BALANCING CONFIDENTIALITY AND INNOVATION: SAFEGUARDING PATIENT PRIVACY IN AI-ENHANCED HEALTHCARE

Ambika Sharma, Delhi Metropolitan Education Affiliated to GGSIPU

Paritosh Kumar Gupta, Lloyd Law College

ABSTRACT

Our quest for technology should not be oblivious to the country's real problems: social exclusion, impoverishment and marginalisation. Dignity and rights of individuals cannot be based on algorithms or probabilities-

- Justice Chandrachud

Privacy is a socially crafted idea shaped by cultural, legal, and technical variables rather than an innate quality. The limits of patient privacy are constantly being renegotiated in the context of AI-enhanced healthcare as new technologies become available. For instance, the distinction between private and public health information is becoming hazier due to the increasing use of health-tracking devices and computerized medical records. A lesson can be learned from the Cambridge Analytica affair, in which user data from Facebook was obtained without authorization. Breach incidents in the healthcare industry, such as illegal access to patient records or data leaks from AI algorithms, can significantly damage public confidence in the system. Preserving patient privacy in the age of digitalization and big data is crucial, as is utilizing artificial intelligence (AI) to its fullest potential in healthcare. The complex relationship between privacy and innovation in healthcare is examined in this review, with a special emphasis on the legal, ethical, and technological aspects of data privacy protection. The conversation covers the advantages and difficulties of artificial intelligence (AI) and machine learning systems in the healthcare industry, highlighting the necessity of strong frameworks to protect patient privacy. The analysis highlights the changing environment of privacy policies and the implications for healthcare data management by drawing on ethical principles, legal frameworks like the Belmont Report, and emerging data protection legislation like the Digital Personal Data Protection Act. It also discusses the particular difficulties that nations like India face, emphasizing the complexity of privacy protection in light of various sociocultural elements

and legal frameworks. The analysis ends by promoting a fair strategy that gives equal weight to patient privacy and medical innovation. It also highlights the significance of open communication, the moral use of AI-driven solutions, and the ongoing assessment of privacy protection protocols in the healthcare industry.

Keywords: Privacy, Data, Healthcare

INTRODUCTION

In the era of vast digital repositories and BIG DATA, data privacy has emerged as a paramount concern, particularly in healthcare, where the misuse of data poses significant risks to patient confidentiality.

As custodians of data, healthcare professionals grapple with ethical and legal constraints of protecting doctor-client confidentiality norms and using medical records for in furtherance of the medical R&D process. Consequently, the digitalization of the healthcare system has posed significant advantages and disadvantages.

AI and machine learning systems enable innovations like data retrieval, high-definition medical samples, teleconsultations, and surgery assistance, but also raise concerns about privacy and security due to massive data stores and increased risk of data theft.

In light of these limitations and cutting-edge advantages and the need to balance the usage this review intends to explore the myriad concerns, legal frameworks, and common practices in safeguarding data privacy in the healthcare sector.

We aim to provide insights that can inform ethical and responsible data stewardship in the healthcare industry.

Although, there isn't yet a standard procedure in place for data encryption and sharing in AI-based research. Instead, after receiving permission from institutional ethics committees, these protocols are decided upon a project-by-project basis.

While the inclusion of AI and Machine learning systems in the health sector will yield an efficient system of healthcare deliverance whereby, medical conditions, screening, radiology, and other health-related decisions can be made more efficaciously with the aid of a set database and algorithms.

But this rapid rise in data collection and exchange has also brought attention to a big, pressing problem i.e. the necessity to protect the privacy of medical records is a major issue as a result of the quick increase in data collection and interchange.[1]

For instance, a multitude of open-source repositories, such as Kaggle and The Cancer Imaging Archive (TCIA), provide access to large medical datasets, which aid in the creation of consistent protocols and repeatable results in AI research[2].

Therefore, the optimal utilization of AI as a defence wall by medical institutes for tackling the issue of data privacy and data theft serves as a potent mechanism to draw a harmonious construction between individual data privacy and medical development.

One way of achieving this aspiration is via data anonymization. This method serves as a pivotal apparatus in safeguarding healthcare data privacy within AI frameworks.

Whilst, healthcare practitioners and scholars often leverage extensive datasets for research purposes, ensuring patient confidentiality by employing AI-powered tools to eliminate identifiable information is a potent method to ensure patient privacy.

THE INTERPLAY BETWEEN PRIVACY AND HEALTHCARE DISPENSATION

Privacy is vital in patient-provider interaction, supported by both consequentialist and deontological ethical grounds. The fiduciary nature of this connection and the expectation of reciprocal confidence between patients and healthcare professionals give rise to its significance[3].

The Belmont Report, published in 1979, is a crucial bioethical document in the US, addressing unethical research practices like the Tuskegee Syphilis Study, where participants were withheld without their consent.

[1] Roy, Soumit. (2022). PRIVACY PREVENTION OF HEALTH CARE DATA USING AI. 10.5281/zenodo.7699408. (last accessed on 30th January 2024)
[2] Lee RS, Gimenez F, Hoogi A, Miyake KK, Gorovoy M, Rubin DL, A curated mammography data set for use in computer-aided detection and diagnosis research, 4 Sci Data 170177 (2017) (last accessed on 30th January 2024)
[3] Paarth Naithani, Protecting healthcare privacy: Analysis of data protection developments in India, Volume Number Indian Journal of Medical Ethics Page Number (December 18, 2023).

The Belmont Report[4] in the USA highlights the 3 core linchpins of data ethics namely principle of respect for persons, beneficence, and justice. In addition, it has enumerated two bioethical principles of |non-maleficence and Respect for Autonomy.

These principles play a valuable guideline drawing an ethical balance between individual autonomy/ privacy and clinical utilization of data.

These collective efforts bolster the security of sensitive patient information, aiding healthcare institutions in effectively navigating the complexities of digital healthcare while prioritizing privacy and fostering trust.

For instance, to train and test deep learning algorithms, openly accessible databases such as Optimam and the Digital Database for Screening Mammography (DDSM) provide carefully selected and annotated mammogram images[5].

India faces privacy compounded due to high illiteracy rates, limited awareness, and challenges in obtaining informed consent. This raises concerns about data protection and informed consent, crucial in medical procedures and online services.

Regularly individual health data is being gathered as a result of the growth of mobile applications and websites that support telemedicine, counselling, wellness, and pharmaceutical sales like Netmeds, PharmEasy Apollo Pharmacy etc.[6]

Consequently, the health information of individuals becomes readily available to third parties outside the preview of the doctor-patient relationship, which raises the alarm of privacy risks, harm to one's reputation, prejudice, extortion, psychological distress, denial of service, and restrictions on one's right to free expression.

To address these issues a robust framework and algorithm are required to be used by medical institutes to protect the mammoth data being stored and to have a vigilance cell/committee set

[4] Hit Consultant, "Guarding Patient Privacy in the Age of AI Healthcare" (Nov. 27, 2023), https://hitconsultant.net/2023/11/27/guarding-patient-privacy-in-the-age-of-ai-healthcare/ (last accessed on 30th January 2024)
[5] Id.
[6] Rajaretnam T. Data mining and data matching: Regulatory and ethical considerations relating to privacy and confidentiality in medical data. J Int Commer Law Technol. 2014 Jan; 9(4):294-310. (last accessed on 30th January 2024)

up at both institute and national levels to have a speedy recovery and tracking of data theft and falsification.

Albeit, corrective usage of AI can also provide medical institutes with a defensive edge in the protection of data by employing anomaly-detecting AI-based systems.

This will help to assess real-time alerts for possible security breaches or unauthorized access attempts that can be sent by these systems through behaviour analysis and the identification of deviations from typical usage patterns.

AI algorithms can enhance data encryption techniques for patient information security, using advanced methods like homomorphic encryption or differential privacy to prevent interceptions and ensure unreadable data.

AI-driven authentication systems improve access control by utilizing biometric, behavioral, or multi-factor methods, ensuring only authorized personnel can access patient data based on user behaviour and context.

AI-powered threat intelligence platforms help medical institutes identify emerging threats and security vulnerabilities, enabling proactive defence against cyber threats and mitigating patient data security risks.

Medical institutes can enhance patient data protection by integrating AI-driven solutions, ensuring compliance with regulatory requirements and privacy standards, but ethical implementation is crucial.

CONTINGENCIES UNDER THE INDIAN LANDSCAPE

The Personal Data Protection Bill, of 2019, which sought to provide comprehensive data protection laws in India, addressed these issues. However, the Digital Personal Data Protection Act, of 2023 has subsequently taken its place.

Section 43A of the IT Act and the SPDI Rules, which were issued under Section 43A, have been superseded with the implementation of the DPDP 2023. Nonetheless, the new general law does not supersede health-specific data protection regulations, such as the Health Data Management Policy (HDMP) and the Digital Information Security in Healthcare Act (DISHA).

DPDP 2023 differs from previous data protection frameworks by not defining sensitive personal data, allowing processing without express consent, giving data principals ownership rights, privacy by design policy, or mandating direct care for health data.

From a comparison drawn between the two legislations, it can be concurred that the DPDP 2023 has a lower degree of protection for health data compared to the DPB 2021 due to uncertainty in data categorization and security, the ability to process data without express authorization, and the lack of ownership rights for data principals.

It also lacks requirements for direct care and best interest use and does not include privacy by design regulations or mandates for Data Protection Impact Assessments. The effectiveness and implementation of the DPDP 2023 remain uncertain.

The judiciary has frequently prioritized the public interest over individual privacy when addressing disputes between the "right to be let alone" and other rights.

The *'right to privacy'* is not absolute, as demonstrated by the case of *Sharda v. Dharmpal*[7], where the wife was forced to undergo a medical examination to prove her mental illness to proceed with her divorce. The court held that the absence of such data would impede deciding on the facts of the case.

In the case of *Shri G.R. Rawal v. Director General of Income Tax (Investigation),* the court examined the scope of Section 8(1)(j) of the Right to Information (RTI) Act, 2005, which prohibits the disclosure of 'personal information' in response to an application.

However, the Central Information Commission ruled that this exclusionary rule could be overridden if there is a larger public interest justifying disclosure.[8]

While exceptional circumstances may warrant disclosure in the public interest in certain instances, the judicial trend observed in such cases has resulted in a gradual erosion of principles concerning personal liberty, autonomy, and privacy.

[7] Sharda v. Dharmpal, AIR 2003 SC 3450.
[8]Nimisha Srinivas & Arpita Biswas, Protecting Patient Information in India: Data Privacy Law and Its Challenges (last accessed on 30th January 2024)

The current landscape of pharmacovigilance advocacy in India, primarily led by conglomerates within the pharmaceutical industry such as the Indian Pharmacopoeia Commission (IPC), emphasizes utilizing partially de-identified information for advancing medical research aimed at discovering new treatments.

While this approach is driven by the potential benefits it offers in facilitating medical advancements, it also raises concerns regarding the erosion of data privacy principles.

Advocating for the use of pseudonymized or partially de-identified information may inadvertently undermine individuals' privacy rights, as it could potentially compromise the confidentiality and security of personal health data.

As such, there is a need for careful consideration and balance between advancing medical research and ensuring robust data privacy protection measures are in place to safeguard individuals' sensitive information.

CONCLUSION

A strong dedication to protecting patient privacy must coexist with the pursuit of innovation in AI-enhanced healthcare. The delicate balance between innovation and confidentiality calls for a multifaceted strategy that takes sociological, ethical, and technological aspects into account.

The security of patient data is crucial for AI-related research, as it is used in healthcare applications, including protected health information and user-generated data from sources not covered by HIPAA regulations.

It is important to recognize that privacy is a dynamic and developing construct that is affected by ethical considerations, technology breakthroughs, and societal conventions as we negotiate this terrain. The complex interactions between privacy, trust dynamics, structural inequality, monitoring, and moral quandaries are brought to light by sociological insights. Repercussions in healthcare outcomes and the Cambridge Analytica incident serve as examples of how critical it is to manage these difficulties.

AI in healthcare uses protected health information and user-generated data, but the risk of re-identifying data through cross-referencing remains, especially when supported by tech giants like Google, Apple, and Meta, despite removing necessary identifiers.

Transparency in AI use in healthcare fosters patient trust by demonstrating a commitment to privacy and preferences. Institutions should communicate AI adoption, clarify data usage, and empower patients to manage electronically Protected Health Information, highlighting the growing importance of transparency in healthcare.