MineHealth: Enhancing Ethical Concerns in Health Informatics with Interoperability

Archana Jayaraman
Department of Computer Science
Lakehead University
ajayaram@lakeheadu.ca
1193610

***Abstract*—In today's ever-changing healthcare industry, ensuring accurate data, effective governance, and transparent practices are absolutely crucial. The study puts forth strategic recommendations aimed at enhancing data accuracy by implementing automated data validation processes and standardized data entry techniques using MineHealth. MineHealth is a project that focuses on enhancing data accuracy, transparency, and interoperability in healthcare analytics. With a strong emphasis on data mining techniques, the project integrates diverse healthcare data sources, including Electronic Health Record (EHR) systems, clinical systems, and external data sources. By implementing standardized data entry protocols, data validation and cleansing mechanisms, and data profiling techniques, MineHealth ensures the reliability and integrity of the collected data. Leveraging an interoperability framework based on industry standards and protocols, the project facilitates seamless data exchange and collaboration between healthcare entities, enabling comprehensive analytics and informed decision-making. Privacy and security measures, including access control, data encryption, and privacy management, are implemented to safeguard patient information. MineHealth aims to revolutionize healthcare analytics, promoting data-driven insights, improved patient outcomes, and advancements in precision medicine.**

***Index Terms*—MineHealth, Electronic Health Records (EHR), Data accuracy, Data Governance, Data transparency, Standardized data entry, Interoperability, Access control, Patient data integrity, Healthcare outcomes, Data Quality, Data validation rules.**

I. Introduction

The healthcare industry is a significant and complicated one that focuses on the health and treatment of humans, providing a range of services like diagnosis, treatment, prevention, and control of sickness. Information on patient's demographics, medical histories, test results, imaging data, prescription histories, and other details are all included in health data. Due to technological advancements and the increasing use of electronic health records (EHRs), healthcare organizations have recently experienced a large surge of data. This plethora of data has the potential to transform medical research, patient outcomes, and healthcare delivery when properly tapped and analyzed. However, managing healthcare data involves important problems and ethical obligations that need to be carefully handled [1]. In recent reports, the WHO has highlighted the critical importance of accurate data in healthcare decision-making and patient outcomes. The organization estimates that up to 1 in 10 medical diagnoses worldwide may be incorrect, leading to suboptimal treatments and potential harm to patients. Inaccurate data, including lab reports and blood group information, can significantly impact clinical decision-making, jeopardizing patient safety and effective healthcare delivery. While beneficial, health informatics poses ethical challenges requiring responsible use of health data [2]. This report delves into the realm of healthcare data, exploring its importance, challenges, and ethical considerations. MineHealth aims to shed light on the critical role data handling plays in the healthcare industry, and how proper management and utilization of data can have profound implications for patient care, research advancements, and overall healthcare outcomes.

Health informatics is an interdisciplinary field that combines healthcare, information technology, and data management to improve the delivery of healthcare services. It encompasses the acquisition, storage, retrieval, and use of health information to support clinical decision-making, enhance patient care, and advance medical research. With the widespread adoption of EHRs, telemedicine, mobile health applications, and other technological advancements, health informatics has become an integral part of modern healthcare systems [3].

In the field of health informatics, various types of data play a critical role in supporting decision-making, optimizing healthcare processes, and improving patient outcomes. Three key types of data that are prominent in health informatics are Organizational data, managerial data, and diagnostic data. This report provides an overview of each of these data types and their significance within the context of health informatics [4], [5].

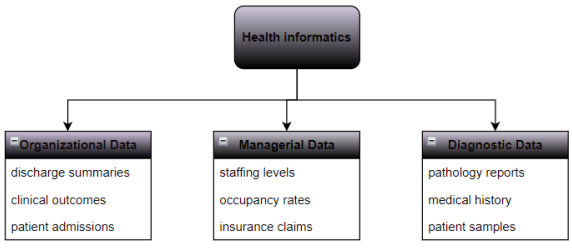

Fig. 1. Classification of Health care records

Figure-1 represents the classification of data in the healthcare system. Organizational data in health informatics: Data

generated during routine operations in healthcare organizations, providing insights into processes and resource management. Managerial data in healthcare: Information used for administrative and managerial purposes, enabling financial management, workforce tracking, and performance measurement. Diagnostic data in health informatics: Information derived from diagnostic tests and medical imaging, supporting accurate diagnoses, treatment planning, and patient monitoring [6], [7].

Understanding the significance of Organizational, managerial, and diagnostic data in health informatics is essential for healthcare organizations and professionals to leverage the full potential of information technology in advancing healthcare practices and improving patient care. The MineHealth project recognizes the criticality of data accuracy, governance, and transparency in healthcare analytics. By integrating diverse healthcare data sources and implementing standardized data entry protocols, MineHealth aims to ensure the reliability and integrity of collected data. The project emphasizes ethical considerations, including patient privacy, data security, and responsible data use, aligning with the broader ethical concerns in health informatics. Through its ethical and data-driven approach, MineHealth contributes to fostering an ethical culture and responsible use of health informatics technologies, ultimately improving patient outcomes and advancing healthcare practices.

II. Steps Towards the Advancements In Handling Health Records

1. **Paper-based Records:** Historically, health records were primarily paper-based. Patient information, including medical history, diagnoses, and treatment details, was recorded and stored in physical files. This method was labor-intensive and prone to errors, as well as limited in terms of accessibility and data sharing.
2. **Electronic Health Records (EHRs):** With the advent of computers and electronic systems, the transition to electronic health records began. EHRs are digital versions of patient records that contain comprehensive health information, including medical history, test results, medications, and more. EHRs improved accessibility, legibility, and data sharing among healthcare providers within a single institution [8].
3. **Health Information Exchange (HIE):** To enhance data sharing and interoperability between different healthcare organizations, Health Information Exchange systems emerged. HIE enables the secure exchange of patient information across disparate EHR systems, facilitating coordinated care, reducing duplication of tests, and improving patient outcomes [9].
4. **Personal Health Records (PHRs):** PHRs put the patients in control of their health information. These records are managed and maintained by individuals and typically include personal health information, self-reported data, and medical history. PHRs can be either paper-based or electronic and allow patients to have more involvement in their healthcare decisions.
5. **Digital Health Technologies:** The evolution of health informatics has seen a proliferation of digital health technologies, including wearables, mobile health applications, and remote monitoring devices. These technologies generate vast amounts of health data, often referred to as "big data," which can be used for advanced analytics, population health management, and personalized medicine.
6. **Health Information Systems (HIS):** Modern health information systems have emerged to integrate various aspects of healthcare data management. HIS encompasses EHRs, clinical decision support systems, data analytics platforms, and other components. They aim to streamline data capture, storage, analysis, and retrieval while ensuring privacy and security [10].

III. Ethics in Health Infomatics

In the realm of healthcare records, the requirement for ethics is of paramount importance. Ethics serve as the guiding principles and moral compass for handling and managing patient information. With the increasing reliance on electronic health records (EHRs) and digital systems, it becomes crucial to ensure the ethical handling of sensitive healthcare data. Listed below are some of the ethical issues that are listed below.

A. Organizational Data

Organizational data in health informatics includes essential information from daily healthcare operations, such as patient admissions, medication orders, tests, billing, and scheduling. Analyzing this data provides insights into operational efficiency and resource utilization, allowing healthcare organizations to streamline processes and improve service delivery. The 2019 AMCA data breach highlighted the importance of greater security measures when outsourcing data management services, emphasizing the need for due diligence and compliance with privacy standards [11]. Overall, organizational data plays a crucial role in the administration, finance, human resources, quality management, compliance, and strategic decision-making in healthcare organizations.

To ensure ethical practices surrounding organizational data, healthcare organizations should adhere to the following principles:

- **Confidentiality** Respect the confidentiality of organizational data by implementing appropriate security measures and restricting access to authorized personnel. It is crucial to prevent unauthorized disclosure or use of sensitive information.
- **Privacy** By adhering to legal and regulatory regulations such as the Health Insurance Portability and Accountability Act (HIPAA), you can protect patient privacy. When collecting and using data, get informed consent, and use de-identification and anonymization techniques when sharing data for research or other uses. Obtain informed consent for data collection and use, and employ

techniques like de-identification and anonymization when sharing data for research or other purposes.

- **Data Security** Implement better data security measures, including encryption, access controls, and regular security audits. These measures protect organizational data from unauthorized access, breaches, or cyber threats. It is essential to ensure secure storage and transmission of data within the organization and when sharing it externally.

By upholding these ethical principles, healthcare organizations can maintain the integrity, confidentiality, and privacy of organizational data, fostering trust and responsible data management practices.

B. Managerial Data

Managerial data in healthcare encompasses financial, human resources, performance metrics, strategic planning, compliance, and operational information used for administrative purposes. A significant incident occurred in 2020 when Universal Health Services (UHS), a prominent healthcare provider, suffered a ransomware attack, temporarily compromising access to critical managerial data and operational systems. This incident highlighted the vulnerabilities healthcare organizations face and emphasized the importance of cybersecurity measures, proactive risk management, and comprehensive incident response plans [12]. It underscored the criticality of protecting managerial data to preserve its confidentiality, integrity, and availability within healthcare organizations.

When it comes to data management, it is crucial to uphold ethical principles and practices. Here are key ethics to follow:

- **Integrity** Maintain the reliability and integrity of managerial data by implementing processes for data validation, quality assurance, and regular audits. This ensures that decision-making is based on accurate and trustworthy information.
- **Informed Consent** Obtain informed consent from individuals before collecting and using their data for managerial purposes. Provide clear information about the purpose, potential risks, and benefits of data processing, allowing individuals to make informed choices regarding their data.
- **Continuous Monitoring and Improvement** Regularly monitor and evaluate the effectiveness of data management practices and ethical guidelines. Conduct thorough reviews of policies and procedures, establish feedback mechanisms, and learn from experiences to continuously improve managerial data ethics.

By adhering to these ethical principles, healthcare organizations can maintain the integrity of their managerial data, respect individuals' rights and privacy, and strive for continuous improvement in data management practices.

C. Diagnostic Data

Diagnostic data in healthcare refers to the information collected during the process of diagnosing medical conditions. It includes medical history, symptoms, examination findings, test results, imaging studies, and procedures. This data guides accurate diagnoses, treatment planning, and patient monitoring. In a 2017 incident at a Veterans Affairs Medical Center, a manual data entry error resulted in incorrect diagnostic test results for 88 patients, emphasizing the importance of accurate data entry and the need for standardized processes and technology solutions to ensure data integrity in diagnostics [13].

When dealing with diagnostic data, it is crucial to adhere to ethical principles. Here are the key ethics to follow:

- **Data Accuracy and Quality** Maintain the accuracy, integrity, and quality of diagnostic data. Implement high-level processes for data collection, verification, and validation to minimize errors and inaccuracies that could impact clinical decision-making.
- **Transparency and governance** Promote transparency in the use of diagnostic data by clearly communicating how the data will be utilized, shared, and protected. Establish mechanisms for individuals to access their diagnostic data and provide them with an understanding of how it is used. Ensure accountability for the proper handling and use of diagnostic data.

By upholding these ethical principles, healthcare professionals can ensure the reliability of diagnostic data, foster transparency in data usage, and maintain individuals' trust in the handling of their sensitive medical information.

IV. Literature Survey

The significance of confidentiality in healthcare applications and the demand for security methods to safeguard sensitive healthcare data are both covered in the study by Rizwan, Muhammad, et al. It suggests a tiered approach using the Modular Encryption Standard (MES) and condition-centric risk monitoring to protect the confidentiality of healthcare data [14]. The usage of a machine learning technique, specifically a Fuzzy Inference System coupled with Neural Networks, to support decision-making in the risk monitoring strategy of MES is also mentioned in the article. The findings imply that MES achieves low error rates and high precision rates, demonstrating its efficacy in boosting security precautions.

In a study by Tang et al. [15], a privacy-preserving healthcare system was proposed to enhance trust between patients and caregivers within a trusted network. The Sybil attack was employed to identify and remove fake patients from the network, ensuring that only authenticated individuals can access the healthcare center.

Salnitri et al. [16] implemented a computer-aided design for the security and privacy of trusted systems. Their approach also provided specifications for experts to utilize the system based on various characteristics. They emphasized the importance of setting higher goals for the business and maintaining vigilance against external threats to uphold network trustworthiness.

The topic of the study by Haibing Liu et al. is the use of distributed ledger and blockchain technology to improve privacy and data security in healthcare applications. It intends to create an Improved Biomedical Security system (BDL-IBS)

based on Blockchain and Distributed Ledgers to support secure information sharing and consent mechanisms amongst various healthcare organizations and applications [17].

The paper by Mohammad Zarour, et. al highlights the risks associated with incorrect or improperly changed data and the challenges it poses in managing healthcare information. The study aims to provide insights into the threat landscape of data integrity globally and in Saudi Arabia. The study suggests that blockchain technology is prioritized for ensuring data integrity in Saudi Arabia. Overall, the research aims to address masked authenticated messaging approaches to improve integrity in healthcare [18].

Deborah S. Loeff, et. al discuss the importance of informed consent and shared decision-making in pediatric surgery and highlights the need for further exploration of the topic. It mentions that the terms ”informed consent” and ”shared decision-making” are used interchangeably and emphasize the unique aspects of informed consent in the medical care of children [19].

Ibrar Yaqoob1, et. al highlights the potential benefits of leveraging blockchain technology in healthcare data management systems [20]. It mentions key features such as immutability, auditability, data provenance, flexible access, trust, privacy, and security that blockchain offers. The abstract also points out that centralized healthcare systems have potential risks of a single point of failure.

Taryn Vian focuses on corruption, transparency, and accountability in healthcare systems. This paper also identifies frameworks and approaches to understand and address corruption, highlighting the role of transparency using PubMed [21]. Overall, addressing transparency is crucial for strengthening health systems and achieving Universal Health Coverage (UHC) in line with sustainable development goals.

Also, Governments have a responsibility to ensure transparency in healthcare delivery processes by clearly defining the rules and disclosing the outcomes. Additionally, they should disclose any secondary interests that might influence the decisions made by healthcare providers and policymakers [22], [23].

V. Proposed System

Digital records of the patients are very very important when an emergency situation occurs. Digitilizing the health records will do a lot of favors for the doctors because they do not need to wait for all the patient records to arrive in the file instead a single touch makes all the records appear in front of them, MineHealth is an innovative project that enhances data accuracy, governance, and transparency in healthcare analytics. By integrating diverse healthcare data sources and implementing standardized data entry protocols, MineHealth ensures reliable and consistent data. The project prioritizes patient privacy, data security, and responsible management, adhering to industry standards. Through advanced data mining techniques, MineHealth enables comprehensive analytics and evidence-based decision support. The project aims to revolutionize healthcare practices, improve patient outcomes, and drive advancements.

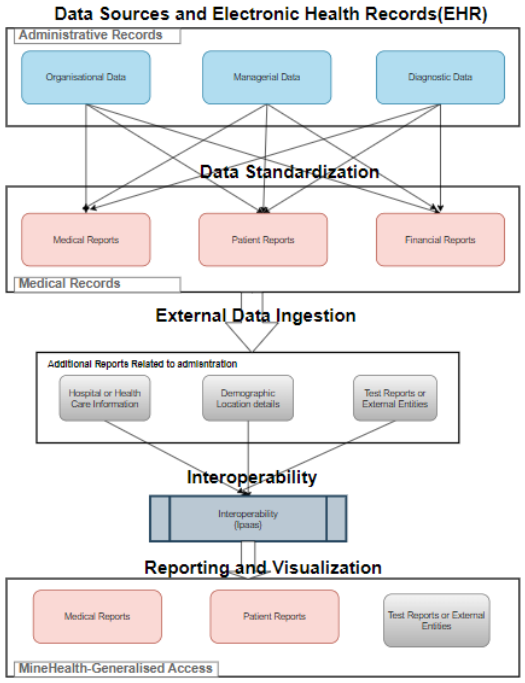

Fig. 2. Design of MineHealth

Figure-2 is the architecture for MineHealth that supports standardized data entry, interoperability, data accuracy, and transparency in healthcare records can be designed as follows:

A. Data Sources and Systems:

The Data sources are integrated with various healthcare systems and can be achieved through standardized interfaces, APIs, and data exchange protocols. This involves collaboration with EHR vendors, clinical system providers, and external data source providers to establish secure and reliable connections.

- Electronic Health Record (EHR) Systems: Integration with EHR systems to extract relevant patient data, including demographics, medical history, lab results, and treatment information.
- Clinical Systems: Integration with various clinical systems such as laboratory information systems, radiology systems, and pharmacy systems to capture specialized data.
- External Data Sources: Integration with external data sources, such as research databases, public health databases, and wearable devices, to enrich the dataset.

B. Data Ingestion and Standardization:

A data ingestion layer can be developed using data integration tools and techniques. This layer should support secure data transmission, data transformation, and data cleansing processes. Standardization can be achieved

through the use of data normalization techniques and the development of mapping rules to transform data into a common format.

- Data Ingestion Layer: Responsible for acquiring data from different sources securely and efficiently.
- Data Standardization: Implementing a data standardization process to transform data into a common format and structure, ensuring consistency across different data sources. The effective data management and integration of these diverse data sources are crucial when it comes to health informatics because it improves the healthcare sector with full potential and leverages the management of data and population of health management.

C. Interoperability Framework:

Adhering to industry standards, such as HL7, FHIR, and DICOM, requires the development or adoption of software modules that support these standards [24]. The use of APIs and middleware can facilitate seamless communication and data exchange between systems. Integration with existing healthcare systems may require custom development or the use of interoperability platforms. Can be developed as tool that can be used is an Integration Platform as a Service (iPaaS), which is a cloud-based integration solution. iPaaS platforms offer pre-built connectors and APIs that facilitate the integration of different systems and data sources, enabling seamless interoperability.

- Standards and Protocols: Adhering to industry standards and protocols, such as HL7, FHIR, and DICOM, to enable seamless interoperability between different healthcare systems and data sources [25], [26].
- APIs and Middleware: Implementing APIs and middleware to facilitate secure and standardized communication and data exchange between systems.
- Data Quality Assurance: Data Validation and Cleansing: Employing data validation rules and techniques to ensure data accuracy, completeness, and consistency. The below Figure-3 shows the explanation of each and every protocol used in the framework

Protocol_Standards	Description
HL7	HL7 (Health Level 7) is a set of international standards for the exchange, integration, sharing, and retrieval of electronic health information, enabling interoperability between different healthcare systems and facilitating the seamless flow of data in healthcare environments.
HITECH	HITECH (Health Information Technology for Economic and Clinical Health) is a U.S. federal law that promotes the adoption and meaningful use of electronic health records (EHRs) to improve healthcare quality, efficiency, and patient privacy
HIPAA	HIPAA (Health Insurance Portability and Accountability Act) is a U.S. federal law that safeguards the privacy and security of individuals' protected health information (PHI) and sets standards for the electronic exchange of healthcare data.

Fig. 3. Protocol Standards Used in Interoperability

D. Data Quality Assurance:

Data validation and cleansing can be implemented through the development of validation rules and algorithms. These rules can be applied during data ingestion or as part of data processing pipelines. Data profiling can be achieved through the use of data profiling tools and techniques that analyze data characteristics, structure, and patterns [27]. Data governance policies and procedures can be established in collaboration with stakeholders to ensure compliance with data quality standards and regulatory requirements.

- Data Validation and Cleansing: Employing data validation rules and techniques to ensure data accuracy, completeness, and consistency.
- Data Profiling: Analyzing the characteristics, structure, and patterns of the data to identify potential data quality issues.
- Data Governance: Implementing data governance policies and procedures to maintain data integrity, security, and privacy.

E. Analytics and Decision Support:

Data mining and analytics can be implemented using a combination of software tools, machine learning algorithms, and statistical techniques. These tools can be integrated into the data processing pipelines to extract insights, patterns, and predictive models from the standardized data. Reporting and visualization can be achieved through the development of interactive dashboards and visualization platforms that provide users with intuitive and actionable insights.

- Data Mining and Analytics: Utilizing advanced data mining techniques, such as machine learning and predictive analytics, to extract insights and patterns from standardized data.
- Reporting and Visualization: Presenting analytics results through interactive dashboards and visualizations to enable easy interpretation and decision-making.

F. Security and Privacy:

Access control mechanisms can be implemented through user authentication and authorization systems that enforce role-based access to data. Data encryption can be achieved using encryption algorithms and secure communication protocols to protect data at rest and in transit [28]. Privacy and consent management modules can be developed to provide patients with control over their data and ensure compliance with privacy regulations.

- Access Control: Implementing role-based access control mechanisms to ensure that only authorized personnel can access and manipulate the data.
- Data Encryption: Employing encryption techniques to protect sensitive data both at rest and in transit.
- Privacy and Consent Management: Incorporating privacy and consent management modules to ensure compliance

with regulations and enable patients to control the use of their data.

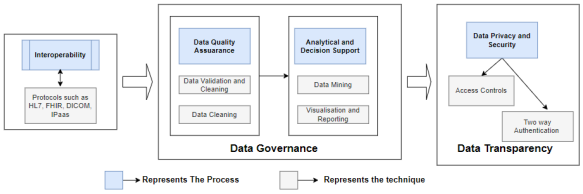

Fig. 4. Flow of Interoperability to Achieve Data Governance and Transparency

Figure-4 describes the working flow of how data governance and transparency are achieved by Interoperability.

VI. Benefits of Standardized Data Entry & Interoperability

MineHealth offers a range of benefits in the healthcare industry. It improves data accuracy through standardized data entry and validation processes, ensuring reliable and error-free healthcare records. The project promotes ethical data governance and transparency, prioritizing privacy protection and consent management. MineHealth enables seamless interoperability, facilitating efficient communication and data exchange between healthcare systems. It empowers advanced analytics and decision support, extracting valuable insights from healthcare data for evidence-based decision-making. By improving patient care coordination, MineHealth enhances the continuity and quality of care across providers and settings. The project supports research and innovation by integrating with external data sources, contributing to medical advancements. Additionally, MineHealth drives cost efficiency and resource optimization by reducing errors and inefficiencies in data management. Overall, MineHealth ensures ethical data practices, prioritizes patient privacy, and upholds data security in the healthcare ecosystem.

VII. Comparison and Evaluation of MineHealth with another system

In comparison to the existing approach, the existing approach proposes the use of a blockchain and cloud computing network, MineHealth focuses on enhancing data accuracy, transparency, and interoperability by implementing standardized data entry protocols, data validation and cleansing mechanisms, and data profiling techniques [29]–[31]. MineHealth emphasizes the integration of diverse healthcare data sources, such as Electronic Health Record systems and clinical systems, to ensure reliable and accurate data. Furthermore, MineHealth prioritizes data privacy and security through the implementation of access control, data encryption, and privacy management measures. With a strong emphasis on data mining techniques, MineHealth enables comprehensive analytics and informed decision-making in healthcare.

Ref_Year	Existing_Papers_refered	Issues_Addressed	MineHealth_Addressing_Issues
2019	Blockchain-Based Interoperable Electronic Health Record Sharing Framework	Data Security, Interoperability	Data Accuracy and Interoperability
2019	BinDaaS: Blockchain-based deep learning as a Service in Healthcare 4.0 applications.	Privacy, data ownership, collusion attacks, scalability of mined transactions, cost and storage issues	Transparency
2012	Achieving Interoperability among Healthcare Standards	Interoperability, Semantic Interchangeability	Governance and Interoperability

Fig. 5. Some Existing Interoperability Framework with their Issues

In Figure-5 the existing papers referenced focused on issues such as data security, privacy, interoperability, and semantic interchangeability in healthcare. In comparison, MineHealth addresses the specific challenges of data accuracy and interoperability. It emphasizes standardized data entry, validation mechanisms, and an interoperability framework to ensure reliable and seamless data exchange. Additionally, MineHealth emphasizes transparency, governance, and proper data management to maintain integrity, security, and privacy in healthcare analytics.

VIII. Open Challenges on the Ethics of Data

Extracting Relevant Information: One open challenge in dealing with unstructured clinical notes is extracting relevant and meaningful information from the text. Clinical notes often contain lengthy narratives, abbreviations, and medical jargon, making it difficult to identify and extract key data elements. Developing natural language processing (NLP) algorithms that can accurately extract and structure relevant information from unstructured clinical notes is an ongoing challenge.

Ensuring Data Privacy and Security: Unstructured clinical notes may contain sensitive patient information, including personal identifiers, medical history, and diagnostic details. Ensuring data privacy and security while processing and analyzing these unstructured notes poses a significant challenge. Safeguarding patient privacy, anonymizing data, and implementing secure data storage and transmission protocols are essential to maintain data confidentiality and comply with privacy regulations.

IX. Future works

The creation of an automated monitoring system based on health information is one potential future task for MineHealth. This system would analyze patient data to find patterns and send out automated reminders for forthcoming exams and checkups using cutting-edge algorithms and machine learning. By empowering people to actively participate in their healthcare, the system would increase patient compliance, optimize resource allocation, enable proactive healthcare management, and enable. The implementation of this system would entail integrating communication, data analytics, and machine learning capabilities into the MineHealth framework while assuring privacy compliance and encouraging stakeholder cooperation.

X. Conclusion

In conclusion, MineHealth presents a transformative solution for healthcare data management, governance, and interoperability. By implementing standardized data entry, robust data validation, and an interoperability framework, MineHealth ensures data accuracy, transparency, and seamless exchange across healthcare systems. The project addresses critical challenges in healthcare informatics, such as unstructured clinical notes and data integration, while prioritizing patient privacy and data security. Through advanced analytics and decision support, MineHealth empowers healthcare organizations to make data-driven decisions, improve patient outcomes, and advance precision medicine. As a future work, integrating advanced technologies like blockchain and automating monitoring systems further enhances the capabilities of MineHealth. By leveraging these advancements, MineHealth has the potential to revolutionize healthcare practices, foster collaboration, and shape the future of data-driven healthcare which provides benefits both patients and the whole of the healthcare industry. It is essential to maximize the benefits of health informatics while ensuring patient rights, improving healthcare outcomes, and maintaining public trust in the healthcare system.

References

[1] Bath, Peter A. "Health informatics: current issues and challenges." Journal of information science 34.4 (2008): 501-518.

[2] Patrick Kierkegaard. 2012. Medical data breaches: Notification delayed is notification denied. Computer Law & Security Review 28, 2 (2012), 163–183.

[3] Bates, David W., et al. "A proposal for electronic medical records in US primary care." Journal of the American Medical Informatics Association 10.1 (2003): 1-10.

[4] Loomis, Glenn A., et al. "If electronic medical records are so great, why aren't family physicians using them?." Journal of Family Practice 51.7 (2002): 636-641.

[5] Norris A C, Brittain J M. Education, training and the development of health informatics. Health Informatics Journal 2000; 6(4): 189-95

[6] Peute, Linda W., et al. "Challenges and best practices in ethical review of human and organizational factors studies in health technology: a synthesis of testimonies." Yearbook of medical informatics 29.01 (2020): 058-070.

[7] El-Kareh, Robert, Omar Hasan, and Gordon D. Schiff. "Use of health information technology to reduce diagnostic errors." BMJ quality & safety 22.Suppl 2 (2013): ii40-ii51.

[8] Kim, Ellen, et al. "The evolving use of electronic health records (EHR) for research." Seminars in radiation oncology. Vol. 29. No. 4. WB Saunders, 2019.

[9] Cowie MR, Blomster JI, Curtis LH, et al: Electronic health records to facilitate clinical research. Clin Res Cardiol 106:1-9, 2017. https://doi.org/10.1007/s00392-016-1025-6

[10] Dagliati, Arianna, et al. "Health informatics and EHR to support clinical research in the COVID-19 pandemic: an overview." Briefings in Bioinformatics 22.2 (2021): 812-822.

[11] Ugwu, Augustina O., et al. "Ethical Implications of AI in Healthcare Data: A Case Study Using Healthcare Data Breaches from the US Department of Health and Human Services Breach Portal between 2009-2021." 2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC). IEEE, 2022.

[12] López Cabello, Andrés. "Pandemic momentum for health systems financialization: Under the cloaks of Universal Health Coverage." Global Public Health 16.8-9 (2021): 1334-1345.

[13] Klap, Ruth, et al. "Prevalence of stranger harassment of women veterans at Veterans Affairs medical centers and impacts on delayed and missed care." Women's Health Issues 29.2 (2019): 107-115.

[14] Rizwan, Muhammad, et al. "Risk monitoring strategy for the confidentiality of healthcare information." Computers and Electrical Engineering 100 (2022): 107833.

[15] Tang, W.; Ren, J.; Zhang, Y. Enabling trusted and privacy-preserving healthcare services in social media health networks. IEEE Trans. Multimed. 2019, 21, 579–590.

[16] Salnitri, M.; Angelopoulos, K.; Pavlidis, M.; Diamantopoulou, V.; Mouratidis, H.; Giorgini, P. Modelling the interplay of security, privacy and trust in sociotechnical systems: A computer-aided design approach. Softw. Syst. Model. 2019, 19, 467–491.

[17] Liu, Haibing, Rubén González Crespo, and Oscar Sanjuán Martínez. "Enhancing privacy and data security across healthcare applications using blockchain and distributed ledger concepts." Healthcare. Vol. 8. No. 3. MDPI, 2020.

[18] Zarour, Mohammad, et al. "Ensuring data integrity of healthcare information in the era of digital health." Healthcare Technology Letters 8.3 (2021): 66-77.

[19] Loeff, Deborah S., and Baddr A. Shakhsheer. "The ethics of informed consent and shared decision-making in pediatric surgery." Seminars in pediatric surgery. Vol. 30. No. 5. WB Saunders, 2021.

[20] Yaqoob, Ibrar, et al. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." Neural Computing and Applications (2021): 1-16.

[21] Vian, Taryn. "Anti-corruption, transparency and accountability in health: concepts, frameworks, and approaches." Global health action 13.sup1 (2020): 1694744.

[22] Vian T. Exploring the construction of transparency: an analysis of health managers' narratives. Global Health Governance. 2012;V:1–24.

[23] Paschke A, Dimancesco D, Vian T, et al. Increasing transparency and accountability in national pharmaceutical systems. Bull World Health Organ. 2018;96:782–791.

[24] Iroju, Olaronke, et al. "Interoperability in healthcare: benefits, challenges and resolutions." International Journal of Innovation and Applied Studies 3.1 (2013): 262-270.

[25] Cardoso, Luciana, et al. "Interoperability in healthcare." Health Care Delivery and Clinical Science: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018. 689-714.

[26] Bender, Duane, and Kamran Sartipi. "HL7 FHIR: An Agile and RESTful approach to healthcare information exchange." Proceedings of the 26th IEEE international symposium on computer-based medical systems. IEEE, 2013.

[27] Berndt, Donald J., et al. "Healthcare data warehousing and quality assurance." Computer 34.12 (2001): 56-65.

[28] Shrestha, N. M., et al. "Enhanced e-health framework for security and privacy in healthcare system." 2016 Sixth international conference on digital information processing and communications (ICDIPC). IEEE, 2016.

[29] Carter, Gracie, Hossain Shahriar, and Sweta Sneha. "Blockchain-based interoperable electronic health record sharing framework." 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC). Vol. 2. IEEE, 2019.

[30] Bhattacharya, Pronaya, et al. "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications." IEEE Transactions on network science and engineering 8.2 (2019): 1242-1255.

[31] Khan, Wajahat Ali, et al. "Achieving interoperability among healthcare standards: building semantic mappings at models level." Proceedings of the 6th International Conference on Ubiquitous Information Management and Communication. 2012.