nasiri et al., 2019, pp. 253–258). They emphasize the need for measures such as authentication and authorization to ensure that only authorized individuals can access patient data. They also emphasize the importance of confidentiality as one of the ultimate security objectives for healthcare systems (Kawu et al., 2023). They discuss the risks associated with data breaches and the potential harm data breaches can cause to individuals.

Another cyber risk is the threat to the integrity of EHRs that discusses the lack of robust cybersecurity in healthcare, since it can lead to the lack of integrity and security of electronic health records (Yusuf and Ayinde, 2023). It is necessary to prepare a security framework for EHR systems that considers the integrity of health records (Ganiga et al., 2020, p. 455). Enough focus has been laid on the risks posed by ransomware attacks in the healthcare industry (Farringer, 2019, p. 91). The rapid transition from paper records to electronic platforms has increased the risk to patient data integrity. Ransomware attacks can render medical records inaccessible, compromising patient care and privacy. Farringer (2019, p. 91) emphasizes the need for coordinated efforts to address cybersecurity risks in the healthcare industry. The researcher highlighted that concern over cyber-attacks targeting medical information systems is growing. The illegal market for electronic health records has led to an increase in virtual attacks,

posing a threat to the reputation and financial stability of medical institutions. Protecting the network infrastructure that supports healthcare systems is crucial to mitigating these cyber risks (Angel, 2022, p. 3455).

Phishing and ransomware attacks are specific cyber risks that can compromise the integrity and availability of EHRs. Health care organizations are ideal targets for these attacks due to outdated cybersecurity systems and limited staff training on safety practices (Croke, 2020). These attacks can lead to the disclosure of patient health information, identity theft, and medical fraud, highlighting the wide-ranging consequences of cyberattacks in the healthcare sector (Croke, 2020). Availability is also a critical aspect of EHR security. It highlights the need for maintaining the availability of healthcare technology and the confidentiality of health records (Lekshmi, 2022). The unauthorized availability of EHR systems can be compromised and disrupt the functioning of the systems or cause downtime. In the extended version, accountability refers to ensuring traceability of performed activities or processes to specific individual or a group and such processes that cannot be repudiated. Non-repudiation is ensuring that a person cannot deny due to the authenticity of their credentials or any act like sending a message (Anderson, 2003, pp. 308–313).

It is essential to frame a flexible EHR system that ensures availability, confidentiality, and integrity by integrating different hospital information systems (Nielsen et al., 2019, p. 5). One of the key concerns is the security of healthcare data and devices. Increased connectivity to existing computer networks has exposed medical devices to new cybersecurity vulnerabilities (Coventry and Branley, 2018, p. 48). These vulnerabilities can be exploited by cyber attackers to disrupt the availability of EHRs and compromise patient care.

Remote access to EHRs is another cyber risk that can impact availability. With the increasing use of telemedicine, the remote access to electronic medical records of patients has become more widespread, making it a potential target for cyber-attacks (Sardi et al., 2020). Unauthorized access or manipulation of EHRs can lead to disruptions in healthcare services and compromise patient care.

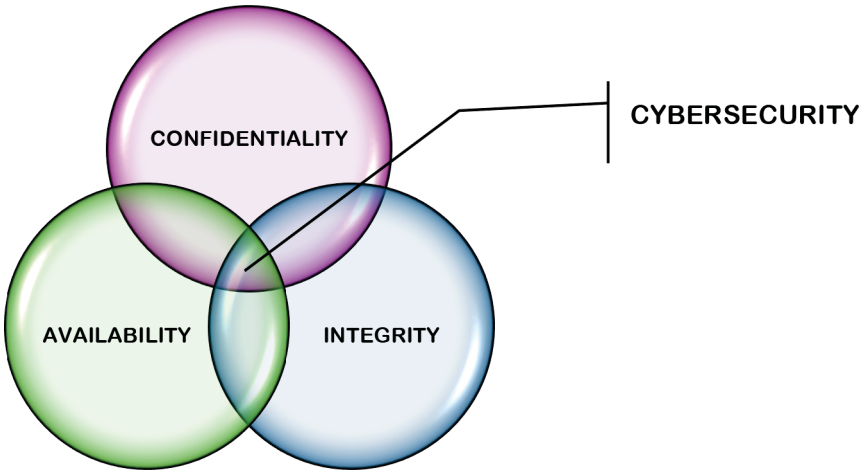

Figure 1. C-I-A Triad

The essence of cybersecurity underlies in the context of understanding what are the risks and vulnerabilities in the network. The cyber-risk has a wide meaning, it has been defined differently by different scholars. To understand what are the kinds of underlying threats to healthcare industry, it is also important to understand what cyber-risks and cyber-vulnerabilities are in healthcare industry.

IV.1. Vulnerability

Vulnerability with respect to cyber-infrastructure refers to internal component of the risk and specifies weakness in a digital system of organization. It refers to circumstances related to fact, processes, people or any phenomenon that can reduce the capacity of the organization to respond, recover and act against a risk or any event which is likely to occur because of such risk (Zodian, 2024, p. 20). Vulnerability refers to a weakness in an asset or in any infrastructure or implementation or operation that can be severely exploited by an adversary (Cox, 2008, p. 1749). Vulnerability can exist in software, hardware or in network (Savin and Anysz, 2021).

IV.2. Cyber Threats

A cyber-threat relates to occurrence of any incident with the capacity to result in loss or damage to asset or individual (Škiljić, 2020, p. 51). A threat can be anything ranging from cyber-attack to sophisticated forms of espionage, data breaches, identity theft, financial fraud, disruption of critical infrastructure. Threat is usually the exploitation of an existing weakness in the organization's infrastructure. The list of sources of threats is not exhaustive; this may include unsanctioned access, lack of cybersecurity policy, lack of awareness and training, information security breach, etc. A threat can emanate from frivolous motive or any act or omission of the perpetrator, which can be intentional or accidental in nature or can be altogether demonstrate perpetrator's incompetence. The origin of a threat can be external or within the organization. A threat does not necessarily should lead to a cyber-incident, if mitigated at an early stage. To analyze risk, threat is based on evaluating the intention and potential of the adverse party to perform a detrimental activity (Strupczewski, 2021, p. 105).

IV.3. Impact/Likelihood

It is significant to estimate potential damage that can be caused by a particular cyber-incident. One needs to take into consideration certain characteristics that are related to information security to ensure and maintain the three angles in CIA Triad. Therefore, careful analysis and evaluation of the organization's information security system should be done with respect to the loss of integrity, availability and confidentiality. The impact/likelihood/probability of occurrence should be analyzed as:

— High: Severely affects the goals and working of the organization.

— Medium: Leads to financial damage and may cause challenges for human resources.

— Low: Causes minor financial losses.

IV.4. Cyber-Risks

Risk is associated with the threat and likelihood of an uninvited incident and its adverse impact. It is a potential incident that can be discovered and quantified; likelihood and impact can be assessed. It

is estimated as the combination of probability and consequence of any hostile event like a threat. When numerical values represent the probability and consequences (impact), the anticipated risk is calculated by multiplying these values, taking uncertainty into account. In the realm of security, risk assessment involves analyzing and aggregating three well-established factors: threat, vulnerability, and consequence. When probability and consequences are quantified, the expected risk is determined by multiplying these numerical values, incorporating considerations for uncertainty. In the context of security, the evaluation of risk involves analyzing and consolidating three widely acknowledged factors: threat, vulnerability, and consequence. This approach provides a comprehensive understanding of potential risks and aids in effective risk management. Risk can be managed by implementation of appropriate controls and different response and recovery strategies that may reduce the likelihood and impact of a threat or an unwanted event (Zahid et al., 2021). Thus, the following equation can be provided for cyber-risks assessment:

Vulnerability × Threat × Impact = Risk

V. Kinds of Cyber-Threats to Healthcare Industry

It is significant to note that although there is an upside to digitization of healthcare industry, the complexity of computing environment makes it easier for cybercriminals to exploit vulnerabilities. Information security incidents that include sensitive health information and different malware attacks on critical services pose incredible danger (Cremer et al., 2022, p. 698). Medical staff can easily access patient information. Offenders can abuse illegally obtained information in several ways, e.g., commission of identity theft, initiate unlawful transactions or even blackmail victims (Martin et al., 2017).

Another possible scenario is installation of a malicious code or committing sensitive credentials. Consequently, the entire network suffers. One of the most frequently occurring incidents is stealing information through genuinely looking websites or emails. The primary element to gain patient confidence is safeguarding the privacy and security of the EHR and personal health information during medical

visits. Healthcare organizations face several cybersecurity issues every year. In the USA approximately 88 % of healthcare organizations have faced some form of cyber-attack usually performed in the form of ransomware attacks, cloud compromise, phishing emails and supply chain attacks (Bhatia, 2022, p. 103). Such cyber-incidents have caused healthcare organizations to suffer losses for more than 100 million $ USD and have also affected the patients or the end-users availing the services. Such incidents have in different ways have also affected confidentiality, integrity and availability of medical information. Some common but severe form of cyber-threats are discussed below in Table 1.

Table 1: Different kinds of cyber-threats

Types of Cyber-Threats	Description
Phishing Attacks (Coventry and Branley, 2018)	Phishing e-mail is the way to gain access to valuable credentials like passwords, medical information, and financial data using targeted communication methods like email or text messages where the prospective victim clicks the link and is directed to malicious code or malware
Remote Desktop Protocol (Thamer and Alubady, 2021)	Remote desktop protocol is copyrighted protocol that provides ability to users to connect to their respective workspace. RDP allows access to managers and employees to their systems from any location. Such remote access is followed by severe vulnerability and can be exploited using brute force attacks to gain valuable credentials like username and passwords
Removable Media and Universal Serial Bus (Thamer and Alubady, 2021)	Removable media and Universal Serial Bus (USB) is a way of externally infiltrating the targeted devices and it is different from attacks based on internet-based
Ransomware (Nusairat et al., 2023, p. 238)	Ransomware is the form of malware that encrypts the recorded information and decryption is only possible after ransom is paid to the perpetrator

DDOS (Argaw et al., 2020, p. 146)	Distributed denial of service attacks floods a particular server with false connection permission to interfere with its working. This coordination utilizes several end-points and IoT devices that by force affects through malware infection through botnet
Internal Threats (Javaid et al., 2023)	Insider threats are security risks arising from individuals within an organization exploiting privileged access to compromise information security intentionally or inadvertently
Breach of Data (Javaid et al., 2023)	Data breach incidents are no usually the result of form risk however they can be consequence of any malware, insider attacks or compromised emails

VI. Legal and Regulatory Framework for Protection of Electronic Health Records

The peculiar sensitive nature of digital health information is known internationally in order to ensure that data is protected specifically (Kaplan, 2014). It is essential to prevent privacy from being infringed in order to utilize for better prospects like patient care, progressive public health and research purposes (Price et al., 2019, p. 448). The present legal framework and regulatory measures in India do neither. These legal instruments were not brought in force for the purpose to promote the progressive research and improve public health. Instead, they are established for obsolete and redundant technologies (Kaplan, 2020). As the technology upgrades, data gathered for certain purpose may become interdependent with other kind of data and the basic notion of privacy may also evolve gradually with time, which may render a particular law that may be not completely obsolete but definitely inadequate and having several loopholes.

Furthermore, we know little about how data are collected, generated, combined, used, and protected, as well as about the specific algorithms that collect, process, and use it. For example, communication companies track users' locations and personal contact data, which can inadvertently reveal sensitive health information. In the United States, as in many other countries, privacy regulation often relies on de-identification to

preserve privacy, particularly under laws like HIPAA and the Common Rule. However, this approach only covers certain types of data. With advancements in data analysis, re-identifying de-identified data has become increasingly feasible, rendering de-identification an inadequate legal protection in many cases.

This part of the article will highlight legal and regulatory issues in the existing legal framework.

Issues in Legal and Regulatory Framework. The threats and risks as provided in 5th section of this paper have not been discussed or mentioned precisely in the Indian legal framework that comprises legislations, policies and guidelines. Information Technology Act, 2000, is the primary Indian legislation that governs protection of data and individual's privacy relating to their health data and medical records.

VI.1. Primary Legislations and Policies

VI.1.1. Information Technology Act, 2000

Information Technology Act, 2000[8], is a comprehensive legislation focused on governance of several different electronic transactions and interchange electronic data. The Act came into force on 9 June 2000 and specified in its Preamble that it is "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." IT Act provides for several offences (20021 § 43A). Under Chapter IX, however, the Act does not specifically deal with data breach or cyber-attack. The Act provides for compensation on part of the body corporate on account of failure to protect sensitive data from being stolen or unlawfully accessed (Information Technology Act, 2000, 21 § 43A) The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, is one of the corresponding rules that aim at explicit protection of sensitive personal

[8] Available at: https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf [Accessed 21.09.2024].

data and information and these Rules are supposed to be read with Section 43A (Information Technology, 200021 21 § 43A).

Rule 3 of the IT Rules, 2011 (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules, Part II-Sec. 3(i) § Rule 3, 2011) 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, do not provide for specific provisions and classification of health and medical data and kinds of data constituting health data. Furthermore, the Rules have major application to body corporate only and not to other organizations or individuals. Consequently, there will not be any imposition of compensation on individuals or other organizations that are not within the ambit of "body corporate."[9]

VI.1.2. Electronic Health Records Standards, 2016

Electronic Health Records Standards, 2016[10] provides for extensive standards that specifically apply on healthcare institutions or anybody, which lead to creation of medical history and record. In a way, EHR

[9] Information Technology Act, 21 § 43A Explanation.

[10] Electronic Health Records Standard (Q-11011/3/2015-eGov). Available at: https://main.mohfw.gov.in/sites/default/files/17739294021483341357.pdf [Accessed 21.09.2024].

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, are used not only for protection of sensitive data but also for maintenance, sharing or enhancing of 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. Most importantly, they define and differentiate in an elaborate manner between "Electronic Health Record (EHR)," "Electronic Medical Records" (EMR), "Electronic Personal Health Information" (E-PHI) and "Personal Health Record" (EPR).

a. Electronic Health Record

An 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."[11]

b. Electronic Medical Record

An EMR has been defined as a varied form of EHR "restricted in scope to the medical domain or at least very much medically focused."[12]

c. Electronic Personal Health Information

E-PHI has been defined as any protected health information that has been "created, stored, transmitted, or received electronically" (Savin and Anysz, 2021). 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.[13]

The EHR Standards, 2016 is a comprehensive document but lacks enforceable character due to unavailability of such provision. Subsequently, due to lack of enforceability, the application and the

[11] Electronic Health Records Standard (Q-11011/3/2015-eGov).

[12] Electronic Health Records Standard (Q-11011/3/2015-eGov).

[13] Electronic Health Records Standard (Q-11011/3/2015-eGov).

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.

VI.1.3. The Digital Data Protection Act, 2023

The Digital Data Protection Act, 2023 (DPDA) is a comprehensive proposed legislation for the governance of the personal digital data. It states, "The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto."[14] The consent of an individual is supposed to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose."[15] The consent sought should be followed by conveying all the relevant information describing the purpose of processing such data.[16] Section 7 stipulates that data so processed is "for legitimate purposes" along with the condition that Data Principal has willingly provided the personal data and "has not indicated to the Data Fiduciary that she does not consent to its use." Besides, data fiduciary can also process medical data of data principal in two other scenarios:

a. for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;[17]

b. 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.[18]

[14] DPDA, 2023, CG-DL-E-12082023-248045 22 of 2023. § Preamble, 2023.
[15] DPDA, 2023, § 6, 2023.
[16] DPDA, 2023, § 5, 2023.
[17] DPDA, 2023, § 7 (f), 2023.
[18] DPDA, 2023, § 7(g), 2023.

Section 2(s) of DPDPA provides additional provision for "Significant Data Fiduciary."[19] A significant data fiduciary is a "Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under Section 10."[20] A significant data fiduciary is appointed by Central Government on the basis of different factors including:

a. the volume and sensitivity of personal data processed;
b. risk to the rights of Data Principal;
c. potential impact on the sovereignty and integrity of India;
d. risk to electoral democracy;
e. security of the State; and
f. public order.[21]

The relevant provisions do not provide for privacy, security and confidentiality of health data specifically and most importantly, it does not define sensitive personal data nor differentiate between sensitive and non-sensitive personal data. Consequently, there are no provisions for regulation of the same. The Digital Personal Data Protection Act, 2023 ensures that personal data is processed only after consent and for legitimate uses.[22]

VI.2. Regulatory Framework

VI.2.1. National Digital Health Ecosystem, 2019

National Digital Health Ecosystem, 2019 (NDHE) is a framework developed for easier interchange of health data between health service providers and stakeholders. NDHE developed overtime since 2019 to National Digital Health Blueprint (NDHB) in 2020 and finally rolled out as Ayushman Bharat Digital Mission (ABDM) in 2020 in 6 Union territories on 15 August (National Heath Mission, 2022). ABDM has 5 major components: ABHA Number, UHI interface, Health Professional Registry, Health Facility Registry and ABHA Mobile App (PHR app). ABDM provides for data exchange between all of these components for it primary objective of enhancing interoperability and reducing

[19] DPDA, 2023, § 2, 2023.
[20] DPDA, 2023, § 2, 2023.
[21] DPDA, 2023, § 10(1), 2023.
[22] DPDA, 2023, § 4 Preamble, 2023.

paper health records. Such interchange is governed by guidelines and policies brought out in public with ABDM framework, of which the most relevant here is Health Data Management Policy (HDMP) that provides for several aspects of data exchange along with how health data is supposed to be exchanged in a safe and confidential manner only after explicit consent of the patient.

However, it is noteworthy that such a policy document is not rolled out as an obligation thereby limiting the benefits. Furthermore, the ABDM is defined as a framework and does not possess mandatory force over private hospitals, clinics or laboratories. The framework requires an enforcing Act or provision.

VI.2.2. National Cybersecurity Policy, 2013

National Cybersecurity Policy, 2013 (NCP) is a comprehensive document that enables different businesses, citizens and government bodies to establish a resilient and secure cyber ecosystem. The NCP 2013 aims to achieve the following objectives:

1. To establish a resilient cyber-ecosystem and develop trust and confidence in IT systems and transactions which take place in a cyberspace.

2. To formulate framework to design security policies and promote and enable global security compliant standards and practices.

3. To establish a stringent regulatory framework to ensure a protected cyber ecosystem.

4. To establish and develop machinery to obtain significant information with reference to risks to ICT infrastructure, creation of solutions for response, risk management and assessment procedures by way of "predictive, preventive, protective, response and recovery actions."

5. To enhance protection of critical infrastructure and establish a 24 × 7 National Critical Information Infrastructure Protection Centre and mandate security and privacy practices.

6. To introduce and develop technologies for purposes of National Security.

7. To improve transparency and integrity of different technologically connected products and services by developing systems for testing and validation of security.

8. To upscale the number of professionals in cybersecurity.

9. To ensure fiscal benefits for organizations adopting security standards and practices.

10. To reduce economic losses due to cybercrimes and data theft by protecting information.

11. To enact an efficient prosecution and investigation of cybercrimes through legislative intervention.

12. To enable cybersecurity culture and privacy enabled responsible behavior.

13. To develop public-private partnerships.

14. To promote and develop global cooperation towards furthering the cause of security in cyberspace.

15. To establish such mechanisms which provide for early warnings, risk and response management.

16. To formulate a framework for assessment for conformance and compliance certification to best cyber practices and policies.

17. To reduce of supply chain risks in cyber infrastructure.

It is relevant here to know that National Cybersecurity Policy, 2013 is a comprehensive document but it does not introduce provisions mandating organizations and corporations to establish an internal policy in compliance with the NCP, 2013. Besides this, the policy is more like a guiding stick in the dark and developing room of technology that will turn obsolete in coming time. Moreover, the policy does not introduce any rights and/or obligations for a data owner or consent. Even though it is a holistic framework having preventive characteristics, it does not cover enough area to protect sensitive data.

VII. Indian Judiciary and Digital Privacy

In India, a definition of privacy has been framed by both Indian Judiciary and the Legislature. After a review of literature discussing different aspects of privacy, it can be laid down that in Indian Scenario privacy can be subjectively categorized into four aspects: a. privacy and

press freedom; b. privacy and surveillance; c. privacy and decisional autonomy; and d. informational privacy. However, we will be discussing all of them briefly but our primary focus is laid upon information privacy. Freedom of expression has been enshrined as a constitutional and fundamental right in India under Art. 19 of the *grundnorm*. The right to privacy has also been given a status of a fundamental right under Art. 21(15).

The conflict situation was laid rest by the Supreme Court in case *R. Rajagopala v. State of Tamil Nadu* (1994).[23] The Honorable Supreme Court highlighted that only private and confidential information related to national security shall remain out of the ambit of right to information.

The second aspect of privacy — surveillance — has been lately the most discussed part of privacy. With recent upsurge in technology and public policies, surveillance especially by the state has been in focus because it leads to gross violation of digital and manual privacy.

In India, privacy has been claimed in two aspects, in property and in communications. However, in earlier times, the notion of privacy did not hold a significant status in the eyes of law. The concept of privacy was denied the status of fundamental right in *M.P. Sharma v. Satish Chandra* (1954)[24] and *Kharak Singh v. State of Punjab* (1977).[25]

In Kharak Singh case (1977), surveillance related constitutional claim of privacy was challenged, and the concept of privacy was acknowledged. In: Kharak Singh (1977), the court was not concerned with the concept of privacy for a while; however, in the next case *R.M. Malkani v. State of Maharashtra* (1972) the Apex Court held that attaching a recording device to a telephone line did not violate Section 25 of the Telegraph Act. Even though the judicial pronouncement was related to admissibility of evidence but the Honorable Supreme Court denied the privacy claim based on Art. 21. Subsequently, case *Gobind v. State of Madhya*

[23] R. Rajagopal v. State of Tamil Nadu (no date) Global Freedom of Expression. Available at: https://globalfreedomofexpression.columbia.edu/cases/r-rajagopal-v-state-of-t-n/ [Accessed 21.07.2024].

[24] M.P. Sharma vs Satish Chandra (1954). Available at: https://indiankanoon.org/doc/1306519/ [Accessed 21.09.2024].

[25] Kharak Singh vs The State Of, U.P. & Others (1962). Available at: https://indiankanoon.org/doc/619152/ [Accessed 21.09.2024].

Pradesh (1975), similar to case of Kharak Singh (1977), involved police visits at the personal property of a history-shelter. The court in this case inclined towards recognizing and determining the right to privacy as the constitutional and a fundamental right under Art. 21 but instead declared privacy, a right subject to "compelling state interest". The right to privacy was finally given the status of fundamental right in *K.S. Puttuswamy v. Union of India* (2018)[26] where it overruled both MP Sharma (1954) and Kharak Singh (1977).

The Puttuswamy case (2018) put forth a three-tier test to check whether a legislation infringes the right to privacy. The first tier is concerned with legality, the second is concerned with requirement, i.e., legitimate objective to enact that particular law and lastly, the third tier involves proportionality where the burden is on the state to highlight the legitimate aim supposed to be achieved. In addition to this, the Puttuswamy judgment also highlighted that "privacy is not surrendered just because an individual is in public sphere." The court asserted that privacy is an inherent part of living a life with dignity.

The right to privacy was given the status of fundamental right in *K.S. Puttuswamy v. Union of India* (2018) where it overruled both *MP Sharma* (1954) and *Kharak Singh* (1977). *The Puttuswamy case* (2018) put forth a three-tier test to check whether a legislation infringes the right to privacy. The first tier is concerned with legality, the second is concerned with requirement, i.e., legitimate objective to enact that particular law and lastly, the third tier of proportionality where the burden is on the state to highlight the legitimate aim supposed to be achieved. In addition to this, the Puttuswamy judgment also highlighted that "privacy is not surrendered just because an individual is in public sphere." The court asserted that privacy is an inherent part of living a life with dignity.

Regardless of this judgment, privacy does not have a status of an absolute right. In 2018, the Apex Court laid down in Puttuswamy (II) that AADHAR Act was not unconstitutional and and it was invalid since

[26] Justice, K.S. Puttaswamy (Retd) vs Union Of India (2018). Available at: https://indiankanoon.org/doc/127517806/ [Accessed 21.09.2024].

the intrusion of privacy is proportional to the objective of the legislation. The judgment laid down in 2018 was formed based on 2017 decision.

In Puttuswamy (II) (2018), Justice Sikri laid down a four-pronged test to confirm proportionality of the legislation. The first prong means ensuring that a provision restricting a right must be legitimate; secondly, such provision must be appropriate for furthering the concerned goal; thirdly, there must be another alternate remedy available; and lastly, the provision should not disproportionately affect the owner of the right. Upon analysis of constitutional validity of AADHAR Act on the above four parameters, the majority inclined towards upholding the constitutional validity of the Act and barred some of its provisions. The court held that AADHAR, being a unique and biometric identity system, is effective and meets with the conditions of necessity. Thus, they are constitutional.

The issue regarding privacy in healthcare was also brought up in *Mr. X v. Hospital Z* (1998) where Mr. X was diagnosed with HIV+ when donated blood. It was alleged that unauthorized disclosure of his positive result of his ailment by the hospital led to Mr. X's marriage and seeking legal course. The court held that doctors are obliged with the irrefutable duty to maintain confidentiality of their patients. However, the court asserted, "public interest would override the duty of confidentiality, specifically where there is an immediate or future health risk to others." In this situation, there was an inherent risk to the health of the woman Mr. X was going to marry.

It is important to note that, although the Right to Privacy has been given the status of a fundamental right under Art. 21, such a status is not absolute. On the contrary, it is a qualified right. It is subject to certain restrictions and such restrictions vary case to case. Furthermore, the concerns related to digital health information still remain unaddressed by Indian Judiciary. The AADHAR judgment (Puttuswamy (II) (2018)) though it addresses the concerns relating to biometric identity and upholds the protection of digital data privacy, the lack of consideration towards digital health information may lead to higher instances of violation of the confidentiality of health data.

VIII. Overview and Comparative Analysis of the Legal Systems in India, the European Union, and the United States

Upon analysis of Indian legal and regulatory framework, it can be stated that Indian legal framework suffers from several shortcomings. An assessment of legal framework implemented in International counterparts, primarily United States and European Union, will provide an overview of provisions that can also be incorporated in Indian legal regime. The comparative assessment of Health Insurance Portability and Accountability Act, 1996 enforced in the U.S. and General Data Protection Regulation applicable to member states of European Union with Digital Personal Data Protection Act, 2023 and Information Technology Act, 2000 currently in force in India will provide a comprehensive view of provisions primarily dedicated to protection of personal health information.

The landscape of health data protection and privacy regulations varies significantly across different jurisdictions, with notable differences between Health Insurance Portability and Accountability Act, 1996 (HIPAA — United States), General Data Protection Regulation (GDPR- European Union), the Information Technology Act, 2000 & Information Technology Rules, 2011 (India), and the Digital Personal Data Protection Act, 2023 (India). Each framework offers a distinct approach to handling health data, consent, data breach notifications, and the rights of data subjects.

HIPAA is a robust framework specifically addressing the protection of health information in the United States. It provides comprehensive definitions of health information, including requirements for safeguarding electronic protected health information (ePHI) and restrictions on its use and disclosure. These provisions ensure that health data remains confidential and secure, with specific guidelines on how such data can be used and shared. HIPAA's stringent rules highlight its focus on maintaining the privacy and security of health information, making it a cornerstone of health data protection in the U.S.

In contrast, the European Union's GDPR includes provisions for the protection of health data under its broader data protection framework. GDPR recognizes the sensitive nature of health information and provides

it with special protection, mandating that such data be processed only under stringent conditions. Explicit consent from the data subject is often required, and GDPR outlines detailed requirements for obtaining and managing this consent. This regulation ensures that individuals are fully aware of how their health data will be used and have the right to withdraw consent at any time, reflecting the EU's strong emphasis on individual privacy rights.

India's Information Technology Act and the Digital Personal Data Protection Act (DPDP Act) differ significantly from HIPAA and GDPR. These acts lack explicit provisions specifically tailored to the protection of health data. While they cover aspects of data protection more broadly, they do not offer the detailed and specialized regulations concerning health information found in HIPAA and GDPR. This gap indicates a less comprehensive approach to health data protection in India, where the focus is more on general data protection principles rather than specific health data regulations.

Consent is another critical area where these frameworks differ. GDPR and the DPDP Act emphasize obtaining explicit, informed, and unambiguous consent from data subjects for processing personal data. GDPR, in particular, outlines detailed requirements for consent, ensuring that data subjects are fully informed and have control over their data. The DPDP Act aligns with these principles, emphasizing clear and affirmative consent from individuals. HIPAA, while not focusing explicitly on consent in the same way, requires detailed authorizations for the use and disclosure of protected health information, particularly for uses beyond treatment, payment, or healthcare operations.

Data breach notification requirements also vary. Both GDPR and HIPAA mandate specific obligations for organizations to notify supervisory authorities and affected individuals in the event of a data breach. These requirements ensure transparency and accountability, providing clear guidelines on how to handle data breaches. In contrast, the Information Technology Act and the DPDP Act lack detailed provisions for breach notifications. While they include broader data security provisions, they do not have the specific and stringent requirements for notifying breaches comparable to GDPR and HIPAA.

The rights of data subjects form another area of divergence. GDPR and the DPDP Act grant extensive rights to data subjects, including the right to access, rectification, erasure, and the right to object to processing. These rights empower individuals to have significant control over their data. HIPAA provides certain rights related to accessing and amending health information but does not offer the same level of granularity as GDPR and the DPDP Act. The Information Technology Act does not specifically outline detailed rights for data subjects, lacking the specific procedures and protections found in GDPR and the DPDP Act.

IX. Conclusion and Suggestions

Health data privacy is an extremely important aspect of Electronic Health Records. EHRs carry vital medical information of an individual that may turn out to be dangerous if not recorded, stored and protected carefully. Currently, there are numerous risks and threats developing every day and the current legislation governing privacy of data of any kind in India are not specifically framed to deal with privacy, confidentiality and security of medical records, thereby rendering EHRs susceptible to high level risks and threats, one of which is a cyber-attack. A cyber-attack is not a merely fictitious event anymore; the incidences are occurring frequently and a legal machinery to handle such incidences is not properly equipped with requisite provisions.

If one takes a look at the IBM report, India has suffered the loss of 2.18 million USD in the year 2023 alone and 2.23 million USD in 2022 (Raizada and Biswal, 2024). Furthermore, an authorized government body responsible to deal with such occurrences is CERT-IN established under Section 73 of the Information Technology Act, 2000 in 2004 set up to prevent cyber-attacks, issue guidelines, advisories and enforce emergency measures as well. However, it is also important to note that guidelines, advisories issued by CERT-IN do not possess enforcing characteristics.

The legislative measures that have been introduced through the new Digital Data Protection Bill last year also do not consist of provisions directed at protection of health data specifically, nor it have been addressed in the current legislation, i.e., Information Technology Act,

2000 or succeeding Amendment in 2008. Recurring attacks, threats and risks are putting our health data at stake and lessons must be learnt not only from the recent cyber-attack on All India Institute of Medical Sciences hospital or Indian Council for Medical Research database but subsequent incidences occurring internationally as well.

Another step can be taken towards bringing in the private practitioners, clinics, laboratories and health service providers within the ambit of regulatory frameworks like Ayushman Bharat Digital Mission (India's own digital health architecture). Furthermore, the country's policies require not just punitive but a preventive legislation as well, which can be attained through making provisions of Electronic Health Records Standards, 2016 mandatory for all health service providers including private sector. Besides legal machinery, there is also an utmost necessity of training among clinicians and law enforcement personnel to be aware of issues concerning cybersecurity and procedure thereby required to be complied with in case of occurrence of such event.

The absence of provisions of sensitive records database management has made it only harder to achieve the primary objective of protecting privacy individual's data. To address different types of cyber-risks, various approaches can be taken. They can emphasize the need for security, privacy, and confidentiality in electronic health information systems (Jayawardena, 2013).

They may help in highlighting the vulnerability of EHRs to unauthorized access and misuse of sensitive information and suggest investing time and resources in maintaining cybersecurity and ensuring the confidentiality of health records (Iasiello, 2013).

The blockchain technology is also proposed as a solution to enhance the security of EHRs. The use of blockchain-enabled EHRs provides patients with traceable, trustworthy, and secure ownership over their medical data (Rai, 2022). Cyber-risks to electronic health records pose significant threats to the confidentiality, integrity, and availability of patient information. Measures such as authentication, authorization, encryption, and the use of technologies like blockchain can help mitigate these risks and ensure the security of EHRs. Technology is now undergoing rapid upgrades and is developing every single minute. Threats are inevitable, so at the very least the entities

responsible for recording, storing and protecting data should be well equipped and properly made aware of the technicalities in order to avoid such encounters. Furthermore, cybersecurity is not a destination or a milestone; it is a continuous process that requires constant development and evolution to keep up with the changing dynamics of digital health.

Now with the healthcare organizations outsourcing most of their services, cybersecurity needs to be considered as another important aspect of security for healthcare organizations. Several steps are required to be adopted and practiced in consonance with other significant activities. Healthcare organizations can adopt different initiatives to minimize numerous forms of cyber-risks and threats. The list of steps is not exhaustive but can be a rewarding initiative towards protection of patient privacy.

1. Establishing Cybersecurity Policies

In the aspect of health data, cybersecurity policies and regulations differ for each organization. Policies are supposed to be flexible and constantly adapt the changing circumstances. This should include protocols related to data encryption, access controls, functions related to communication, leadership and organizational commitments, and other risk management frameworks it adopts.

2. Proper Allocation of Resources

Proper allocation of resources is critical for maintenance of a robust cybersecurity in health information management system. It includes proper investment in innovative technologies and solutions, constant updating of software and ensuring skilled personnel. Furthermore, funding plays a significant role in adoption of security measures, establishing firewalls, detection systems, etc.

3. Education and Awareness

Education and awareness plays a significant role in forming an indispensable fortress for patient privacy. It is crucial to communicate employees about sensitivity of health information and potential risks associated with it. Various education and informative sessions should be organized by the organizations and employee enrollment should be compulsory. Such sessions will develop a culture for cybersecurity awareness and reduce likelihood of different events that could harm the digital infrastructure.

4. Training of Personnel

Proper training and skill development of employees working with the digital health system is necessary. Training of individuals who regularly deal with patient data should be trained to recognise and mitigate different threats like phishing attacks, ransomwares, etc. Employees should understand the significance of password hygiene and established protocols. It is an ongoing process and staff should be updated on evolving threats and practices.

5. Maintenance of Employee Records

Employee records support in maintaining track of personnel authorized to access sensitive information. A proper account for employees with their authorized access rights should be formed and continuously maintained. It is essential for ensuring cyber-resilience in health data management.

6. Adherence to Related Laws

Strict compliance to respective laws actually aids organizations to mitigate accountability issues in case of a breach. European Union's General Data Protection Regulation (GDPR) and US' Health Insurance Portability and Accountability Act lay down crucial aspects of patient privacy and security practices to be mandatorily adopted by the healthcare organizations. Similar obligations should be obligated under relevant laws of the jurisdiction in which healthcare organizations lie.

References

Adebayo, O.S. and AbdulAziz, N., (2014). An Intelligence Based Model for the Prevention of Advanced Cyber-Attacks. *The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M)*, pp. 1–5, doi: 10.1109/ICT4M.2014.7020648.

Alder, S., (2021). Healthcare Industry Cyberattacks Increase by 45 %. *The HIPAA Journal*. January 6. Available at: https://www.hipaajournal.com/healthcare-industry-cyberattacks-increase-by-45/ [Accessed 23.03.2024].

Almaghrabi, N.S, and Bugis, B.A., (2022). Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature.

Dr. Sulaiman Al Habib Medical Journal, 4(3), pp. 126–135, doi: 10.1007/s44229-022-00016-9.

Anderson, J.M., (2003). Why We Need a New Definition of Information Security. *Computers & Security*, 22(4), pp. 308-313, doi: 10.1016/S0167-4048(03)00407-3.

Ang, A., (2022). 1.9 Million Cyberattacks against Indian Healthcare Recorded in 2022. *Healthcare IT News*. December 5. Available at: https://www.healthcareitnews.com/news/asia/19-million-cyberattacks-against-indian-healthcare-recorded-2022 [Accessed 21.09.2023].

Angel, D., (2022). Protection of Medical Information Systems against Cyber Attacks: A Graph Theoretical Approach. *Wireless Personal Communications*, 126(4), pp. 3455–3464, doi: 10.1007/s11277-022-09873-x.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., et al., (2020). Cybersecurity of Hospitals: Discussing the Challenges and Working towards Mitigating the Risks. *BMC Medical Informatics and Decision Making*, 20(1), p. 146, doi: 10.1186/s12911-020-01161-7.

Bhatia, D., (2022). A Comprehensive Review on the Cyber Security Methods in Indian Organisation. *International Journal of Advances in Soft Computing and Its Applications,* 14(1), pp. 103–124, doi: 10.15849/IJASCA.220328.08.

Blessing, G., Azeta, A., Misra, S., Osamor, V.Ch., Fernandez-Sanz, L. and Pospelova, V., (2022). The Emerging Threat of Ai-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence,* 36(1), pp. 1–34, doi: 10.1080/08839514.2022.2037254.

Coventry, L. and Branley, D., (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. *Maturitas*, 113, pp. 48–52, doi: 10.1016/j.maturitas.2018.04.008.

Cox, Jr, L.A., (2008). Some Limitations of "Risk = Threat × Vulnerability × Consequence" for Risk Analysis of Terrorist Attacks. *Risk Analysis*, 28(6), pp. 1749–1761, doi: 10.1111/j.1539-6924.2008.01142.x.

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Stefan Materne, S., (2022). Cyber Risk and Cybersecurity: A Systematic Review of Data Availability. *The Geneva Papers on Risk*

and Insurance — Issues and Practice, 47(3), pp. 698–736, doi: 10.1057/s41288-022-00266-6.

Croke, L., (2020). Protecting Your Organization from E-mail Phishing and Ransomware Attacks. *AORN Journal*, 112(4), doi: 10.1002/aorn.13229.

Desjardins, J., (2018). Why Hackers Hack: Motives Behind Cyberattacks. *Visual Capitalist*. January 3. Available at: https://www.visualcapitalist.com/hackers-hack-motives-behind-cyberattacks/#google_vignette [Accessed 21.09.2024].

Farringer, D.R., (2019). Maybe if We Turn it off and then Turn it back on again? Exploring Health Care Reform as a Means to Curb Cyber Attacks. *Journal of Law, Medicine & Ethics*, 47(S4), pp. 91–102, doi: 10.1177/1073110519898046.

Gajwani, A., (2020). Electronic Health Records and Data Privacy Regimes in India. *iPleaders*. November 28. Available at: http://blog.ipleaders.in/electronic-health-records-data-privacy-regimes-india/ [Accessed 21.09.2024].

Ganiga, R., Pai, R.M., Manohara Pai, M.M. and Sinha, R.K., (2020). Security Framework for Cloud Based Electronic Health Record (Ehr) System. *International Journal of Electrical and Computer Engineering (IJECE),* 10(1), pp. 455–466, doi: 10.11591/ijece.v10i1.pp455-466.

Hakak, S., Khan, W.Z., Imran, M., Choo, K-K.R. and Shoaib, M., (2020). Have You Been a Victim of Covid-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. *IEEE Access*, 8, pp. 124134–124144, doi: 10.1109/ACCESS.2020.3006172.

Han, Ch. and Dongre, R., (2014). Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10), pp. 40–42, doi: 10.22215/timreview/838.

Hoffman, Sh. and Podgurski, A., (2013). The Use and Misuse of Biomedical Data: Is Bigger Really Better? Faculty Publications, January, pp. 497–538. Available at: https://scholarlycommons.law.case.edu/faculty_publications/606 [Accessed 21.09.2024].

Howden, E., (2023). Retaining and Destroying Patient Records. *BDJ Team,* 10(1), p. 23, doi: 10.1038/s41407-023-1712-x.

Iasiello, E., (2013). Cyber Attack: A Dull Tool to Shape Foreign Policy. *2013 5th International Conference on Cyber Conflict (CYCON 2013)*,

pp. 1–18. Available at: https://ieeexplore.ieee.org/document/6568392 [Accessed 21.09.2024].

Ibarra, J., Jahankhani, H. and Kendzierskyj, S., (2019). Cyber-Physical Attacks and the Value of Healthcare Data: Facing an Era of Cyber Extortion and Organised Crime. In: Jahankhani, H., Kendzierskyj, S., Jamal, A., Epiphaniou, G. and Al-Khateeb, H., eds, (2019). *Blockchain and Clinical Trial: Securing Patient Data*. Cham: Springer International Publishing, doi: 10.1007/978-3-030-11289-9_5.

Javaid, M., Haleem, A., Singh, R.P. and Suman, R., (2023). Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends. *Cyber Security and Applications,* 1, 100016, doi: 10.1016/j.csa.2023.100016.

Jayawardena, A.S., (2013). A Systematic Literature Review of Security, Privacy and Confidentiality of Patient Information in Electronic Health Information Systems. *Sri Lanka Journal of Bio-Medical Informatics*, 4(2), p. 25, doi: 10.4038/sljbmi.v4i2.5740.

Kaplan, B., (2014). How Should Health Data Be Used? Privacy, Secondary Use, and Big data Sales. *Yale University Institute for Social and Policy Studies Working Paper No. 14-025, Cambridge Quarterly of Healthcare Ethics,* 25(2), 312–329, doi: 10.2139/ssrn.2510013.

Kaplan, B., (2020). Seeing through Health Information Technology: The Need for Transparency in Software, Algorithms, Data Privacy, and Regulation. *Journal of Law and the Biosciences*, 7(1), lsaa062, doi: 10.1093/jlb/lsaa062.

Kawu, A.A., Hederman, L., Doyle, J. and O'Sullivan, D., (2023). Patient Generated Health Data and Electronic Health Record Integration, Governance and Socio-Technical Issues: A Narrative Review. *Informatics in Medicine Unlocked*, 37, 101153, doi: 10.1016/j.imu.2022.101153.

Keshta, I. and Odeh, A., (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal,* 22(2), pp. 177–183, doi: 10.1016/j.eij.2020.07.003.

Langer, S.G., (2017). Cyber-Security Issues in Healthcare Information Technology. *Journal of Digital Imaging*. 30(1), pp. 117–125, doi: 10.1007/s10278-016-9913-x.

Lekshmi, A.S., (2022). Growing Concern on Healthcare Cyberattacks & Need for Cybersecurity. Preprint. Available at: https://

www.researchgate.net/publication/357753537_Growing_Concern_on_Healthcare_Cyberattacks_Need_for_Cybersecurity [Accessed 21.09.2024].

Martin, G., Kinross, J. and Hankin, Ch., (2017). Effective Cybersecurity Is Fundamental to Patient Safety. *The British Medical Journal*, 357, j2375, doi: 10.1136/bmj.j2375.

Muthuppalaniappan, M. and Stevenson, K., (2021). Healthcare Cyber-Attacks and the Covid-19 Pandemic: An Urgent Threat to Global Health. *International Journal for Quality in Health Care: Journal of the International Society for Quality in Health Care,* 33(1), mzaa117, doi: 10.1093/intqhc/mzaa117.

Nasiri, S., Farahnaz, S., Tadayon, M. and Dehnad, A., (2019). Security Requirements of Internet of Things-Based Healthcare System: A Survey Study. *Acta Informatica Medica*, 27(4), pp. 253–258, doi: 10.5455/aim.2019.27.253-258.

Negro-Calduch, E., Azzopardi-Muscat, N., Krishnamurthy, R.S. and Novillo-Ortiz, D., (2021). Technological Progress in Electronic Health Record System Optimization: Systematic Review of Systematic Literature Reviews. *International Journal of Medical Informatics*, 152, 104507, doi: 10.1016/j.ijmedinf.2021.104507.

Nielsen, M., Saavedra, A., Villarreal, V., Muñoz, L. and Castillo, Y., (2019). Flexehr: Proposal of a Platform for Interoperability between Information Systems Based on Electronic Medical Records in Panama. *Proceedings of the 13th International Conference on Ubiquitous Computing and Ambient Intelligence UCAmI 2019*, 31(1), 5, doi: 10.3390/proceedings2019031013.

Nusairat, T., Saudi, M.M. and Ahmad, A.B., (2023). A Recent Assessment for the Ransomware Attacks against the Internet of Medical Things (Iomt): A Review. *2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE)*, pp. 238–242, doi: 10.1109/ICCSCE58721.2023.10237161.

Pal, P., Sahana, B.C. and Poray, J., (2024). Secure electronics medical infrastructure for healthcare 4.0: a voice identity management-based approach. *Procedia Computer Science*, 235, pp. 468–477, doi: 10.1016/j.procs.2024.04.046.

Paliwal, S., Parveen, S., Singh, O., Alam, A. and Ahmed, J., (2023). The Role of Ayushman Bharat Health Account (Abha) in Telehealth: A New Frontier of Smart Healthcare Delivery in India. In: Kohei Arai, ed., (2023). *Proceedings of the Future Technologies Conference (FTC)*. Vol. 2, pp. 388–406. Cham: Springer Nature Switzerland; doi: 10.1007/978-3-031-47451-4_28.

Pears, M. and Konstantinidis, S.T., (2021). Cybersecurity Training in the Healthcare Workforce — Utilization of the Addie Model. *2021 IEEE Global Engineering Education Conference (EDUCON)*, pp. 1674–1681, doi: 10.1109/EDUCON46332.2021.9454062.

Price, W.N., Kaminski, M.E., Minssen, T. and Spector-Bagdady, K., (2019). Shadow Health Records Meet New Data Privacy Laws. *Science (New York, N. Y.)*, 363(6426), pp. 448–450, doi: 10.1126/science.aav5133.

Rai, B.K., (2022). Blockchain-Enabled Electronic Health Records for Healthcare 4.0. *International Journal of E-Health and Medical Communications (IJEHMC)*, 13(4), pp. 1–13, doi: 10.4018/IJEHMC.309438.

Raizada, N. and Biswal, M., (2024). An evidence-based investigation of cert-in's reporting on cyber-threats in healthcare sector. *Conhecimento & Diversidade*, 16(42), pp. 219–246, doi: 10.18316/rcd.v16i42.11694.

Reshmi, T.R., (2021). Information Security Breaches Due to Ransomware Attacks — a Systematic Literature Review. *International Journal of Information Management Data Insights*, 1(2), 100013, doi: 10.1016/j.jjimei.2021.100013.

Richter, J.G. and Thielscher, Ch., (2023). New Developments in Electronic Health Record Analysis. *Nature Reviews Rheumatology*, 19(2), pp. 74–75, doi: 10.1038/s41584-022-00894-1.

Sardi, A., Rizzi, A., Sorano, E. and Guerrieri, A., (2020). Cyber Risk in Health Facilities: A Systematic Literature Review. *Sustainability*, 12(17), 7002, doi: 10.3390/su12177002.

Savin, V.D. and Anysz, R.N., (2021). Cybersecurity Threats and Vulnerabilities of Critical Infrastructures. *American Research Journal of Humanities Social Science,* 04(07), pp. 90–96. Available at: https://www.arjhss.com/wp-content/uploads/2021/07/L479096.pdf [Accessed 21.09.2024].

Sengupta, K., (2017). Isis-Linked Hackers Attack NHS Websites to Show Gruesome Syrian Civil War Images. *The Independent*. February 8. Available at: https://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html [Accessed 21.09.2024].

Shah, Sh.M. and Khan, R.M., (2020). Secondary Use of Electronic Health Record: Opportunities and Challenges. *IEEE Access*, 8, pp. 136947–136965, doi: 10.1109/ACCESS.2020.3011099.

Škiljić, A., (2020). Cybersecurity and Remote Working: Croatia's (Non-)Response to Increased Cyber Threats. *International Cybersecurity Law Review,* 1(1), pp. 51–61, doi: 10.1365/s43439-020-00014-3.

Strupczewski, G., (2021). Defining Cyber Risk. *Safety Science*, 135, pp. 105–143, doi: 10.1016/j.ssci.2020.105143.

Sudhanshu, N., (2022). Indian Healthcare: Attack Surfaces, Personal Digital Data Protection, and Cyber Resiliency. *Observer Research Foundation*. December 28. Available at: https://www.orfonline.org/expert-speak/indian-healthcare-attack-surfaces-personal-digital-data-protection-and-cyber-resiliency/ [Accessed 21.09.2024].

Thamer, N. and Alubady, R., (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. *2021 1st Babylon International Conference on Information Technology and Science (BICITS),* pp. 210–216, doi: 10.1109/BICITS51482.2021.9509877.

Tully, J., Selzer, J., Phillips, J.P., O'Connor, P. and Dameff, Ch., (2020). Healthcare Challenges in the Era of Cybersecurity. *Health Security*, 18(3), pp. 228–231, doi: 10.1089/hs.2019.0123.

Warkentin, M. and Orgeron, C., (2020). Using the Security Triad to Assess Blockchain Technology in Public Sector Applications. *International Journal of Information Management*, 52, 102090, doi: 10.1016/j.ijinfomgt.2020.102090.

Yusuf, A. and Ayinde A., (2023). Cybersecurity Plan for a Healthcare Cloud-Based Solutions. *Journal of Cyber Security,* 4(3), pp. 185–188, doi: 10.32604/jcs.2022.035446.

Zahid, M., Inayat, I., Daneva, M. and Mehmood, Z., (2021). Security Risks in Cyber Physical Systems — A Systematic Mapping Study. *Journal*

of Software: Evolution and Process, 33(9), e2346, doi: 10.1002/smr.2346.

Zodian, M., (2024). Recourse Allocation and Capabilities Generation in Security Studies. In: Anton, S., Tutuianu, I.S., editors (2024). *The Complex and Dynamic Nature of the Security Environment. Proceedings of the International Scientific Conference "Strategies XXI."* Vol. 2, pp. 19–26. Available at: https://www.academia.edu/103421710/THE_COMPLEX_AND_DYNAMIC_NATURE_OF_THE_SECURITY_ENVIRONMENT_Volume_2 [Accessed 23.03.2024].

Information about the Authors

Niharika Raizada, Assistant Professor, CHRIST University, Bengaluru, India
niharika95raizada@gmail.com
ORCID: Orcid ID: 0000-0002-6919-104X

Pranjal Srivastava, Research Scholar, Rashtriya Raksha University, Gandhinagar, India
niharika95raizada@gmail.com
ORCID: 0009-0007-2298-3510