American Journal of Medicine and Medical Sciences 2024, 14(12): 3134-3140
DOI: 10.5923/j.ajmms.20241412.11

Ethical Data Management in Healthcare Industry

Anshuman Srivastava[1,*], Rishika Sharma[2], Ritvik Srivastava[3]

[1]Department of Family Medicine, Family Health Care Network, 1632 West Glendale Avenue, Visalia CA 93291, USA
[2]Department of Pediatrics, Family Health Care Network, 5151 Lakewood Dr, Visalia CA 93291, USA
[3]Student Grade XI, American High School, Fremont CA, USA

Abstract In today's hyper competitive digital landscape it's very important for healthcare providers to manage data as per ethical standards. Patient data is the cornerstone on which patient care, outcome and research is being carried out. Therefore, ethical standards of handling patient data are extremely crucial. One of the most important challenges is how to secure patient data (private) while at the same time using it well. The entire cycle includes ensuring patients are well informed about how their data will be used and as much consent is obtained amongst other measures. Healthcare datasets are supposed to be managed well, safeguarding patient privacy and ensuring that any information used is both secure and released with consent & as per their preferences. And these behaviors are all reinforced by good data governance principles and practices such as using strong encryption, pursuing or implementing proactive audits and compliance standards like HIPAA, GDPR to name a few. In practice, managing data and ensuring that it is used in an ethically correct manner also means reducing the risk of misuse and unintended bias-in-powered analytics (as many biases are not algorithmic but instead stem from incorrect interpretation). Putting a spotlight on how data is deployed and decisions are made, particularly in health care, is critical to patient trust but equally important if patient data is actually going to be helpful rather than cause harmful consequences for patients. Beyond legal stipulation, in the interest of prioritizing ethical standards, health organizations have an infinitely greater impact on shaping a professional culture that is based upon mutual respect and accountability among medical specialists as well as safety of patients' rights for confidentiality resulting in maintaining quality improvement at health care.

Keywords Ethical data management, Patient privacy, Data security, Informed consent, Data governance, Regulatory compliance

1. Introduction

In the rapidly connected digital age, data is integral to improve patient care, to facilitate treatment, and for research. While this reliance is critical for proper treatment, there is an obligation that comes with it which is the ethical handling of personal health data. Data Management is an umbrella term that comprises a set of principles and practices concerning data collection, preservation, sharing and use ensuring the respect of the privacy of patients, maintaining trust and compliance with legal frameworks.

But for healthcare organizations attempting to navigate the difficult regulation around data management, they are met with challenges such as protecting patient privacy, obtaining informed consent and managing ethical considerations. What is at stake more than ever before, providers and their organizations are acutely aware of two things with regard to trust in healthcare (1) how important it is and (2) the cost of a breach.

Ethical data management is in this case understood as a regulative framework that ensures transparency, accountability and integrity. Further, it enables patient advocacy while promoting new approaches to the use of data that will ultimately bring about better health outcomes. These guidelines are important because it tells the patient that they can trust their healthcare provider to act according to a set of moral and ethical standards, creating a sense of respect and moving the advancement of health care forward in a responsible manner.

It's extremely critical to look at the ethics behind how data is managed in healthcare, and as an asset and its role in creating a fairer and stronger healthcare system. Current practices for regulating the processing of personal data are oriented principally towards notions of governance, risk management, and regulatory compliance - based on data protection laws that have, in some jurisdictions, been in place for decades. Despite this framework, individuals are likely to encounter uses of their personal data which, while legal, may appear to lack fairness or legitimacy, [1].

2. Literature Review

Literature review on the Ethical Data management in the Healthcare industry. Each entry summarizes the key findings, methodologies, and implications of relevant studies. List of literature review as mentioned in the table.

* Corresponding author:
anshuman.srivastava87@gmail.com (Anshuman Srivastava)
Received: Nov. 10, 2024; Accepted: Nov. 28, 2024; Published: Dec. 10, 2024
Published online at http://journal.sapub.org/ajmms

3. Importance of Data Management in Healthcare

Data management is essential in healthcare for several reasons, all of which add to the success, safety and efficiency of patient care and organization performance.

Information management here is understood as the power of health professionals to control the disclosure or withholding of information to their patients (Ewuoso et al., 2017). This encompasses information about diagnosis, prognosis, and preferred available therapy (Swaminath, 2008).

Touching upon its significance, here is a scatter of few points for quick reference:

Improved Patient Care: Better data management allows for a fuller patient history and better determinant of treatment plans and outcomes. Such comprehensive care implies more data-informed decision-making, personalized treatments and even better patient results. When the data is accurate, clinicians can spot trends, pinpoint those at-risk patients ahead of time and intervene quickly.

Improved Operational Efficiency: Can be improved significantly when data management is automated and workflow is optimized. This approach is achieved with integration of multiple data sources like EHR, RCM etc.

Regulatory Compliance: Inorder to protect data and ensure proper usage, regulations are mandated like HIPAA in the USA. These regulatory compliances make its necessary for providers to have proper data management practices ensuring trust & transparency.

Data-Driven Decision Making: In other words, data analytics has the potential to empower healthcare organizations through extensive digital capabilities that enable them to make strategic life-saving decisions based on complex analysis of information. These include recognizing areas where operations are less than optimal, predicting what patients will need in the future and assessing how well treatments work. With the help of insights care givers can make informed decisions to improve quality of care.

Enabling Research and Innovation: Quality, organized data is a critical component of medical research and innovation. But data management can enable scientists to explore huge sets of data, and thus, seek novel treatments, know the patterns of diseases and assess intervention effectiveness. This kind of knowledge will ultimately help us make great strides in healthcare and, consequently, public health.

Patient data, managed appropriately, opens opportunities for patient-centered engagement and empowerment delivered via secure websites or portals. By ensuring that their health information is readily accessible, patients are more empowered to participate in the care of their condition and comply with treatment regimens which result in better health output.

Risk Management and Safety: An essential aspect of healthcare is data management, as it helps in recognizing and managing risks effectively. Organizations can use this information to institute safety protocols or to improve quality assurance by examining adverse events, medication errors and patient outcomes.

Integration and Cooperation: With proper data management, the interoperability of health systems and other specialists can be facilitated to share information quickly. Such collaboration assures continuity of care, reduces duplication and most importantly elevates patient experiences.

Data management is critical to help make healthcare safer. It is the foundation of all patient care, operational efficiency and organizational viability. In the dynamic urban environment, the healthcare industry is changing as well and there will come new challenges waiting for data management to answer them and foster a better quality of care.

The privacy and confidentiality of patients should be protected with serious caution, because concerns about privacy and confidentiality limit the ability to link external data to a person's insured data in ways that could otherwise personalize services and improve consumer experiences with healthcare (Yuen-Reed & Mojsilovi, 2016). Because so much health care data is centralized, it is especially vulnerable to misuse. (Mohr et al., 2013). There are a number of key ethical issues in the use of big data in healthcare likeInformed consent, bias, privacy, ownership, data security, [8].

4. Ethical Data Management in Healthcare

Healthcare data management involves the creation, storage, organization, processing, archiving, and destroying of unnecessary data. It involves the processing of management of health data lifecycle., [5].

Ethical data management is critical in healthcare to retain patient confidence, compliance with rules and regulations, and the accuracy of sensitive health information. Best practice guidelines for an ethical approach to data by organizations.

Informed Consent: Patients have rights to know exactly how their data will be utilized, preserved, and distributed. This will involve the provision of unambiguous and accurate information about why the data is being collected, what it may be used for and possible risks and rewards. An open explanation of consent, which permits the patient to be involved in the decision making process and not a veneer for irrational expanse.

Data Minimization: Healthcare organizations should follow a data minimization approach, meaning only the necessary data required per purpose should be collected. By doing this, should there be a data breach at any point, the exposure would not be as high, and hence patients' privacy would still be protected.

Pseudonymization and Anonymisation: Wherever possible, patient data should be cleaned of identifiers and de-identified. The practice is conducive to data analysis and research that are useful, while maintaining patient confidentiality.

Store Data Securely and Add ControlAccessType: Employing strong security ensures that your health data remains sensitive. Everything from encryption, to secure

access controls, down to regular security audits aimed at ensuring that they are the only people with legal access to patient data.

Openness and Responsibility: Transparency in Data Management Healthcare organizations should be transparent around their management of data. These things involve, for example, transparency in the data handling rules and indicators to find out if patients inquire about their information usage. Working to create accountability structures enforces ethical standards.

Conventional Training and Learning: Continual education for healthcare personnel regarding data privacy, security and ethics is crucial. This in turn helps to create a good culture around accountability and awareness of data related issues within the organization.

Artificial Intelligence usage Ethics: The ethical questions that come with AI implementation have to be resolved as it is gradually being woven into healthcare. AI algorithms should be designed to minimize bias, preserve patient privacy, and explain how decisions are made with data.

Data Sharing Agreements: Providers have to stop sharing data to third parties or have clear agreements with them on how they will use your data and put security measurements in place, and agree on the ethical compliance standards. It controls how shared data is accessed in an extremely responsible and ethical way.

Patient Empowerment: Empowering patients to manage their own data will promote ethical standards. Giving them their own record to view and some ability to make choices in regards to sharing that information creates an environment of ownership, accountability, and trust.

Ethical data management is not just a regulatory requirement, healthcare organizations have an ethical duty to protect patient rights and breed trust. These processes help organizations set up secure, open and ethical ways of dealing with delicate health information that can improve patient care and outcomes.

Current practices for regulating the processing of personal data are oriented principally towards notions of governance, risk management, and regulatory compliance - based on data protection laws that have, in some jurisdictions, been in place for decades. Despite this framework, individuals are likely to encounter uses of their personal data which, while legal, may appear to lack fairness or legitimacy. Such uses may lead us to conclude that third parties are failing to take due account of our wishes and preferences. An organisation's handling of personal data might fall short of our expectations in a number of ways, such as through over collection, insufficient care, unexpected or unwelcome use, or excessive sharing, [4].

Data privacy and the rise of ethical challenges continue to undergo a detailed analysis as part of the digital revolution. Safeguarding data privacy constitutes a fundamental right, often overlooked amid the exchange of data transfer for commercial and scientific purposes [28].

A failure to disclose information could also expose a health professional to legal liability (Murray, 2012).

5. Regulations Around the World for Ethical Data Management in Healthcare

Ethical data management which is key to better patient care is governed by different national regulators worldwide. The governing bodies act as custodian of best practices reflecting the importance of protecting patient data and integrity.

Scholars have examined the security risks associated with storing and transmitting sensitive patient data in the cloud, emphasizing the importance of robust encryption, access controls, and data governance mechanisms. Moreover, regulatory compliance with laws such as HIPAA and GDPR has been a focal point, with researchers exploring strategies for ensuring compliance while leveraging the benefits of cloud computing, [9].

Here's an overview of key regulations across different regions:

United States

Health Insurance Portability and Accountability Act (HIPAA): Enforces rigid privacy / security measures around protected health information (PHI). HIPAA mandates all stakeholders like providers and insurers including their business associates, adhere to data usage & protection policies, [29].

Health Information Technology for Economic and Clinical Health (HITECH) Act: Toughens privacy and security protections within HIPAA. Promotes the meaningful use of health information technology within EHR ecosystem.

Growing concern over healthcare information security in the USA has led to increased regulation and changes in the required security practices needed to achieve compliance. However, some surveys by both industry groups and the US Department of Health and Human Services noted wide disparity both in security practices and in perceived compliance with federal (Health Information Technology for Economic and Clinical Health (HITECH)/Health Insurance Portability and Accountability Act (HIPAA)) and state regulations, [10,11].

Ethics has been core to the practice of medicine at least since the formulation of the Hippocratic oath [26], but the digital era introduces new risks which require ethical responses, [26-27].

European Union

General Data Protection Regulation (GDPR): GDPR is one of the most expansive data protection laws across the globe from Europe, with processing of personal information, including healthcare information covered mostly by it. It builds on the principles of privacy by design, consent and data minimization, gives people rights to access their data and tells companies how to apply this in practice. Non-compliance could result in hefty fines.

European Data Protection Board (EDPB) Guidelines: Is the other complementary guidance on the application of GDPR to health data, building on issues related to

transparency and patient rights.

HIPAA establishes standards for the protection of sensitive patient information, mandating measures such as encryption, access controls, and audit trails to safeguard electronic protected health information (ePHI). GDPR, on the other hand, applies to the processing of personal data of individuals within the European Union (EU), requiring organizations to obtain explicit consent for data processing, implement data protection measures, and report data breaches promptly [12].

United Kingdom

Data Protection Act 2018: Puts GDPR in place across the UK, laying out the legal structure for data security and privacy. It has details of how to get valid consent and accountability including handling personal sensitive health data.

National Health Service (NHS): The NHS has its own red lines on data governance and confidentiality, particularly in terms of ethical health data research and innovation.

Canada

Personal Information Protection and Electronic Documents Act (PIPEDA): PIPEDA (Personal Information Protection and Electronic Documents Act): Specifically addresses how private-sector organisations collect, use or disclose personal health data.

Provincial Regulations: There are provincial laws specific to health information (e.g., Health Information Act in Alberta and Extra-Provincial Law Application and Extension Act in Ontario) that would protect health data.

PIPEDA would also apply to health care providers who are funded through the public health insurance system. Though PIPEDA does not apply to public hospitals as the core activities are not commercial; non-core activities, such as a pharmacy carrying on a commercial organisation in a hospital space could be subjected to PIPEDA. Quebec, British Columbia, and Alberta have provincial privacy laws substantially similar to PIPEDA and therefore PIPEDA will not be applied in those provinces on private sector commercial activities that occur within the territorial boundaries of the province (Bernier, A & Noppers, M.B., 2020), [15].

Australia

Privacy Act 1988: The Australian Privacy Principles (APPs) also include responsibilities with respect to consent, security and access of personal information.

My Health Records Act 2012: Establishes the governance framework for my Health Record, an online system through which individuals can securely access their health information and contribute to maintaining their protective privacy.

Asia

Japan: Health information falls under the Act on the Protection of Personal Information [APPI], which in principle requires personal data to be collected based on cons.

India: The Personal Data Protection Bill: It is this bill which aims to introduce a data protection regime that covers a vast range of issues, including (through specifically designed sections) protecting health data.

Interpreting and implementing regulatory requirements accurately requires expertise and resources, adding to the complexity of compliance efforts.Finding the right balance between security and accessibility is crucial to ensure that patients can access their health information when needed while maintaining the confidentiality and integrity of the data [13-14].

Although the healthcare industry faces different regulatory frameworks across regions for ethical data management practices, all tie down to common principles such as providing patient privacy and informed consent among others. With the technological advancement in healthcare, it is important that these regulations are still followed for companies looking to maintain ethical standards in data management.

6. Existing Study

Several studies have addressed ethical data management in the healthcare industry, focusing on various challenges and frameworks. Kaye and Heeney (2015) conducted a scoping review highlighting the ethical dilemmas associated with health data sharing, emphasizing the necessity of informed consent (BMC Medical Ethics). Reddy and Jonnalagadda (2020) explored the balance between data privacy and patient autonomy in the context of big data, discussing the implications for ethical practices in healthcare (Journal of Medical Ethics). Additionally, Lemaire and Mackey (2019) proposed a framework for ethical data management in health research, offering guidelines to ensure responsible handling of sensitive health information (International Journal of Medical Informatics). Together, these studies underscore the critical importance of ethical considerations in managing healthcare data., [16-18].

7. Challenges & Considerations

Principles of data privacy, bias and risk in data sharing makes AI a double-edged sword when it comes to ethical data management in healthcare. In the healthcare, protecting patient privacy is vital as AI systems use large datasets to inform healthcare decisions. The large volumes of sensitive and detailed personal health data increase the risk of access, breaches of secure storage facilities, or misuse. While the utmost compliance with peppered regulations like HIPAA (Health Insurance Portability and Accountability Act) is a necessity, the task of governing through these rules spanning various jurisdictions and healthcare systems brings along its own set of challenges. Few challenges involve a careful balance between the use of AI for predictive analytics and personalized treatment, and effective patient privacy protection.

Furthermore, machine learning models are also susceptible to bias owing to the datasets they have been trained on producing biased clinical outcomes (which is a greater concern

with non-representative mainstream data used in training AI systems). as the datasets may not represent every patient group. This could result in unfair treatment suggestions or misdiagnoses affecting underrepresented populations. In addition, the process of exchanging healthcare data between platforms and institutions or with third-party vendors increases the vulnerability of patient data to outsiders. To mitigate these many risks, its important to build secure and ethical frameworks for data sharing accompanied with informed patient consent.

As the AI models are trained based on data, if the distribution of training data is biased or do not sufficiently capture the underlying reality of what would be expected in real use, this will result in systems perpetuating these biases and may lead to unfair outcomes through decision-making, [31].

8. Future Scope

Technology Changes, Regulation and Patient Expectations drive Ethical data management in Healthcare for better patient care.

These are some of the areas where we can expect to see growth and change in ethical data management:

Artificial Intelligence & Machine Learning Integration: Ethical data management will need to give output which is unbiased. Transparent algorithm development is warranted as AI and machine learning increasingly enter mainstream, healthcare ecosystems. This would include setting guidelines in areas such as the ethical use of AI-based assistance in diagnostics, treatment suggestions and patient monitoring.

The advent of artificial intelligence (AI) in healthcare presents unprecedented opportunities for improving patient outcomes and healthcare efficiency. However, it also introduces significant challenges in data management and governance, particularly in balancing the drive for innovation with ethical responsibilities, [25].

Advance Analytics: Enhanced decision-making, transparency and accountability in ethical data management are made simple with advanced analytics, which therefore become an integral part of ethical data management. Healthcare providers are trained to examine and interpret trends based on expanded patient data through condensed ethical predictive modeling, machine learning, and data mining methods. They can identify trends, optimize treatment plans and improve patient outcomes by leveraging data gained through them while maintaining the integrity of data privacy using advanced encryption and secure access protocols over it. Additionally, with advanced analytics it is more useful for complete and bias-free information in datasets by identifying patterns that may lead to discriminatory practices which helps train AI models on diverse & representative data. Incorporating ethical principles in the analytics process can help healthcare companies to maintain responsible and equitable health data use while improving patient care and trust in AI technologies.

Greater Patient Empowerment and Control: Patients need more control of their data and this is only getting easier to do. In the future data management systems might offer more flexible patient portals and tools to manage their preferences about who can access their information and for what purpose.

Open data and Data interoperability: Interoperability of healthcare systems will be a priority. This type of open source transparency with an ethical framework is required to be in place so that data can be shared across providers. A prerequisite of this however will be the establishment of agreed frames and benchmarks that respects patient consent and security.

Blockchain Technology: Through blockchain technology, data management can be done in a viral and consistent manner. Decentralized, transparent and immutable storage solutions while at the same time provides privacy in healthcare. Blockchain guarantees the integrity and confidentiality of sensitive patient information. Each piece of information generated or updated is securely recorded on an irreversible ledger that cannot be corrupted. This gives us more control over who can see our data, as it allows us to allocate ownership and transfer protection accordingly. In addition, it offers data sharing across stakeholders (hospitals, doctors, researchers etc.), with maintaining patient consent and privacy. By providing a transparent audit trail, blockchain keeps any unauthorized access away and reduces the risk of data breaches.

Regulatory Evolution: With further technological improvements, regulations may adapt to regulate new demand issues and guarantee moral practices. Legal rulings and statutes are constantly evolving, companies will have to adjust their data management strategies accordingly.

Telemedicine and Continuous Monitoring: The increasing adoption of telehealth and remote monitoring solutions has produced higher amounts of health data that are both relevant and sensitive. Given that increasing the extent of virtual care threatens patient security and privacy, ethical data management practices will require stringent measures to protect this invaluable information.

Focus on Equity and Inclusion: This extends to consideration of issues such as equity, i.e., ensuring that healthcare data is representative of the entire populace and that algorithms think about all communities. This involves looking at gaps and challenges in data access, as well as the use of research data in particular.

Public Trust and Transparency: As health deals with increasing amounts of data, the ability to build and retain public trust will become a matter of life or death for organisations. Earning patient trust can be accomplished by informed ethical transparency- this means relaying the ethics behind data collection, processing and protection in an easily understandable manner.

Data Ethics Committees: Organisations might start setting up data ethics committees to govern the way they manage their data, embedding ethical considerations in the decision-making process concerning data use and sharing.

Education and training are ongoing: Healthcare professionals should be educated and trained consistently about ethical data management as they continue to face novel

tech and regulations. Performance pay can be more closely aligned to how administrators act towards one another and relates back to using external motivators, instead of intrinsic motivation to build a culture of ethical awareness and accountability in health care organizations.

The landscape of ethical data management in healthcare is complex with various elements, yet to be determined. How healthcare organizations can harness technology for good Patient care and trust-building As the landscape rapidly evolves ethical approach will be crucial in the maintenance of patient rights and healthcare data quality.

The integration of big data in healthcare presents numerous ethical challenges, particularly concerning patient privacy and informed consent. Addressing these issues requires a systematic approach to ethical data management.

The integration of big data in healthcare presents numerous ethical challenges, particularly concerning patient privacy and informed consent. Addressing these issues requires a systematic approach to ethical data management (Miller & Lutz et al. 2020), As healthcare increasingly relies on digital data, the ethical implications of data management practices become more pronounced. Developing a robust framework for ethical oversight is essential for future advancements (Tully & Grady et al, (2021), Digital health technologies introduce new ethical dilemmas in data governance, necessitating a reevaluation of existing practices. Critical review of these frameworks can pave the way for responsible data management in the future (Harney & Ellis et al 2022), Navigating the ethical landscape of health data management is increasingly complex as technologies evolve. Prospective strategies must address the balance between innovation and ethical responsibility, (O'Leary & Kearns et al 2019"), The management of genetic data raises unique ethical considerations that require careful policy formulation. Future approaches must prioritize patient autonomy and data security to foster trust in genetic research, (McGowan & Haga et al 2020), [19-23].

9. Conclusions

In healthcare, good data management is not just a regulatory requirement but a fundamental obligation to the trust between patients and those who provide their care. Healthcare is transforming rapidly with the advancement of technology. so the requirement for strong, ethical practices is more than ever. By leveraging the data insights there is tremendous scope to improve care and foster innovations but at the same time navigating the complexities of data privacy, security and patient consent is a delicate balance.

The Evolution of Ethical Data Management will be Defined by Emerging Technologies, the Rise of Improved Patient Empowerment and a Commitment to Equity & Transparency. Centring around these ethical ideals can go a long way in promoting trust, as well as performance that contributes to the growth of healthcare as a profession.

In conclusion, going forward ethical data management becomes a prerequisite to combat its challenges and exploit the opportunities which are forthcoming so that patient rights should not be encroached upon and healthcare data should responsibly be used for the benefit of all.

REFERENCES

[1] Wilton, R. Trust and ethical data handling in the healthcare context. Health Technol. 7, 569–578 (2017). https://doi.org/10.1007/s12553-017-0206-2.

[2] Tillemans, S. (2008). South African Journal of Bioethics and Law. South African Journal of Bioethics and Law, 1(1).

[3] Swaminath, G. (2008). The doctor's dilemma: Truth telling. Indian journal of psychiatry, 50(2), 83-84.

[4] Wilton, R. Trust and ethical data handling in the healthcare context. Health Technol. 7, 569–578 (2017). https://doi.org/10.1007/s12553-017-0206-2.

[5] Prasad, Sanjana & Rajendra Prasad, Deepashree. (2024). Comparative Analysis of Blockchain Technology in Healthcare Data Management. 10.1007/978-981-99-9043-6_22.

[6] Yuen-Reed, G., & Mojsilović, A. (2016). The role of big data and analytics in health payers transformation to consumer -centricity. In Weaver, C., Ball, M., Kim, G., & Kiel, J. (Eds.), Healthcare information management systems (pp. 399–420).

[7] Mohr, D. C., Burns, M. N., Schueller, S. M., Clarke, G., & Klinkman, M. (2013). Behavioral intervention technologies: Evidence review and recommendations for future research in mental health. General Hospital Psychiatry, 35(4), 332–338.

[8] Olarewaju, Oluwaseun. (2023). Ethical Considerations in the use of big data in Healthcare.

[9] Shah, V., & Konda, S. R. (2022). Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. Revista Espanola de Documentacion Cientifica, 16(3), 50-71.

[10] HHS (the US Department of Health and Human Services). The summary of nationwide health information network request for information responses. USA: Department of Health and Human Services.

[11] Pavolotsky J. Compliance best practices for information security: a perspective. corporate compliance insights. 2011.

[12] Schmidt, A. (2020). Regulatory Challenges in Healthcare IT: Ensuring Compliance with HIPAA and GDPR. Academic Journal of Science and Technology, 3(1), 1-7.

[13] M. Artetxe, G. Labaka, E. Agirre, and K. Cho, "Unsupervised neural machine translation," arXiv preprint arXiv: 1710.11041, 2017. [11]

[14] S. S. Gadde and V. D. R. Kalli, "Technology Engineering for Medical Devices-A Lean Manufacturing Plant Viewpoint," Technology, vol. 9, no. 4, 2020.

[15] Bernier, A., & Knoppers, B. M. (2020). Pandemics, privacy, and public health research. Canadian Journal of Public Health, 111(4), 454-457.

[16] Kaye, J., & Heeney, C. (2015). Ethical challenges in the use

of health data for research: A scoping review. BMC Medical Ethics, 16(1), 12. https://doi.org/10.1186/s12910-015-0009-7.

[17] Reddy, M., & Jonnalagadda, S. (2020). Balancing privacy and patient autonomy in the era of big data. Journal of Medical Ethics, 46(8), 542-546. https://doi.org/10.1136/medethics-2019-105831.

[18] Lemaire, J., & Mackey, T. (2019). A framework for ethical data management in health research. International Journal of Medical Informatics, 123, 33-39. ttps://doi.org/10.1016/j.ijmedinf.2018.11.004.

[19] Miller, T. A., & Lutz, C. (2020). Ethical implications of big data in healthcare: A systematic review. Health Informatics Journal, 26(3), 1910-1921. https://doi.org/10.1177/1460458218788290.

[20] Tully, S., & Grady, C. (2021). Ethical challenges in managing health data: A framework for the future. Journal of Medical Ethics, 47(2), 83-90. https://doi.org/10.1136/medethics-2020-106498.

[21] Ramdurai, B. (2021). Use of artificial intelligence in patient experience in OP. *Computer Science and Engineering*, *11*(1), 1-8.

[22] Harney, J., & Ellis, C. (2022). Future directions for ethical data governance in digital health: A critical review. International Journal of Medical Informatics, 158, 104631. https://doi.org/10.1016/j.ijmedinf.2021.104631.

[23] O'Leary, S., & Kearns, G. (2019). Navigating the ethical landscape of health data management: Prospects and challenges. Journal of Health Ethics, 15(1), 45-60. https://doi.org/10.18785/jhe.1501.5.

[24] McGowan, M. L., & Haga, S. B. (2020). The future of genetic data management: Ethical considerations and policy recommendations. Genetics in Medicine, 22(4), 678-685. https://doi.org/10.1038/s41436-019-0677-y.

[25] Wahab, N. A. B. A., & Nor, R. B. M. (2023). Challenges and Strategies in Data Management and Governance for AI-Based Healthcare Models: Balancing Innovation and Ethical Responsibilities. AI, IoT and the Fourth Industrial Revolution Review, 13(12), 24-32.

[26] North M. On nlm.nih.gov "Greek Medicine - The Hippocratic Oath" U.S. National Library of Medicine, 02 July 2012. 2012. http://www.nlm.nih.gov/hmd/greek/greek_oath.html. Accessed 19 June 2017.

[27] Wilton, R. (2017). Trust and ethical data handling in the healthcare context. Health and Technology, 7(4), 569-578.

[28] Reeves, M. G., & Bowen, R. (2013). Developing a data governance model in health care: although the term may be unfamiliar, data governance is a longstanding obligation of the healthcare industry. *Healthcare Financial Management*, *67*(2), 82-87.

[29] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public law*, *104*, 191.

[30] Murray, B. (2012). Informed consent: what must a physician disclose to a patient?. *AMA Journal of Ethics*, *14*(7), 563-566.

[31] Kumar, A. (2024). AI-Driven Innovations in Modern Cloud Computing. *arXiv preprint arXiv:2410.15960*.