IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IMPORTANCE OF DATA PRIVACYINHEALTHCARE

Ashish L, Assistant Professor, Nehru College of Engineering and Research Centre.
Radhideve, Department of MCA, Nehru College of Engineering and Research Center.

Abstract:

Trust is one of the cornerstones of the healthcare system. Patients must have faith that the individuals and institutions giving their care have their best interests in mind. When visiting a doctor, people frequently divulge information about themselves that they might not otherwise. They must have faith that their healthcare provider won't reveal that information to anyone else, including pharmaceutical companies, interested family members, or other healthcare professionals, without their explicit permission.

Trust between consumers and medical professionals is extremely important. Patients are more likely to seek the treatment they require or follow their doctor's advise when they have confidence that their information will be kept private. Following medical guidance can help prevent the spread of some diseases and alleviate the burden on the healthcare system as a whole.

Keywords:
Data privacy, Health data, Medical Sector, Pharmaceutical, Security, Artificial intelligence

1. INTRODUCTION

For many reasons, data protection in healthcare is essential. Building confidence benefits the healthcare system as a whole, which is facilitated by maintaining the security and confidentiality of patient information. Data on patients is further shielded from malicious parties by maintaining anonymity. Breakdown can and does happen. The Office for Civil Rights at the U.S. Department of Health and Human Services keeps tabs on and looks into the annual data breaches.

Health plans and healthcare providers are just two of the covered organisations that are impacted by data breaches. They manifest as theft, unauthorised access to or disclosure of email or medical data, network server hacks, and email hacks. Bad actors might need access to patient data for a variety of purposes, such as selling the information for a profit or extorting the people who will be impacted.

Data security is crucial in the healthcare industry because it may be necessary for the organisation to briefly halt operations if a health plan or provider experiences a breach. Patients may need to wait longer for the care they need or may skip it if operations are postponed. There are additional reasons for your healthcare company to take every precaution to protect the privacy of your patient's health information in addition to ensuring that patients continue to have access to healthcare.

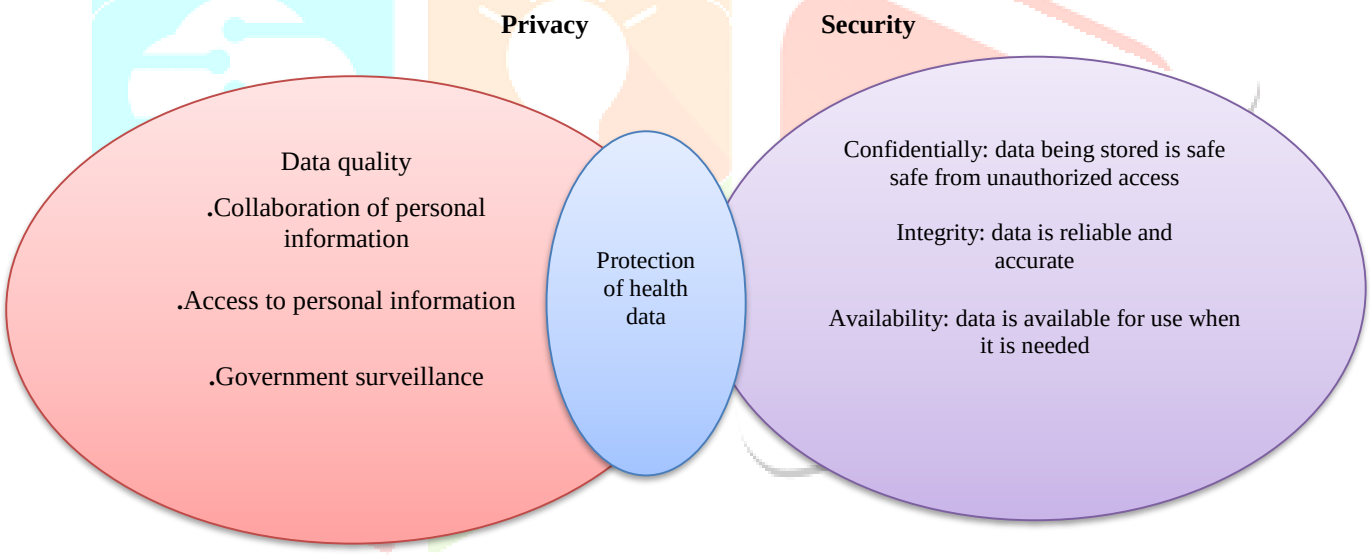
II.LITERATURE SURVEY

Shailendra Sinhasane proposed Data Privacy in Healthcare - A Necessity in protecting Health Information Data (2022).This study says the correct way of handling and protecting sensitive patient data from various cyber security threats. An create awareness revolves around the significance of data privacy in health care. Due to the immense impact of the COVID-19 pandemic, the dramatic increase of utilizing smart devices and digital health tools boosts the levels of productivity. In this Article deeply explain the data challenges in healthcare Ransomeware attacks, Healthcare mobile application, Reduce interoperability, Vulnerabilities in Internet of Thinks, Limitations in resources.

Abigail Sims proposed Perspectives on What is Data Privacy in Healthcare? Everything You Need to Know (2022). This study aims for total study of data privacy in healthcare. Patient trust and Patient safety are the important key reasons of healthcare data. Healthcare organizations face the same potential penalities for non-compliances if they fail to protect patient data adequately. Another main point of this article is Regulation of health data. They are HIPAA(Health Insurance Portablity and Accountability Act, GDPR(General Data Protection Regulation) .

Fengjun Li, Xukai Zou, Peng Liu & Jake Y Chen proposed New threats to health data privacy (2012). The aim of this systematic review was to provide a well findings of Rapid digitalization of health data. There is an increasing concern on maintaining data privacy while garnering the benefits, especially the when the data are required to be published by secondary use. They studied how patient privacy could be compromised with the help of today's information technologies.

III.DETAILED STUDY ABOUT DATA PRIVACY IN HEALTH CARE



3.1. What is data privacy in healthcare?

Policies and technology used to safeguard sensitive health information for medical clients and patients are considered aspects of health care data privacy. Only authorised personnel, such as doctors, are permitted to view sensitive patient medical data or protected health information (PHI).

3.2. What is meant by the privacy of healthcare data?

To ensure that only approved people and groups can access patient data and medical information, a set of rules and regulations are necessary for health care data privacy.it may also apply to a company's procedures for safeguarding patient health information and preventing unauthorized access to it.

3.3. Why is data privacy significant in the healthcare industry?

As digitalization expands quickly today, patient information is at greater risk than ever before from data breaches and cyberattacks. The greatest level of data privacy is crucial for healthcare services because of this.

1. **Avoid fines for noncompliance**

Patient privacy laws and rules are in place for a reason, and the government views violations seriously. When a breach occurs, a company won't be able to shrug its shoulders and claim not to know the laws. Penalties for noncompliance differ depending on how serious the problem is. A healthcare organization's employer may deal with a specific employee personally if they are to blame for the privacy breach or other problems.

2. **Increase patient trust and customer trust**

A patient is more apt to divulge highly private information to a doctor than to others. The confidentiality of any health-related information by the provider is crucial to maintaining the patient's confidence in them.

3.4. Privacy laws and guidelines for healthcare records

The privacy of health data is protected by a number of laws. Examples include the Health Insurance Portability and Accountability Act (HIPAA) In the united states and the Global Data Protection Regulation (GDPR), which covers data more broadly.

IV.METHODOLOG

4.1. Research questions

This systematic mapping study's main objective is to provide an overview of recent research on privacy mechanisms in health records (HR). Hence, the study aims to understand the current state and future trends on HR systems privacy. The steps of the systematic mapping study method are documented in the following research questions:

– RQ1: What are the main privacy challenges related to health records?
– RQ2: What are the main requirements identified by the laws that HR systems should respect?
– RQ3: What are the main published techniques to provide privacy in the HR system?
– RQ4: How well are the published techniques addressing the requirements?

4.2 Search process

Our research was carried out in the base Scopus, the largest database of abstracts and citations in the literature with peer review: scientific journals, books, conference proceedings, and industry publications which index the main sources. We decided not to search in other databases like Google Scholar because we only wanted publications with peer review. Examples of sources indexed by Scopus are shown in Table 1. To define the search string, we used terms related to the healthcare domain, privacy, and health records .The main goal was to obtain significant research on these terms. Thus, the defined search string was: – (" Data Privacy" AND "Healthcare" AND " Health Records")

4.3. Screening of papers

We establish the inclusion and exclusion criteria to filter the search results. Our goal is to select relevant Health data privacy articles over the past 6 years. Thus, our article selection process intends to cover peer-reviewed articles on the subject. The research on privacy in health data brought us many sources; for this reason, we decided to limit our research only to articles published in journals and conferences indexed based on Scopus. Finally, we also removed the review articles, as we intend to analyze the articles' individual contributions instead of a compilation of articles. In order to get the appropriate papers in this systematic literature review, we decide the criteria for inclusion and exclusion. The filtering strategy adopted is summarized below. –

4.3.1. Inclusion criteria

This review included published works limited to results from fonts written between 2015 and 2021. Written in English. We have limited only articles published in journals or conference papers. Articles focused on privacy, healthcare, and electronic health records in their titles, abstracts, keywords, or introductions were taken into account

4.3.2. Exclusion criteria

Articles that did not have an electronic health record and where the researchers did not have access, were excluded from the review, as well as papers not written in the English language, review, and surveys, books and gray literature, Informal literature surveys.

V. How will healthcare data security develop in the future?

Like many other industries, the healthcare sector is going through a significant data-driven revolution. More detailed medical data is produced and is now easier to access because to new technologies like telehealth platforms and the internet of things (IoT). While there are obvious advantages to this, there are also significant security risks about healthcare data.

714 healthcare data breaches involving 500 or more records occurred in 2021, nearly twice as many as in 2018. As personal health information (PHI) is so sensitive, fraudsters are drawn to it. Security must advance in step with the industry's growing data-centricity and adoption of new data-sharing technologies.

5.1. Adapting regulatory environment

The regulatory environment is changing, which is one of the biggest shifts happening. New legislation will probably replace or modify laws like HIPAA because they don't offer enough precise direction for the data transfer and security requirements of today. Sector data professionals need to get ready to adjust to these new laws

5.2. Increased patient authority and access

Increasing patient access is another control development that is reshaping healthcare data security. Technologies like healthcare meet consumer demands for greater openness and control over their medical information. It might be difficult to strike a balance between anonymity and accessibility.

Expanding access to patients who might not have through cybersecurity knowledge raises concerns because restricting access privileges is essential to data security. In 2019, 31% of healthcare data breaches were due to simple human error, and medical groups are less able to train patients than they are employees. Data experts must therefore create a data access platform that takes into consideration user's propensity for making errors.

5.3. Technology of data security

The main focus of any company's cybersecurity strategy should be on protecting corporate data loss. This covers information that is stored, transferred**,** and used.

5.3.1. Data protection technology types

Data protection is essential because hackers constantly search for ways to break into business networks. Enterprises can use the following seven technologies to correctly protect data.

1. **Firewalls**

The first layer of protection in a system is a firewall. It is made to prevent unauthorized sources from getting access to corporate info. A router acts as a bridge between a private or business network and the open internet. Firewalls help prevent malware and other unauthorized traffic from connecting to devices on a network by using pre-configured rules to examine all packets entering and leaving the network.

2. **Authentication and authorization**

Authentication and authorization are two procedures used to make sure that only authorized users can access company data. Users must prove they are who they say they are in order to be authorized. A secret, like a password or pin, or biometric authentication can be used as this evidence. Users may be required to provide one or more extra factors when logging in, known as two-factor authentication or multifactor authentication, depending on the authentication scenario (MFA).

3. **Data encryption**

To keep data private while it is at rest and in transit between authorized parties, data encryption transforms it into coded ciphertext. Data encryption prevents unauthorized users from viewing the information in its initial plain text form. If hackers obtain encrypted material, it is useless.

4. **Data masking**

Data filtering hides data so that they can't understand what they have taken, even if they exfiltrate it. Contrary to encryption, which encrypt data using encryption algorithm, data masking includes swapping out real information for identically fake information. The business can also use this information in situation were using actual data is not necessary life software testing or user training.

5. Hardware-based security

Physically securing a device is a component of hardware-based security, as opposed to relying exclusively on software that has been loaded on to the hardware. Companies need protection build into the silicon to guarantee hardened devices because attackers target every IT layers.

6. Data backup and resilience

Particularly if they want to completely recover after a data breach or other catastrophe, organizations should save multiple copies of their data. Companies that have data backups in place can restart regular business operations more quickly and without as many hiccups. Organizations need safeguards in place to keep the backed-up data safe and usable in order to guarantee data resilience.

7. Data erasure

Organizations must ensure that data is correctly deleted and that it cannot be recovered. This method of entirely overwriting stored data, also known as data erasure, renders the data unrecoverable. Data erasure, also known as data destruction, frequently entails making data unreadable after deleting it.

5.4. Future medical technology

Figure: Future of healthcare

Due to artificial intelligence, healthcare services are likely to undergo significant change in near future. Ai makes the lives of patients, medical staff, medical students, and hospital manager easier by performing tasks that would typically be completed by humans, but in a fraction of the time and cost.

VI.CONCLUSION

Privacy protections and ethical health studies both benefit society in significant ways. In order to perform ethical research and improve both human health and healthcare, it is crucial to safeguard research participants' rights and keep them safe from harm. Protecting people's interests is the main justification for safeguarding personal privacy. On the other hand, the main justification for gathering personally identifiable health data for medical study is to aid society. But it's crucial to emphasise that privacy also has worth on a societal level because it enables the conduct of complex activities like research and public health initiatives in ways that uphold people's dignity. Also crucial to note is how health study can assist people, such as when it makes it easier to get access to novel treatments, better diagnostics, and more efficient methods to treat patients and prevent illness.

In accordance with the Health Insurance Portability and Accountability Act of 1996, the U.S. Department of Health and Human Services (HHS) created a set of federal standards for safeguarding the privacy of personal health information (HIPAA). 1 The HIPAA Privacy Rule outlined specific guidelines for the uses and disclosures that "covered entities" are allowed to make of individuals' personally identifiable health information, also known as "protected health information" (health plans, health care clearing houses, and health care providers who transmit information in electronic form in connection with transactions for which HHS has adopted standards under HIPAA). 2 The Privacy Rule's main objective is to guarantee that people's health information is appropriately secured while enabling the information flow required to support high-quality healthcare. The Privacy Regulation also included specifications.

VII. REFERENCES

[1] Karim Abouelmehdi , Big healthcare: preserving security and privacy. Department of computer science laboratory LAMPI and LAROSERI, Chouaib Doukkali University, EI jadida, Morocco. Abouelmehdi et al. J Bigdata (2018) 5: 1.
[2] Devan McGraw and Kenneth D. Mandi, Privacy protection to encourage use of health-relevant digital data in a learning health system. Harvard medical school, bostin, MA, USA.Npj Digital Medicine (2021)4:2; https://doi.org/10.1038/s41746-020-00362-8
[3] Dingyi Xiang and Wei Cai, Privacy Protection and Secondary Use of Health Data.Biomed Res Int. 2021; 2021: 6967166. Published online 2021 oct 7. doi: 10.1155/2021/6967166
[4] National Academics Press (US), Washington (DC)
[5] James Scheibner, Marcello Ienca & Effy Vayena**,** Health Ethics and Policy Laboratory, Department of Health Sciences and Technology (D-HEST), ETH Zürich, Zurich, Switzerland ,James Scheibner, Marcello Ienca & Effy Vayena
[6] Barbara Blechner 1, Adam Butera, Health Insurance Portability and Accountability Act of 1996 (HIPAA): a provider's overview of new privacy regulations. J Am Med Inform Assoc. 2008 Nov-Dec;15(6):729-36. doi: 10.1197/jamia.M2547. Epub 2008 Aug 28.PMID: 18756002
[7] T J Kasperbauer, Protecting health privacy even when privacy is lost. Correspondence to Dr T J Kasperbauer, Center for Bioethics, Indiana University School of Medicine, Indianapolis, IN 46202, USA; tkasperb@iu.edu
[8] Ahmed Altameem, Viacheslav Kovtun, Mohammed AlMa'aitah, Torki Altameem, Fouad H, Ahmed
E. Youssef, Patient's data privacy protection in medical healthcare transmission services using back propagation learning. **Privacy preserving monitoring protocol for Cyber–Physical System**
Computers and Electrical Engineering, Volume 102, 2022, Article 108232