International Journal of Multidisciplinary Research and Growth Evaluation.

Leveraging advanced information systems for enhanced data management and security in healthcare

Lekan Afolabi
Department of Information Systems and Business Analytics, Auburn University, Auburn, Alabama, 36830, USA
Department of Business, Auburn University, Auburn, Alabama, 36830, USA

* Corresponding Author: **Lekan Afolabi**

Article Info

ISSN (online): 2582-7138
Volume: 05
Issue: 02
March-April 2024
Received: 10-03-2024
Accepted: 13-04-2024
Page No: 980-985

Abstract
Amidst the digital revolution, the healthcare industry has enormous hurdles in protecting and managing enormous volumes of sensitive patient data. Utilizing cutting-edge information systems presents a viable solution for successfully addressing these issues. To improve data management and security inside healthcare organizations, this article examines the role of advanced information systems, such as electronic health records (EHR), health information exchanges (HIE), and data analytics platforms. This study looks at the advantages, difficulties, and best practices of implementing advanced information systems in healthcare settings through a thorough analysis of the literature and case studies. Additionally, it investigates how cutting- edge technologies like blockchain, and artificial intelligence (AI) can transform healthcare data management and security procedures.

Keywords: Information system, healthcare, sensitive and personal information, data protection and security

Introduction

The healthcare sector has experienced a dramatic digital transformation in recent years, with the use of cutting-edge information technologies being essential in changing the way patient data is safeguarded and maintained. The rapid expansion of data analytics platforms, health information exchanges (HIEs), and electronic health records (EHRs) has transformed the way healthcare is delivered by facilitating effective information sharing, strengthening clinical decision-making, and ultimately improving patient outcomes. Alongside these developments, though, the healthcare industry now faces never-before-seen difficulties in maintaining regulatory compliance and protecting confidential patient data from emerging cyber threats.

It is impossible to overestimate how important it is for healthcare to use cutting-edge information technologies. Conventional paper-based record-keeping systems are unreliable, laborious, and unable to adapt to the changing needs of the healthcare industry. Healthcare professionals may decrease medical mistakes, expedite administrative procedures, and promote smooth communication across multidisciplinary care teams by implementing digital technology.

Furthermore, by facilitating collaborative decision-making and granting patients access to their medical records, sophisticated information systems enable patients to take an active role in their treatment.

Even with these developments, healthcare organizations may suffer greatly from antiquated and ineffective information systems. Significant dangers to patient privacy and confidentiality are posed by data breaches and security events, which also undermine the integrity of the healthcare system overall and erode public confidence in healthcare institutions. Furthermore, ineffective data management techniques may lead to redundant services, fragmented treatment, and impaired patient safety. Healthcare organizations' capacity to provide high-quality, cost-effective treatment is hampered by their failure to fully utilize information technology in an era where data-driven insights drive clinical and operational decision-making.

Healthcare firms must abide by a plethora of laws and guidelines aimed at protecting patient data and guaranteeing information security to lessen these dangers and difficulties. Strict guidelines protecting the confidentiality, integrity, and accessibility of patient information are imposed on healthcare providers, payers, and business associates by laws like the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Serious fines, harm to one's reputation, and legal repercussions may arise from breaking these rules.

With these things in mind, the purpose of this article is to investigate how modern information systems might help healthcare organizations meet the dual demands of security and data management. This study looks at the advantages, difficulties, and best practices related to implementing advanced information systems to give healthcare stakeholders useful information for navigating the complicated world of healthcare IT. Additionally, this study aims to identify creative ways to improve data management and security practices in healthcare by highlighting cutting-edge technologies like blockchain and artificial intelligence. This will ultimately advance the goal of providing safe, effective, and patient-centered care in the digital age.

Methodology

This study aims to conduct a comprehensive literature review to analyze the design and impacts of leveraging advanced information systems on data management and security in the healthcare sector. This will be achieved through a systematic review of peer-reviewed literature, synthesizing findings to understand how different advanced information systems have been adapted and their effectiveness in this sector. The methodology for this literature review follows the three-stage process outlined by (Tranfield *et al*., 2003) [30], which consists of planning the review, conducting the review, and reporting and disseminating. This structured approach ensures transparency and repeatability and minimizes research bias.

Planning the review

The review will focus on literature published since 2000 to ensure contemporary relevance and applicability. Databases such as Google Scholar, Journal of Biomedical Informatics, Journal of Global Information Management, and others will be utilized to gather relevant research papers. The criteria for inclusion will be based on the depth and applicability of advanced information systems for improvement with a focus on identifying benefits, challenges, and outcomes. A search strategy will be developed involving key terms related to advanced information systems and data security, combined with terms specific to healthcare data management.

Conducting the review

The terms ‘Advanced Information Systems’ ‘Healthcare data management’ and ‘Healthcare data security’ were used to search for articles. The initial screening will be based on titles and abstracts, focusing on papers that specifically address advanced information systems applications for the improvement of data management and business. Papers not directly related to these methodologies or outside the scope of this review will be excluded. Relevant papers will undergo a detailed examination, including full-text review, to evaluate methodologies, findings, and relevance. Data extraction will include the author(s), publication year, study focus, tools and techniques used, and key findings.

Reporting and Disseminating

The integrated knowledge extracted from the examined literature will be combined into an extensive report. This research, which offers insights into the advantages, difficulties, and results connected with the application of cutting-edge information systems, will be an invaluable resource for stakeholders in the field of healthcare data management. The results will be disseminated through a variety of venues, such as scholarly journals, conferences, and focused talks, to guarantee broad accessibility and relevance in the field of healthcare IT.

A Critical review of traditional information systems

In the rapidly evolving landscape of healthcare, the importance of efficient data management and robust security measures cannot be overstated [1]. However, traditional information systems, once considered standard practice, often fall short of meeting the complex demands of modern healthcare delivery. These systems, characterized by fragmented data storage, limited accessibility, data entry errors, security vulnerabilities, and compliance challenges, pose significant risks to patient safety, privacy, and the integrity of healthcare operations [2]. In this essay, we will explore the weaknesses of traditional information systems in healthcare, highlighting their impact on data management and security, as well as the implications for patient care and organizational efficiency.

Traditional information systems in healthcare are often characterized by fragmented data storage methods, including paper-based records, standalone databases, and disparate systems for different departments or functions. This fragmentation creates data silos, hindering the efficient exchange and sharing of patient information among healthcare providers. As a result, healthcare providers may struggle to obtain a comprehensive view of patients' medical histories, leading to gaps in care and potential medical errors. For example, a patient's medical history stored in paper records at one healthcare facility may not be accessible to providers at another facility, compromising care coordination and continuity.

The reliance on paper-based records and legacy systems in traditional information systems may restrict access to patient information, particularly in remote or decentralized healthcare settings. Healthcare providers may encounter difficulties retrieving patient records on time, hindering care coordination and continuity. Moreover, limited accessibility can impede the adoption of telemedicine and remote monitoring solutions, which rely on real-time access to patient data for remote consultations and interventions. In rural or underserved areas where access to healthcare facilities is limited, the lack of accessible patient information can exacerbate disparities in care and outcomes.

Manual data entry processes in traditional information systems are prone to errors, including transcription mistakes, illegible handwriting, and duplication of records [3]. These errors can compromise the accuracy and integrity of patient data, leading to misdiagnosis, incorrect treatment decisions, and compromised patient safety. Additionally, manual data entry increases administrative burden and reduces efficiency, as healthcare providers spend valuable time correcting errors and reconciling discrepancies. For example, a transcription error in a patient's medication list could result in a prescription error, leading to adverse drug reactions or treatment complications.

Traditional information systems may lack robust security measures to protect sensitive patient information from unauthorized access, data breaches, and cyberattacks [4]. Paper-based records are susceptible to physical theft, loss, or damage, while legacy systems may have outdated security protocols and vulnerabilities that expose them to hacking and malware attacks. Several high-profile data breaches in the healthcare industry, such as the Anthem data breach in 2015 [5] and the Equifax breach in 2017 [6], underscore the risks

associated with inadequate data security measures. These breaches not only compromise patient privacy and confidentiality but also erode trust in healthcare organizations and the integrity of the healthcare system.

Traditional information systems may struggle to meet regulatory requirements and standards for data security and privacy, such as HIPAA and GDPR. Paper-based records lack audit trails and access controls, making it difficult to track and monitor data access and usage. Legacy systems may require costly upgrades or customizations to achieve compliance, leading to financial strain and operational disruptions for healthcare organizations [7]. Failure to comply with these regulations can result in severe penalties, reputational damage, and legal ramifications, further exacerbating the challenges faced by healthcare organizations.

In conclusion, the weaknesses of traditional information systems in healthcare have significant implications for data management, security, and the delivery of patient care. Fragmented data storage, limited accessibility, data entry errors, security vulnerabilities, and compliance challenges undermine the efficiency, effectiveness, and integrity of healthcare operations [8]. To address these weaknesses effectively, healthcare organizations must prioritize investments in modernizing their IT infrastructure, implementing robust security measures, and adopting interoperable, user-friendly information systems that support the delivery of high-quality, patient-centered care. By leveraging advanced technologies and best practices, healthcare organizations can mitigate risks, improve outcomes, and build a secure and resilient healthcare ecosystem for all [9].

Integration of advanced information systems into healthcare

The integration of advanced information systems into healthcare represents a transformative shift in the way patient data is managed and secured. Advanced information systems encompass a wide range of technologies and platforms, including electronic health records (EHRs), health information exchanges (HIEs), data analytics solutions, interoperability standards, and cybersecurity protocols. By harnessing the power of these systems, healthcare organizations can streamline data management processes, enhance security measures, and improve the overall quality of care [10].

One of the key benefits of advanced information systems in healthcare is their ability to centralize and standardize patient data, thereby facilitating seamless information exchange and interoperability across different healthcare settings [11]. EHR systems, for example, provide healthcare providers with a comprehensive view of patients' medical histories, medications, lab results, and treatment plans, regardless of where the care was delivered. This interoperability enables care coordination, reduces duplicate testing and procedures, and enhances patient safety by ensuring that clinicians have access to up-to-date and accurate information at the point of care.

Furthermore, advanced information systems play a critical role in enhancing data security and privacy in healthcare. Modern EHR systems employ robust encryption techniques, access controls, and audit trails to protect sensitive patient information from unauthorized access, data breaches, and cyberattacks [12, 13]. Additionally, advanced authentication methods, such as biometrics and multi-factor authentication, help verify the identity of users and prevent unauthorized access to patient records. By implementing these security measures, healthcare organizations can mitigate the risks associated with data breaches and ensure compliance with regulatory requirements such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) [14, 15].

Moreover, advanced information systems enable healthcare organizations to leverage data analytics and artificial intelligence (AI) technologies to derive actionable insights from large volumes of healthcare data [16]. By analyzing clinical data, financial data, and operational data, healthcare organizations can identify trends, patterns, and outliers that inform clinical decision- making, optimize resource allocation, and improve patient outcomes. For example, predictive analytics can help identify patients at risk for readmission or complications, enabling proactive interventions and personalized care plans.

Despite these benefits, integrating advanced information systems into healthcare poses several challenges including interoperability issues [17], data governance concerns [18], and cybersecurity threats. Interoperability standards such as Fast Healthcare Interoperability Resources (FHIR) aim to address these challenges by defining standardized data formats and protocols for exchanging health information between different systems and applications.

Additionally, healthcare organizations must implement robust data governance frameworks to ensure data integrity, privacy, and compliance with regulatory requirements. Cybersecurity remains a constant concern, requiring healthcare organizations to continually monitor and update their security measures to protect against evolving threats and vulnerabilities.

In conclusion, the integration of advanced information systems into healthcare holds tremendous promise for improving data management and security while enhancing the quality and efficiency of patient care. By leveraging these technologies effectively and addressing associated challenges, healthcare organizations can unlock the full potential of data-driven healthcare delivery and realize the vision of a safer, more interconnected, and patient-centered healthcare ecosystem.

Core technologies for advanced information systems

Advanced information systems in healthcare rely on a combination of core technologies to enable efficient data management, secure information exchange, and advanced analytics. Some of the core technologies include:

Electronic Health Records (EHRs): EHR systems serve as digital versions of patients' paper charts, containing comprehensive information about their medical history, diagnoses, medications, allergies, lab results, and treatment plans. EHRs facilitate real-time access to patient data by authorized healthcare providers, enabling seamless communication and care coordination across different healthcare settings [19].

Health Information Exchanges (HIEs): HIEs are platforms that facilitate the electronic sharing of patient health information among healthcare organizations, such as hospitals, clinics, pharmacies, and laboratories. HIEs enable interoperability by standardizing data formats and protocols, allowing healthcare providers to exchange information securely and efficiently, regardless of the systems they use

[20].

Data Analytics and Business Intelligence: Data analytics and business intelligence tools enable healthcare organizations to derive actionable insights from vast amounts of structured and unstructured data. By analyzing clinical, financial, and operational data, healthcare organizations can identify trends, patterns, and outliers that inform decision-making, optimize processes, and improve patient outcomes [21].

Interoperability Standards: Interoperability standards such as HL7 (Health Level Seven) and FHIR (Fast Healthcare Interoperability Resources) define common data formats and protocols for exchanging health information between different systems and applications. These standards enable seamless integration and interoperability across disparate healthcare IT systems, facilitating the exchange of patient data and enabling care coordination [22].

Cybersecurity Solutions: Cybersecurity solutions are essential for protecting sensitive patient information from unauthorized access, data breaches, and cyberattacks. These solutions encompass a range of technologies, including encryption, access controls, intrusion detection systems, and security monitoring tools, designed to safeguard electronic health records, communication channels, and network infrastructure from security threats.

Artificial Intelligence (AI) and Machine Learning: AI and machine learning technologies hold promise for revolutionizing healthcare by enabling advanced analytics, predictive modeling, and personalized medicine. AI-powered algorithms can analyze complex datasets, identify patterns, and make predictions about patient outcomes, supporting clinical decision-making, disease management, and population health initiatives [23].

Blockchain Technology: Blockchain technology offers a decentralized and immutable ledger for recording and sharing healthcare transactions securely. In healthcare, blockchain can be used to enhance data security, integrity, and transparency, enabling secure sharing of sensitive health information, authentication of medical records, and tracking of pharmaceutical supply chains [24].

Cloud Computing: Cloud computing enables healthcare organizations to store, manage, and access data and applications over the internet, without the need for on-premises infrastructure. Cloud-based solutions offer scalability, flexibility, and cost-effectiveness, allowing healthcare providers to leverage advanced information systems without the burden of managing and maintaining physical hardware and software [25].

By leveraging these core technologies, healthcare organizations can build advanced information systems that support data-driven decision-making, enhance care coordination, improve patient outcomes, and ensure the security and privacy of sensitive health information.

Impact of advanced information systems on data management Medical Records

Advanced information systems, particularly Electronic Health Records (EHRs), revolutionize the management of medical records by digitizing and centralizing patient information. EHRs allow healthcare providers to access comprehensive patient histories, treatment plans, medications, and diagnostic tests in real time, improving care coordination and efficiency [26]. Moreover, features such as electronic prescribing and automated reminders streamline administrative tasks, reducing errors and improving workflow. Despite the benefits, the digitization of medical records introduces security challenges. Advanced information systems must implement robust security measures, including encryption, access controls, and audit trails, to protect sensitive patient information from unauthorized access and data breaches. Additionally, regular security assessments and staff training are essential to mitigate risks and ensure compliance with regulatory requirements such as HIPAA [27].

Genomic Data

Advanced information systems enable the storage, analysis, and sharing of genomic data, offering unprecedented insights into an individual's genetic makeup and susceptibility to diseases. Genomic databases and bioinformatics platforms facilitate the management of vast amounts of genetic information, supporting research, clinical trials, and personalized medicine initiatives. Genomic data presents unique security challenges due to its sensitive and identifiable nature [28]. Advanced information systems must employ encryption, anonymization techniques, and access controls to protect genomic data from unauthorized access and misuse. Moreover, ethical considerations, such as informed consent and data ownership, play a crucial role in ensuring the responsible management and sharing of genomic information.

Data from Wearable Devices

Wearable devices, such as fitness trackers and smartwatches, generate a wealth of health-related data [29], including activity levels, heart rate, sleep patterns, and physiological measurements. Advanced information systems can integrate data from wearable devices into EHRs and health monitoring platforms, enabling healthcare providers to track patients' health status in real time and tailor interventions accordingly. The proliferation of wearable devices introduces security risks related to data privacy and integrity. Advanced information systems must implement encryption, secure authentication mechanisms, and data encryption protocols to protect wearable device data from interception and unauthorized access. Additionally, data governance policies should address issues such as data ownership, consent, and data-sharing practices to ensure patient privacy and trust.

In conclusion, advanced information systems play a crucial role in managing and securing medical records, genomic data, and data from wearable devices, each with its unique challenges. By implementing robust security measures, leveraging encryption technologies, and adhering to ethical and regulatory standards, healthcare organizations can harness the power of advanced information systems to improve patient care while safeguarding sensitive health information.

Table 1: Design and structure of advanced information systems in healthcare

Interoperability	The system would be built to easily interchange data with imaging, HIEs, laboratory information systems, EHRs, and other healthcare IT systems. The adoption of interoperability standards, including HL7 and FHIR, would make it easier to transfer structured and unstructured data between various platforms and systems.
Centralized Data Repository	A single source of truth for patient data would be provided via the system's centralized data repository. Complete patient records, including demographic data, medical history, prescriptions, allergies, test results, imaging studies, and treatment plans, would be kept in this repository to guarantee that medical professionals have access to current, correct information at the point of service.
Advanced Analytics Capabilities	To examine clinical, financial, and operational data, the system would include sophisticated analytics and business intelligence capabilities. This would allow healthcare companies to get actionable insights and make choices based on data. Trends, patterns, and outliers that influence clinical decision-making, maximize resource allocation, and enhance patient outcomes would be found using predictive analytics, machine learning algorithms, and data visualization approaches.
Robust Security Measures	Sensitive patient data would be protected from unwanted access, data breaches, and cyberattacks by implementing strong encryption, access restrictions, and authentication procedures. Security would be given top priority in the system's architecture. The system would also include capabilities for security monitoring, audit trails, and routine security assessments to guarantee adherence to legal obligations like GDPR and HIPAA.
Usability and User Experience	With its customizable dashboards, role-based access restrictions, and intuitive interfaces that accommodate various user roles and preferences, the system would be built with usability and user experience in mind. To enable users to efficiently navigate the system and make use of its capabilities to improve patient care and productivity, training and support materials would be made available.
Scalability and Flexibility	The system would be built to develop with healthcare institutions, adapting to their demands as technology advanced and data volumes and user bases increased. Modular design and cloud-based infrastructure would provide flexibility and agility, making it simple to integrate new applications and technologies as they become available.
Compliance with Regulatory Standards	The system would abide by legal requirements as well as industry best practices for privacy, security, and data management. To minimize the risk of non-compliance and related fines, regular audits, risk assessments, and compliance checks would be carried out to assure adherence to industry standards and regulatory requirements.

Conclusion

In conclusion, healthcare companies have a revolutionary chance to improve patient care and operational efficiency, as well as data management and security, through the integration of sophisticated information technologies. The main advantages of advanced information systems have been examined throughout this research, including effective data management, increased information accessibility, improved interoperability, strong data security and privacy measures, advanced analytics capabilities, and increases in operational efficiency.

Healthcare companies can centralize patient data, expedite care coordination, and extract useful insights from massive volumes of healthcare data by utilizing technologies like Artificial Intelligence (AI), Health Information Exchanges (HIEs), Electronic Health Records (EHRs), and data analytics platforms. Furthermore, by putting strong security measures, encryption methods, and access restrictions in place, patients' privacy and confidentiality are protected against cyber threats, illegal access, and data breaches involving sensitive patient information.

It is impossible to overestimate the role that sophisticated information systems will play in fostering innovation, raising standards, and improving patient experiences as healthcare continues to change in the digital era. Healthcare companies can leverage the full potential of sophisticated information systems to offer high-quality, patient-centered care securely and efficiently by making investments in technology, infrastructure, and workforce training a priority.

To solve issues like interoperability, data governance, cybersecurity, and regulatory compliance in the future, ongoing cooperation between healthcare stakeholders, legislators, technology suppliers, and regulatory bodies will be crucial. We can unleash the revolutionary potential of cutting-edge information technologies and bring the vision of a safer, more connected, and data- driven healthcare ecosystem for everyone to life by banding together to solve these challenges.

References

1. El Aboudi N, Benhlima L. Big Data Management for Healthcare Systems: Architecture, Requirements, and Implementation. Advances in Bioinformatics. 2018;2018:4059018. https://doi.org/10.1155/2018/4059018
2. Joukes E, De Keizer NF, De Bruijne M, Abu-Hanna A, Cornet R. Impact of Electronic versus Paper-Based Recording before EHR Implementation on Health Care Professionals' Perceptions of EHR Use, Data Quality, and Data Reuse. Applied Clinical Informatics. 2019;10(2):185–195. https://doi.org/10.1055/s-0039-1681054
3. Krousel-Wood M, McCoy AB, Ahia C, *et al*. Implementing electronic health records (EHRs): health care provider perceptions before and after transition from a local basic EHR to a commercial comprehensive EHR. J Am Med Inform Assoc. 2018;25(06):618–626.
4. Team D. The Disadvantages of Traditional Information Systems. Decision Management Solutions; c2015. Available from: https://decisionmanagementsolutions.com/14831/
5. Bhattacharjee M, Kaposy C, Grossman MR, Marshall Z. Patient photographs on Google Images: A commentary on informed consent, copyright, and privacy laws. Law, Innovation and Technology. 2023;15(2):536-557.
6. Nagi A. Comparing GDPR Against the United States' Approach to Data Breach Notification by Examining Texas and California and the Feasibility of a Universal Standard. Cybaris®. 2024;15(2):14.
7. Sah AK, Ming HY. An Analysis of Market Size Identification as a Strategy of Market Entry Research. Intersecta Minds Journal. 2024;5(1):60-75.
8. Adeniyi AO, Arowoogun JO, Chidi R, Okolo CA, Babawarun O. The impact of electronic health records on patient care and outcomes: A comprehensive review. World Journal of Advanced Research and Reviews.

2024;21(2):1446-1455.
9. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. Systems. 2023;11(1):38.
10. He W, Zhang JZ, Wu H, Li W, Shetty S. A Unified Health Information System Framework for Connecting Data, People, Devices, and Systems. Journal of Global Information Management. 2022;30(11):1–19.
11. Alowais SA, Alghamdi SS, Alsuhebany N, Alqahtani T, Alshaya AI, Almohareb SN. Revolutionizing healthcare: the role of artificial intelligence in clinical practice. BMC Medical Education. 2023;23(1):689.
12. Şerbănați LD. Health digital state and Smart EHR systems. Informatics in Medicine Unlocked [Internet]. 2020;20:100494. [cited 2024 Apr 21]; Available from: https://doi.org/10.1016/j.imu.2020.100494
13. Yogesh M, Karthikeyan J. Health Informatics: Engaging Modern Healthcare Units: A Brief Overview. Frontiers in Public Health; c2022. [cited 2024 Apr 21]; 10. Available from: https://doi.org/10.3389/fpubh.2022.854688
14. Fedorowicz J. Impact of HIPAA on the integrity of healthcare information. International Journal of Healthcare Technology and Management. 2024;5(1-2):11–24. [Internet]. [date unknown] [cited 2024 Apr 21]; Available from: https://www.inderscienceonline.com/doi/abs/10.1504/IJHTM.2004.004954
15. Lea NC, De Meyer F. How Will the General Data Protection Regulation Affect Healthcare? Acta Médica Portuguesa. 2018;31(7–8):363–365. https://doi.org/10.20344/amp.10881
16. Leone D, Schiavone F, Appio FP, Chiao B. How does artificial intelligence enable and enhance value co-creation in industrial markets? An exploratory case study in the healthcare ecosystem. Journal of Business Research. 2021;129:849–859. https://doi.org/10.1016/j.jbusres.2020.11.008
17. Nardi EA, Lentz LK, Winckworth-Prejsnar K, Abernethy AP, Carlson RW. Emerging Issues and Opportunities in Health Information Technology. Journal of the National Comprehensive Cancer Network. 2016;14(10):1231–1236. https://doi.org/10.6004/jnccn.2016.0132
18. Winter JS, Davidson E. Big data governance of personal health information and challenges to contextual integrity. The Information Society. 2018;35(1):1–20. https://doi.org/10.1080/01972243.2018.1542648
19. Seymour T, Frantsvog D, Graeber T. Electronic Health Records (EHR). American Journal of Health Sciences. 2012;3(3):153–159. https://doi.org/10.19030/ajhs.v3i3.7139
20. Menachemi N, Rahurkar S, Harle CA, Vest JR. The benefits of health information exchange: an updated systematic review. Journal of the American Medical Informatics Association. 2018;25(9):1259–1265. https://doi.org/10.1093/jamia/ocy035
21. Khedr A, Kholeif S, Saad F. An Integrated Business Intelligence Framework for Healthcare Analytics. International Journal of Advanced Research in Computer Science and Software Engineering. 2017;7(5):263–270. https://doi.org/10.23956/ijarcsse/sv7i5/0163
22. Strasberg HR, Rhodes B, Del Fiol G, Jenders RA, Haug PJ, Kawamoto K. Contemporary clinical decision support standards using Health Level Seven International Fast Healthcare Interoperability Resources. Journal of the American Medical Informatics Association. 2021;28(8):1796–1806. https://doi.org/10.1093/jamia/ocab070
23. Stanfill MH, Marc DT. Health Information Management: Implications of Artificial Intelligence on Healthcare Data and Information Management. Yearbook of Medical Informatics. 2019;28(1):35–40. https://doi.org/10.1055/s-0039-1677913
24. Bittins S, Kober G, Margheri A, Masi M, Miladi A, Sassone V. Healthcare Data Management by Using Blockchain Technology. Studies in Big Data (Internet). 2020;10(1):3–33. https://doi.org/10.1007/978-981-15-9547-9_1
25. Sharma DK, Chakravarthi DS, Shaikh AA, Ahmed AAA, Jaiswal S, Naved M. The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique. Materials Today: Proceedings. 2023;50(2):732–737. https://doi.org/10.1016/j.matpr.2021.07.388
26. Leventhal JC, Cummins J, Schwartz PH, Martin DK, Tierney WM. Designing a System for Patients Controlling Providers' Access to their Electronic Health Records: Organizational and Technical Challenges. Journal of General Internal Medicine. 2014;30(6):7–12. https://doi.org/10.1007/s11606-014-3055-y
27. Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy. Computers in Biology and Medicine. 2021;129:1–12. https://doi.org/10.1016/j.compbiomed.2020.104130
28. Arshad S, Arshad J, Khan MM, Parkinson S. Analysis of security and privacy challenges for DNA-genomics applications and databases. Journal of Biomedical Informatics. 2021;125:1–18. https://doi.org/10.1016/j.jbi.2021.103815
29. Yıldırım SZ, Pancar T. Smart Wearable Technology for Health Tracking: What Are the Factors that Affect Their Use? Studies in Computational Intelligence (Print). 2021;959:177–197. https://doi.org/10.1007/978-981-15-9897-5_9
30. Tranfield D, Denyer D, Smart P. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. British Journal of Management. 2003;14(3):207–222. https://doi.org/10.1111/1467-8551.00375