LEGAL LOCK JOURNAL

2583-0384

VOLUME 3 || ISSUE 4

2024

RANSOMWARE THREATS IN INDIA'S HEALTHCARE SECTOR: ASSESSING THE NEED FOR DEDICATED LEGISLATION

Nidhi Kamath[1] & Pratik Amit Oke[2]

ABSTRACT

Ransomware attacks have emerged as a pervasive and financially devastating cybersecurity threat worldwide. Ransomware refers to a type of software that is used to hack into a device in a way that helps one acquire the data that can be used for blackmailing and collecting ransom. It is prevalent in almost all the sectors. The healthcare sector is also a victim of this cyber threat. If the statistics are to be believed, then the rate of ransomware attacks in the healthcare sector in 2023 is almost double the rate in 2021 all over the world. The continuous increase in ransomware attacks all over the world, demands strong legislation. India, being a developing digital economy has introduced certain legislations to control and combat the growing ransomware attacks. The present laws in India to control ransomware attacks are not just included in a single piece of legislation. Rather it has its roots spread to the constitution, criminal law, and bills such as that of data protection. However, the effectiveness of these laws remains a concern for the nation. Despite having so many laws, they aren't very effective in curtailing or preventing ransomware attacks. The paper employs a mixed method approach to deeply analyze the reasons why the present legislation isn't much effective in preventing ransomware attacks, what the limitations of present legislation and why is there a need to bring single legislation for dedicated health data law to achieve its objective. The paper also tries to analyze the situation of ransomware attacks in the U.S.A., which introduced the (HITECH) Act in 2009 to transform Public Health information into electronic health records which India is attempting to do right now. The paper analyzes the functioning mechanism of different laws from both countries to finally conclude whether India needs separate personal health data legislation or not.

[1]The author is a student at Nirma University of Law.
[2]The co author is a student at Nirma University of Law.

KEYWORDS: Ransomware Attack, Cybersecurity Threat, Healthcare, Legislation, Effectiveness

INTRODUCTION:

Ransomware is a form of malicious software created to block an organization from accessing its computer systems until a significant sum of money is paid to the hackers. Ransomware is a form of malware usually distributed through phishing emails that mimic legitimate messages from trusted sources. These emails include attachments like Microsoft Word documents, which, when opened, trigger the installation of ransomware. The attachment may seem harmless to delay detection. Concurrently, the ransomware encrypts important files on the user's device and any linked devices. After the encryption process is finished, the ransomware will show an image on the screen with guidance on how the victim can pay a ransom to receive a decryption key. This ransom is usually demanded in bitcoins, offering the malware creator an untraceable and immediate form of payment. The ransomware attack progresses through five specific stages, beginning with the initiation and setup phase, followed by the infection phase, then the encryption stage, the extortion phase, and finally the decryption phase. This process is known to expose sensitive data to scammers or hackers, leaving individuals vulnerable to further scams and larger-scale crimes. The medical industry was identified as one of the main sectors experiencing frequent ransomware attacks. It is a significant sector in the Indian economy, contributing both human resources and physical assets on a large scale. Both public and private hospitals in the medical sector rely heavily on online applications to manage their data and accounts, as well as on advanced technology for the equipment used in the sector. The healthcare setting presents an ideal opportunity for ransomware attacks due to the high value of personal health information (PHI) and its vulnerabilities. Healthcare ransomware attacks are typically aimed at either holding PHI hostage for payment or selling the information to third parties.[3]

Currently, personal health information (PHI) holds a higher value on the black market compared to data from financial institutions. Cybercriminals find PHI particularly valuable as it can be sold multiple times in secondary transactions. According to the FBI Cyber Division, cybercriminals can sell partial electronic health records for $50 each on the black market,

[3] Deborah R. Farringer, Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals, 40 SEATTLE U. L. REV. 937, 937–41, 951–58 (2016).

whereas stolen social security or credit card numbers only fetch $1.[4] Think about this: A hospital, or any healthcare center, stores a large amount of personally identifiable information about people – much more sensitive than any other kind of data that could be taken in a security breach. In 2019, a study calculated the value of a single healthcare record at $250 – much higher than the next most valuable data record, a payment card, which would only earn a malicious actor $5.40.[5]

CloudSEK, a cyber intelligence firm headquartered in Bengaluru, has reported that India's healthcare sector is the second most targeted for cyberattacks globally, comprising 7.7% of all attacks on healthcare institutions in 2021. The United States leads with 28% of the attacks.[6]

The Medical Industry is facing numerous threats from ransomware, with a recent increase in high-profile attacks targeting medical entities. The consequences of these attacks go beyond the ransom paid, as they have caused significant delays in patient care and even put lives at risk. The fragmented nature of health systems, with different parts using software from various vendors, makes them particularly vulnerable to such attacks. Some hospitals have been forced to pay substantial sums of money to cyber criminals following ransomware attacks. As a result, these payments have resulted in numerous fresh assaults on the same organizations, and the effectiveness of these assaults has given the cybercriminal community a greater sense of confidence. In this research article, various attempts are made to understand various instances of ransomware attack cases in India and the legislation available in India for tackling the same. In addition, the paper tries to analyze India's push for the digitization of health data in the absence of a dedicated Personal Health Data law, it further emphasizes the need for strong legislation concerning Personal health data to ensure that there are no further cases of misuse of such health data by making an elaborate comparative analysis with nations like USA, UK, UAE that have dedicated legislations for the same.

---

[4] FED. BUREAU OF INVESTIGATION, HEALTH CARE SYS. & MED. DEVICES AT RISK FOR INCREASED CYBER INTRUSIONS FOR FIN. GAIN (2014), http://www.illuminweb.com/wp-content/uploads/ill-mouploads/103/2418/health-systems-cyber-intrusions.pdf.

[5] AIIMS ransomware attack: What it means for health data privacy - ET CISO (2022) ETCISO.in. Available at: https://ciso.economictimes.indiatimes.com/news/aiims-ransomware-attack-what-it-means-for-health-data-privacy/96538957#:~:text=The%20recently%20revised%20Personal%20Data,up%20to%20Rs%20250%20crore (Accessed: 10 February 2024).

[6] Increased cyber attacks on the Global Healthcare Sector: CloudSEK (2022) RSS. Available at: https://www.cloudsek.com/whitepapers-reports/increased-cyber-attacks-on-the-global-healthcare-sector (Accessed: 10 February 2024).

1. Ransomware attacks in India:

The medical sector in mid-2023 is said to have witnessed one of the most gruesome ransomware attacks in the All-India Medical Science Institute (AIIMS), Delhi. The hospital was being attacked by ransomware further preventing them from carrying on the billing process which also proved to be fatal for some serious patients being treated in ICUs when their systems were made inaccessible. The AIIMS attack severely impacted various services, such as patient registration, online appointments, diagnostic report generation, and billing, as well as administrative functions like salary distribution and drug procurement. The system is currently undergoing the restoration of data from backups, and it is uncertain whether the backups contain the most recent data. The dynamic nature of healthcare environments necessitates instant and reliable access to real-time data. Even backups that are just a few minutes old can jeopardize patient safety. The AIIMS ransomware attack is said to have impacted 40 million records, including those of influential individuals in the country. As a result, the significance of this data extends beyond just its monetary value.[7] Allegedly the hackers demanded a ransom of Rs2bn (£2m; €2.2m; $2.4m) in cryptocurrency.[8] For nearly two weeks, these services had to be handled manually, resulting in long queues and extended patient waiting times. However, online services have now resumed, with data restored from a backup server. The day following the attack, Delhi Police lodged a First Information Report (FIR) for cyber terrorism and extortion. The FIR has been filed under sections 66F (cyber terrorism) and 66 (computer-related fraud) of the Information Technology Act, as well as section 385 (extortion) at IFSO, special cell. Shortly after the AIIMS attack, the private details of 150,000 patients who had visited the Sree Saran Medical Centre, a 100-bed hospital in the southern state of Tamil Nadu, between 2007 and 2011, were discovered being sold on various cybercrime forums.[9]

The previous year, there were reports of 200,000 patient records being leaked on the internet from a different private hospital in Kochi, located in the southern state of Kerala.[10] Recently a

[7] The Economics Times, Supra note 3.
[8] Hackers demand Rs 200 crore in cryptocurrency from AIIMS-Delhi as server remains down for 6th day (2022) PTI. Available at: https://www.ptinews.com/news/national/hackersdemand-rs-200-crore-in-cryptocurrency-from-aiims-delhi-as-server-remains-down-for-6thday/466850.html (Accessed: 10 February 2024).
[9] Standard, B. (2022) Hackers now selling 150K patients' data of TN Hospital on Dark Web: Report, Business Standard. Available at: https://www.business-standard.com/article/current-affairs/hackers-now-selling-150k-patients-data-of-tn-hospital-on-dark-web-report-122120200647_1.html (Accessed: 10 February 2024).
[10] Jacob, J.V. (2021) Data Breach from Kochi Hospital! 2 lakh patient records found on net, Onmanorama. Available at: https://www.onmanorama.com/news/kerala/2021/01/13/data-breach-from-kochi-hospital-2-lakh-patient-records-found-on-net.html (Accessed: 10 February 2024).

Private Hospital in Gujarat (KD Hospital) fell prey to a ransomware attack, The hospital was unable to access any of its online systems, such as patient data, hospital files, and software, due to the cyberattack. A ransom demand was made via an email by the attackers of USD 70,000 in bitcoins to decrypt the files. The FIR was lodged under IPC sections 384 (extortion), 511 (moral guilt and injury), and IT Act sections 43 (penalty and compensation for damage to computer, computer system) and 66 (computer-related offense).[11] In case of a breach the personal Health Data of patients and healthcare workers, as well as several cabinet ministers and senior bureaucrats, is exposed. Personal Health Data when aggregated and processed using various artificial intelligence and modeling software, data from individuals within a specific geographical area, community, interest group, or political leaning can yield patterns and forecasts that may have security implications far beyond privacy concerns. For instance, worries have been expressed regarding the security of politicians receiving treatment at AIIMS, including numerous prime ministers. "This is even before considering the potential consequences of fatalities and harm to health in the event of any mishaps with healthcare data in medical facilities." it seems that they are of no use. Looking at the continuous increase in the number of ransomware Id. at 70.

2. Legislations That Deal with Ransomware Attacks:

The Information Technology Act, of (2000) is a primary legislation that deals with issues on cybersecurity including ransomware attacks.[12] It aims to protect all data, records, and information on a device and also aims to identify any malware attacks or fraud on an electronic device. Certain key sections, especially concerning ransomware attacks, include Section 43, Section 65, Section 66D, Section 66F, Section 72, and other relevant sections based on the situation.[13] According to Section 43, if any person accesses the computer or introduces any virus into the computer, causes denial of access to that computer to the owner, or steals any data from the computer without the permission of the owner shall be held liable to pay compensation.[14] A person held liable in section 43 shall be punished with

[11] Hospital falls prey to ransomware attack, hackers demand $70,000 (2023) The Express News Service. Available at: https://indianexpress.com/article/cities/ahmedabad/hospital-falls-prey-to-ransomware-attack-hackers-demand-70000-8613410/ (Accessed: 10 February 2024).
[12] The Information Technology Act, 2000, No.20, Acts of Parliament, 2000(India).
[13] The Information Technology Act, 2000, §§65, 65D, 66F, 72, No.20, Acts of Parliament, 2000 (India).
[14] Supra note *11*.

imprisonment extending up to three years and a fine expending up to five lakhs or both under section 66.[15] Section 43 read with section 66 is mainly for denial-of-service (DOS) attacks which are similar to ransomware attacks. A denial-of-service attack involves the perpetrator stealing information from a computer device and rendering it unavailable and inaccessible to its rightful users by manipulating the device. This is similar to ransomware attacks. Hence section 43 and section 66 of The Information Technology Act, 2000 are the most crucial sections for ransomware attacks. Ransomware attacks can also impact India's national integrity, security, and sovereignty if a government computer device is hacked and compromised by this malware, putting confidential government information at risk. Therefore another relevant section concerning ransomware attacks is section 66F which provides punishment for cyber terrorism and imprisonment in such cases can extend up to life imprisonment as well. However, in recent years there have been various amendments to The IT Act, of 2000. The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021 governs social media platforms and over-the-top (OTT) platforms.[16] The aim is to provide a complaint mechanism for such platforms in case of any grievances. Nonetheless, it also includes specific clauses for safeguarding information and data on computer devices, making it a pertinent legal provision in the event of a ransomware attack.

The National Cyber Security Policy 2013 was enacted by the Department of Electronics and Information Technology as an additional security framework to evade cyber-attacks.[17] One of the main goals of the National Cyber Security Policy (NCSP) is to guarantee a safe cyberspace for all individuals. Furthermore, it aims to create strong infrastructure and defense systems to counter cyber-attacks.

The principal legislation that deals with data protection in India is the Digital Data Protection Act (2023). As the name of the Act itself suggests, the Act aims to protect the data. One of the main features of The Digital Personal Data Protection Act, 2023 is to obligate the data fiduciaries to protect the data and keep it safe. They are obligated to implement reasonable security safeguards to protect data. In furtherance to this, the act also prescribes penalties upon the data fiduciaries for violating the privacy of the data principles. The DPDP Act also

[15] Supra note *11*.
[16] Ministry of Electronics and Information Technology, Vide G.S.R. 139(E), published in the Gazette of India, Extra., Pt. II, Sec. 3(i), (dated 25.2.2021).
[17] Ministry of Electronics and Information Technology, NCSP-2013, File No: 2(35)/2011-CERT-in (Notified on July 02, 2013).

stipulates significant sanctions to deter breaking its rules.[18] Under the DPDP Act Penalties for breaking the Act can be as high as INR 250 crore, with a minimum of INR 10,000 to INR 200 crore.[19] Notably, the Act's provisions no longer include criminal penalties, such as the potential for incarceration. There haven't been many cases of cyber breaches leading to penalties or compensation up until now. But this is probably going to change once the DPDP Act is put into effect. As such, sufficient arrangements must be made for adherence.

In case the Hospital which is affected is registered as a public limited company the provisions of Companies Management and Administration Rules, 2014 are also attracted. According to Rule 28. (Security of records maintained in electronic form) of the said rules, Companies are obligated to prevent unauthorized access to their computer records. In the event of a data breach, they must demonstrate that they have taken all essential measures to safeguard their data from unauthorized access. This obligation serves as an additional layer of protection for their data privacy.[20] Any negligence on the part of such corporate entities will lead to charges under Section 43A of the IT Act, and they will be obligated to compensate all those affected by such a breach.[21]

A ransomware attack, subject to the facts and circumstances of each case, may constitute an array of offenses under the Indian Penal Code, of 1860. Criminal conspiracy under section 120, theft under section 378, extortion under section 383, cheating under section 415, cheating by personation under section 416, dishonest and fraudulent removal or concealment of property under section 424, mischief under section 425, and criminal intimidation under section 503 are some of the sections that are attracted in case of a ransomware attack.[22]

Ransomware attacks are extensively addressed in the IT Act and its associated regulations. In case of a ransomware attack, both the IT Act and the Indian Penal Code (IPC) can be utilized to take legal action. Courts in India have ruled that to prevent double jeopardy or conflicts between legislations, if the IT Act (considered a special and more recent law) addresses offenses within its scope through specific mechanisms, invoking the IPC provisions for the same offenses with identical elements is not allowed.[23] The Supreme Court in *State of Uttar*

[18] The Digital Personal Data Protection Act, 2023, Acts of Parliament, 2023 (India).
[19] The Digital Personal Data Protection Act, 2023, §33(*1*), Acts of Parliament, 2023 (India).
[20] Companies Management and Administration Rules, 2014, Rule 28.
[21] The Information Technology Act, 2000, § 43A, No.20, Acts of Parliament, 2000(India).
[22] The Indian Penal Code, 1860, §§ 120, 378, 383, 415, 416, 424, 425, 503, No.45, Acts of Parliament, 1860 (India).
[23] Sharat Babu Digumarti vs. Government (NCLT of Delhi); 2017 2 SCC 18, Gagan Harsh Sharma & Another vs. State of Maharashtra Through Sr. Police Inspector and Another; 2018 SCC OnLine Bom 17705

Pradesh v. Aman Mittal & Anr. (obiter), held that if an offense is charged under the IT Act, then it cannot be charged under IPC. A ransomware attack is not only penal in nature but also directly in the teeth of the fundamental right to privacy, enshrined under Article 21 of the Constitution of India[24].[25]

Despite the presence of a strong legislative DPDP Act, the problem persists wherein the entities are charged under the provisions of IPC and are tried by the traditional method not taking into consideration the presence of such a strong legislation.

2.1 Remedial Infrastructure:

Computer Emergency Response Team (CERT-In) comes under the rules and regulations of the IT Act. It was established by Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 and its main aim is to analyze all cybersecurity incidents and provide effective measures to stop them. As soon as an organization reports any cybercrime, it is the responsibility of the CERT-In to take immediate action in the shortest time and stop any further loss of data.[26]

The National Critical Information Infrastructure Protection Centre (NCIIPC) was established under Section 70A of the IT Act, of 2000.[27] The NCIIPC aims to safeguard India's central information infrastructure, specifically critical information infrastructure (CII). Cybersecurity is divided into non-critical infrastructure and CII, with CERT-In overseeing non-critical infrastructure and NCIIPC dedicated to protecting critical sectors such as government, banking, and insurance. NCIIPC is tasked with ensuring the security of these sectors against cyber threats.

Furthermore, if an individual or corporation falls victim to a ransomware attack, they can file a First Information Report (FIR) at the local police station under the applicable sections of the IT Act (and/or the IPC). The cybercrime cell will then investigate the matter. Indian courts are authorized to conduct trials for offenses under the IT Act following the procedures

[24] Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1, (Para. 309, 310, 629-636, pp. 384, 471-472).
[25] India Const. art. 21.
[26] Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013.
[27] Information Technology (National Critical Information Infracture Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.

outlined in the Code of Criminal Procedure, 1973. A complaint may also be made to the Adjudicating Authority established under Section 46 of the IT Act, which has the powers of a civil court to the extent and for the purposes mentioned therein. These are certain legislations and regulating authorities that India has to control any cyber threat including ransomware attacks. However, despite all these legislations, India still faces a huge threat concerning ransomware attacks and they are increasing day by day.

3. Countries That Have Defined Health Data Law:

"Data concerning health" is defined by the DPA 2018 as personal information on an individual's physical or mental health, including information about their health status that is revealed by the provision of health care services.[28] "Data concerning health" refers to personally identifiable information on a person's physical or mental state, including information obtained through the provision of medical services and revealing that person's health status; "Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or healthcare treatment of an individual" is the definition of sensitive protected data in the proposed American Data Privacy and Protection bill. That appears to be a fairly broad description of what we can refer to as health data in this context, which may be the case. All organizations that operate in the United Arab Emirates and the Free Zones and offer healthcare, health insurance, healthcare IT, and other direct or indirect services connected to the healthcare industry, or that are involved in activities that affect the processing of digital health information (Health Service Providers).

3.1 USA (Brief about HIPAA)

A federal law known as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated the development of national standards to guard against the disclosure of private patient health information without the informed consent or knowledge of the patient. To put HIPAA's obligations into practice, the US Department of Health and Human Services (HHS) released the HIPAA Privacy Rule. A portion of the data covered by the Privacy Rule is protected under the HIPAA Security Rule. The Privacy Rule regulates how organizations covered by the Privacy Rule may use and disclose personally identifiable health information, or PHI. "Covered entities" are the names given to these people and institutions.[29]

[28] Data Protection Act, 2018, c. 12, § 205(1) (U.K.).
[29] Health Insurance Portability and accountability act of 1996 (HIPAA) (2022) Centers for Disease Control and Prevention. Available at: https://www.cdc.gov/phlp/publications/topic/hipaa.html (Accessed: 10 February 2024).

Standards for people's rights to know and decide how their health information is used are also included in the Privacy Rule. Ensuring that people's health information is appropriately secured while permitting the flow of health information required to deliver and promote high-quality healthcare, as well as to safeguard the health and well-being of the general public, is one of the main objectives of the Privacy Rule. The Privacy Rule safeguards the privacy of those seeking medical attention and healing while allowing for significant uses of information. The Security Rule covers a portion of the information covered by the Privacy Rule, while the HIPAA Privacy Rule protects PHI.

To adhere to the HIPAA Security Rule, every covered entity needs to assure the availability, confidentiality, and integrity of all e-PHI, identify and protect against potential risks to the information security, guard against potential unlawful uses or disclosures that are prohibited by the regulation, certify that their employees are complying.

3.2 U. K /EU

United Kingdom General Data Protection Regulation [REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL]:

"Data concerning health" is defined as "personal data related to the physical or mental health of a natural person, including the provision of healthcare services, which reveal information about his or her health status" under the General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR). The Information Commissioner's Office (ICO) has affirmed that any information about an individual's past, present, or future health status falls within the category of "data concerning health."[30]

Under the UK GDPR, biometric, genetic, and health-related data are among the "special categories of personal data." Compared to regular personal data, such special category data is protected to a higher extent. In addition to the legal requirements that must be fulfilled for processing personal data in general, these particular data can only be handled if one of a few strict requirements is satisfied, all of which are outlined in the legislation. Under the UK GDPR, the ICO can impose administrative fines of up to £17.5 million or 4% of the company's yearly global turnover, in addition to its extensive investigative powers. There

[30] Participation, E. (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection regulation)(text with EEA Relevance), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation)(Text with EEA relevance). Available at: https://www.legislation.gov.uk/eur/2016/679/contents (Accessed: 10 February 2024).

haven't been any significant enforcement proceedings against digital healthcare technologies thus far; instead, ICO enforcement activities have mostly been brought on by data breaches. Furthermore, a person has the right to compensation if they have experienced "material" or "non-material" (such as emotional) harm as a result of a data protection infringement.

3.3 U.A. E

Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields:

The use of ICT in the UAE's health care system, including its free zones, is governed by Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields.[31]

Goals:

The statute seeks to guarantee:

The best possible application of ICT in the UAE's health sector, and the confidentiality and security of medical records. The law also makes it possible for the Ministry of Health and Prevention to gather, examine, and preserve national health data. Healthcare professionals must abide by the following rules when utilizing ICT including maintaining the confidentiality of any health-related data and information and not sharing it without proper authorization. The "DOH Policy on Digital Health" seeks to make it possible to use digital technologies to enhance the quality of care and patient outcomes. View the policy in its entirety on the Department of Health Abu Dhabi website.[32]

The United Arab Emirates (UAE), including free zones, is governed by Federal Law No. 2 of 2019 on the Use of Information and Communications Technology in Healthcare (also known as the "ICT Health Law"),[33] which has the following four objectives of making sure that information and communications technology is used as efficiently as possible in the health sector; making sure that the bases, standards, and practices used are consistent with those that have been embraced globally; facilitating the gathering, examination, and preservation of health data and information at the national level by the Ministry of Health and Prevention (the "Ministry"); and guaranteeing the security and safety of health data and information.

[31] Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Field

[32] Data protection laws | The Official Portal of the UAE government (no date) Data Protection Laws. Available at: https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws (Accessed: 10 February 2024).

[33] Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Field

4. India's Push for Digitization Of Healthcare In The Absence Of Dedicated Health Data Law:

4.1 Analysis of the USA 2009 Act and how it led to increased instances of Ransomware attacks:

The objective of the HITECH Act of 2009 was to transition personal health information (PHI) into electronic health records (EHRs) nationwide, with a budget of $31 billion.[34] The unexpected surge in cyberattacks targeting the healthcare industry following the implementation of the 2009 economic stimulus package by the US government is an unforeseen consequence.[35] To assist the healthcare industry in transitioning from traditional paper-based patient records in doctors' offices to electronic records accessible globally, HITECH created financial incentives.[36] In theory, electronic health records (EHRs) could provide patients and their caregivers with a central repository for storing their medical history and current details of any ongoing treatments. They could eliminate many errors in patient care that are related to human error, such as illegible handwriting.[37] Furthermore, granting healthcare administrators increased access to a comprehensive view of each patient would result in more efficient patient care. Unfortunately, the transition from paper records, which were never truly secure, to easily accessible digital files has been one of the most negative outcomes of EHRs. Instead of being accessible for the patient's advantage, what was intended for the benefit of cybercriminals with malicious intent has now become accessible for their gain. These malicious intentions may involve selling the data online, holding it for ransom in exchange for large sums of money, or using identity theft to obtain free medical treatment and prescription drugs.[38] The healthcare industry has seen a significant increase in cyberattacks

[34] Health Information Technology for Economic and Clinical Health (HITECH) Provisions of American Recovery and Reinvestment Act of 2009 (ARRA), Title XIII, Pub. L. 111-5, 123 Stat. 115 (2009) (codified as amended in scattered sections of 42 U.S.C.).

[35] American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. 111-5, 123 Stat. 115 (signed into law on Feb. 17, 2009 by President Obama).

[36] See Standards for the Electronic Health Record Technology Incentive Program, 42 C.F.R. § 495.2 (2010) (establishing payment incentive programs for hospitals and healthcare providers that can demonstrate "meaningful use" of certified EHR technology); see also HITECH Act Enforcement Interim Final Rule, U.S. DEP'T OF HEALTH & HUMAN SERVICES (June 16, 2017), https://www.hhs.gov/hipaa/forprofessionals/special-topics/HITECH-act-enforcement-interim-finalrule/index.html.

[37] Electronic Prescriptions for Controlled Substances, Interim Final Rule with Request for Comment, 75 Fed. Reg. 16236, 16238 (Mar. 31, 2010) (finding that EHRs and electronic prescription applications "may reduce medical errors caused by illegible handwriting")

[38] Deborah R. Farringer, Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals, 40 SEATTLE U. L. REV. 937, 937–41, 951–58 (2016).

due to patient data being accessible to hackers on hospital and healthcare provider networks.[39] The increase in ransomware attacks has had a devastating effect on the American healthcare industry. The consequences have included disruptions to patient care and operational outages, among other impacts. Regulators need to do more than just update and modify current regulations to keep pace with modern technology for hospitals and health systems to survive and potentially prevent these attacks. While implementing safeguards may help prevent these attacks, the healthcare industry as a whole must shift its focus to raise awareness about the importance of cybersecurity. Industry leaders should establish best practices that equip healthcare providers and other stakeholders with the necessary tools to not only comply with regulations but also actively thwart these types of attacks. One way to achieve this is by urging EHR vendors to offer improved, more advanced solutions with the latest cybersecurity measures.

In India, the Delhi incident has put a spotlight on the Indian government's ambitious push to digitize patient records and hospital services, through a program known as the Ayushman Bharat Digital Mission. The attack came just as AIIMS was preparing to go completely paperless in 2023—something the Indian government is pushing hard in an attempt to modernize a healthcare system serving over 1.4 billion people, not all of whom have electronic medical records. Ayushman Bharat is no doubt a very progressive step towards the digitalization of the health data of the people to eliminate various human discrepancies. On September 27, 2021, the Prime Minister used a video conference to officially launch the Ayushman Bharat Digital Mission (ABDM). Dignitaries in attendance included Dr. Bharati Pravin Pawar, Minister of State for Health and Family Welfare, and Shri Mansukh Mandaviya, Union Minister of Health and Family Welfare. Hospitals around the nation will be able to communicate with one another using the Ayushman Bharat Digital Mission's digital health solutions. The Mission will not only streamline hospital procedures but also improve quality of life. A plethora of additional services, such as digital consultation and patient consent for medical professionals to view their records, will also be made possible by the digital ecosystem. Old medical records won't disappear after this plan is put into place because every record will be digitally preserved.[40]

---

[39] U.S. GOV'T INTERAGENCY GUIDANCE DOCUMENT, HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE, https://www.justice.gov/criminal-ccips/file/872771/download; see also Khizar A. Sheikh, Ransomware, Social Engineering and Organization Liability, N.J. LAW., Dec. 2016, at 34 (2016).

[40] Ayushman Bharat Digital Mission (ABDM)| National Portal of India, National Portal of India. Available at: https://www.india.gov.in/spotlight/ayushman-bharat-digital-mission-abdm (Accessed: 10 February 2024).

But then again, the fundamental problems persist taking inspiration from the US's HITECH Act that the more we attempt to digitalize and place reliance on digital health data, the more are the chances and risks of ransomware attacks. The inference that can be drawn by these legislations is that there is a need for a strong legal framework following which the digitalization of health data would contribute to strong security and protection of sensitive health data of the citizens.

4.2 Proposed Single Legislation DISHA:

The Digital Information Security in Healthcare Act (DISHA) was suggested in 2017 by the Ministry of Health & Family Welfare, Government of India (MoHFW), however, it was never put into effect. In response to the pressing need, the MoHFW announced the Telemedicine Practice Guidelines on March 25, 2020, which unexpectedly led to an increase in e-consultations within the healthcare sector. The Guidelines impose stringent criteria on technology platforms and hold them accountable by blacklisting them if they are found to be in violation.

Hospitals and clinics can share individual health records digitally, thanks to the DISHA (Digital Information Security in Healthcare Act), which also provides a framework for the development of digital health records in India. The exchange of electronic health records linked to Aadhaar through the National Health Information Network has been approved by the National Health Policy. It appears that DISHA establishes the framework for other health exchanges. With DISHA, each individual is fully in charge of their data and there are significant limitations on how health data can be used. The Stronger Security Provided By DISHA For An Individual's Data Is Evident. The DISHA Prohibits the Use and Processing of Health Data on Any Other Legal Grounds, Including Permission. Furthermore, if a purpose or processing is defined under DISHA, then either the person's agreement or the relevant legislation must require such use.

DISHA is extremely similar to HIPAA, Since both DISHA and HIPAA govern personal health data, the information they both regulate is comparable. DISHA distinguishes between two categories of data: personally identifiable information (PII) and digital health data (DHD), whereas HIPAA governs protected health information (PHI) and PHI that is electronically stored (ePHI).[41] Ensuring the privacy, security, uniformity, and confidentiality

[41] Disha and HIPAA, how do they compare? (2023) Compliancy Group. Available at: https://compliancy-group.com/disha-and-hipaa-how-do-they-compare/ (Accessed: 10 February 2024).

of digital health data was the main objective of the act. Controlling the creation, collection, storage, transmission, and access of digital health data associated with identifiable personal information is the goal of the legislation. This led to the creation of the National Digital Health Authority and Health Information Exchanges. It records every piece of health-related information regarding the individual's physical and mental health, the medical services they received, any physical substance or body part inspections, the information acquired during the provision of medical services, and the particulars of any clinical facility they may have visited.

DISHA, if implemented, will act as concrete legislation and ensure there is no breach of privacy concerning sensitive information and health data. The Information Technology Rules, 2011 in conjunction with the Information Technology Act, 2000 (the "IT Act"), as modified by the Information Technology (Amendment) Act, 2008, addresses the existing legal framework for data privacy and protection. Despite the IT Act's emphasis on information security, data privacy issues are not sufficiently addressed.

In this regard, security, uniformity, privacy, and confidentiality criteria for electronic health data are provided by the proposed Digital Information Security in Healthcare Act 2018 ('DISHA'). DISHA is regarded as the Indian counterpart of the Health Insurance Portability and Accountability Act of 1996 (often known as "HIPAA"), which oversees this matter in the United States. While DISHA appears to have some potential, its application and enforcement have not yet received a thorough assessment. The research thus proposes the need for a proposed single legislation like DISHA.

CONCLUSION:

In India, existing laws lack clarity regarding whether AIIMS is considered a victim or liable for compromising critical data. In the AIIMS Incident, The first information report filed for the case cites sections of the Information Technology (IT) Act, including one related to cyber terrorism, as well as invoking the Indian Penal Code's section concerning extortion. Under the DPDP Act, in the event of a personal data breach, the Data Fiduciary is required to inform each affected Data Principal and the Board. However, the specific format and method of reporting are yet to be prescribed. Thereafter, Data Fiduciaries are required to report all types of personal data breaches, regardless of the sensitivity of the breach or its impact on the Data Principal. However, under the DPDP Act, neither materiality thresholds nor express timelines

have been prescribed for the reporting requirement. Further, the DPDP Act has omitted health data from the category of sensitive personal data. The previous versions of the bill recognized health data as sensitive, which afforded it additional protections. However, the latest version no longer includes this classification. Equating health data with other types of data is a misstep and fails to acknowledge its unique sensitivity and the need for heightened safeguards.

What is even more concerning is the lack of accountability in the event of a large-scale attack like this. In the US, the Health Insurance Portability and Accountability Act (HIPAA) mandates that regulated entities adhere to its breach notification rule. Similarly, the UK and Australia have specific guidelines for handling a data breach involving the loss of protected health information. The UAE also has a well-defined Health Data Law, and the European Union has legislation specifically addressing health data. The JPC recommended a Breach Notification rule however that has not been included in the DPDP Act.

The EU has established a European Data Protection Board, which has developed guidelines that provide a comprehensive list of examples concerning data breach notifications. These guidelines have, *inter-alia*, (a) categorized ransomware attacks based on a variety of aspects, for instance, their nature and veracity, preparedness of the victim in question, prior measures and risk assessment that ought to have been carried out, and so on; (b) provided for detailed mitigation steps; and (c) laid down the obligations cast upon organizations, in possession of sensitive data.[42]

Moreover, Singapore has enacted a comprehensive data protection law, namely the Personal Data Protection Act, 2012 ('**PDP Act**'). This legislation establishes a Personal Data Protection Commission responsible for overseeing and enforcing data protection laws, as well as adjudicating any related proceedings. In a recent ruling, the commission imposed an $8,000 penalty on an organization that fell victim to a ransomware attack due to its failure to implement adequate security measures for data protection as mandated by the PDP Act.[43]

Despite efforts, India remains a prime target for ransomware attacks, highlighting the country's vulnerability to cybercrimes. National Crimes Records Bureau data reveals a nearly doubling of such crimes from 2018 to 2020,[44] underscoring the urgent need for a comprehensive data protection framework to enhance data security. While the DPDP Act

[42] European Data Protection Board, Guidelines on Examples regarding Data Breach Notifications, 2021.
[43] Personal Data Protection Commission Decision, Seriously Keto Pte Ltd, Case No. DP-2006-B6449, 21/07/2021
[44] National Crime Records Bureau, Cyber Crime (2018-2020)

2023 is in force, further amendments may be necessary, particularly to establish a robust mechanism for addressing ransomware attacks.

There is a strong need to take inspiration from the UK jurisprudence and implement a legal provision specifically focused on the protection of health data. It is essentially necessary to learn from the flip side of the implementation of schemes from the US wherein HITECH led to an increase in the number of cases of ransomware attacks. The DPDP Act, no doubt, has certain provisions that deal with the imposition of penalties in cases of breach of data privacy. Irrespective of this, there is not a specific health data law in India. This issue needs a resolution. After COVID hit the Indian healthcare sector, an attempt made by the Indian government to digitalize health data is a commendable one but it is necessary to make an important observation that a similar attempt was made by the US government through (HITECH) only leading to a substantial increase in the ransomware attack cases. It is necessary to have a strong health data law before digitalizing the health data. The need for dedicated legislation like DISHA is necessary to prevent cases of ransomware attacks. In a nutshell, it can be said that as important as it is to digitalize health data, so is the need for dedicated legislation regarding the same.

Ensuring cybersecurity capability in healthcare facilities primarily entails educating the individuals responsible for operating computer systems. However, many hospitals worldwide struggle to allocate resources toward training their staff in cybersecurity due to the demands of their core hospital duties. A study conducted in 2016 and published in Healthcare Informatics Research highlighted the lack of information technology infrastructure in most public hospitals and dispensaries in India.[45] This raises concerns about how the underfunded public health infrastructure in India will manage to incorporate cybersecurity systems and training within its budget constraints. The governments have a significant responsibility to support the health sector adequately.

Experts emphasize that the Indian government must prioritize the regulation of cybersecurity systems and practices across all health facilities. The government authorities should designate the health sector as critical infrastructure, similar to the United States. Also, The Indian government ought to establish more stringent compliance standards for cybersecurity in health facilities, provide support for IT training for healthcare workers, and engage in closer consultation with experts in the field.

[45] Srivastava SK. Adoption of electronic health records: A roadmap for India [PubMed]. Healthc Inform Res 2016;22: -9. doi: 10.4258/hir.2016.22.4.261. pmid: 27895957

Since the AIIMS Incident, the Indian government has introduced several cybersecurity initiatives. A draft of the new national cybersecurity policy is being made, although it has not yet been made public.[46] Furthermore, the Indian government is reportedly establishing a national counter-ransomware taskforce and developing national information security policy guidelines to prevent future attacks.[47]

[46] Pandey DK. Draft cybersecurity strategy has been formulated: Centre. The Hindu 2022 Dec 14.

[47] Das M. After AIIMS ransomware attack, Modi govt's building a task force to fight cyber espionage. The Print 2023 Jan 27.