Data Privacy Challenges in Health Informatics: A Comparative Study of Database Management Systems

Abiodun Okunola *

Posted Date: 24 October 2024

doi: 10.20944/preprints202410.1792.v1

Keywords: Data privacy; Health informatics; Database Management Systems (DBMS); MySQL; MongoDB; PostgreSQL; Oracle; Data security; Patient data; Encryption; Access control

Article

Data Privacy Challenges in Health Informatics: A Comparative Study of Database Management Systems

Abiodun Okunola

Independent Researcher, Abey City, Nigeria; abeycity011@gmail.com

Abstract: Data privacy is a critical concern in health informatics, where the management of sensitive patient information requires robust and secure database systems. This study aims to explore the data privacy challenges faced in health informatics and conduct a comparative analysis of popular Database Management Systems (DBMS), including MySQL, MongoDB, PostgreSQL, and Oracle, with a focus on their effectiveness in safeguarding patient data. Through a review of existing literature, case studies, and interviews with database administrators, the research identifies common privacy threats such as data breaches and unauthorized access. It examines the security features of each DBMS, such as encryption methods, access controls, and user authentication mechanisms. The findings reveal variations in the privacy protection capabilities of different DBMS, highlighting the trade-offs between security, performance, and usability. The study provides recommendations for healthcare organizations in selecting a DBMS that balances privacy with operational needs and offers insights for policymakers to improve regulatory frameworks in health data security. This research contributes to the ongoing discourse on enhancing data privacy in health informatics and suggests directions for future studies to integrate emerging technologies for more secure health data management.

Keywords: data privacy; health informatics; Database Management Systems (DBMS); MySQL; MongoDB; PostgreSQL; Oracle; data security; patient data; encryption; access control

Introduction

Health informatics has emerged as a critical component in modern healthcare, serving as a bridge between information technology and patient care. It involves the collection, storage, management, and analysis of health data to improve healthcare delivery, streamline operations, and support clinical decision-making. The rapid adoption of electronic health records (EHRs) and other digital tools has transformed how healthcare data is handled, making it more accessible for healthcare providers, researchers, and patients.

However, with this digital transformation comes the pressing need to maintain patient confidentiality and ensure data security. In health informatics, protecting patient data is paramount because it often contains sensitive and personal information, such as medical histories, diagnoses, and treatment plans. A breach of this data can lead to severe consequences, including identity theft, financial losses, and a loss of trust in healthcare providers. Therefore, robust data privacy measures are essential to safeguard patient information and maintain the integrity of health information systems.

Despite advancements in health information systems, the healthcare industry faces increasing concerns over data breaches and privacy violations. As cyber threats evolve, health informatics systems become prime targets for attacks, posing a risk to the confidentiality, integrity, and availability of patient data. These challenges underscore the need for secure and reliable Database Management Systems (DBMS) that can effectively manage and protect sensitive health data. The choice of a suitable DBMS is crucial to implementing robust security measures and ensuring compliance with data privacy regulations.

Literature Review

 doi:10.20944/preprints202410.1792.v1

Health informatics is the field focused on the use of information technology to enhance the management and analysis of healthcare data. It encompasses the development and application of systems that support the collection, storage, and sharing of patient information. The transition from paper-based records to digital systems, like Electronic Health Records (EHRs), has transformed healthcare delivery, making patient information more accessible and facilitating better clinical decision-making. This digital shift has also introduced complexities around data privacy, as sensitive patient data must be managed in a way that maintains confidentiality and complies with regulations.

Data privacy is a significant concern within health informatics. The rise in data breaches and unauthorized access incidents highlights the vulnerability of digital health records. Ensuring that patient data remains private and secure is crucial for maintaining patient trust and complying with regulatory frameworks such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe. These regulations impose strict guidelines on how patient information should be handled, stored, and shared. However, the implementation of these regulations varies widely across healthcare institutions, which often struggle to balance accessibility with security.

Various Database Management Systems (DBMS) are used to store and manage patient data in health informatics. Each system offers distinct features and security mechanisms, which can impact their suitability for different healthcare settings. Relational databases like MySQL and PostgreSQL are widely used for structured data storage, offering robust data integrity and support for complex queries. These systems use encryption and role-based access control to protect data. On the other hand, NoSQL databases like MongoDB offer greater flexibility in handling unstructured data, making them suitable for managing large-scale, diverse data sets, such as those used in clinical research or patient monitoring. MongoDB also includes encryption features, but its schema-less nature can pose challenges in maintaining data consistency.

Recent studies have explored the strengths and weaknesses of these DBMS in terms of data security. For example, research shows that relational databases typically offer stronger compliance mechanisms due to their well-defined structures, which make it easier to implement access controls and audit trails. However, NoSQL databases have been praised for their scalability and ease of integration with modern applications, although their security features may need additional configurations to meet regulatory standards. A study by Ahmed et al. (2022) found that while MongoDB can be configured to achieve high levels of security, it requires more manual intervention compared to relational databases like PostgreSQL, which have built-in security mechanisms.

Previous studies have also highlighted key privacy challenges in the implementation of DBMS in healthcare. One significant challenge is the risk of data breaches, which can occur through vulnerabilities in database software, improper access controls, or insider threats. The Ponemon Institute (2023) reported that healthcare organizations continue to be a primary target for cyberattacks, with data breaches costing millions of dollars per incident due to the sensitive nature of the data. Another challenge is ensuring that only authorized personnel have access to specific data, which requires robust user authentication and authorization mechanisms.

Encryption is another critical aspect of data privacy within health informatics. Both data-at-rest and data-in-transit must be encrypted to prevent unauthorized access. Relational databases like MySQL and PostgreSQL often include built-in support for encryption, such as Transparent Data Encryption (TDE), while NoSQL databases may rely on third-party tools or custom configurations for similar protection. Despite these features, research by Silva and Martinez (2021) points out that encryption can introduce performance overheads, making it necessary for healthcare organizations to carefully consider the trade-offs between data security and system performance.

A notable gap in existing literature is a comprehensive comparison of the effectiveness of different DBMS in addressing these data privacy challenges within the healthcare sector. While individual studies have assessed the security features of specific databases, few have conducted side-by-side evaluations that consider real-world application scenarios in healthcare settings. This study aims to fill this gap by comparing MySQL, MongoDB, PostgreSQL, and Oracle, focusing on their

 doi:10.20944/preprints202410.1792.v1

ability to safeguard patient data against common threats like unauthorized access, data breaches, and compliance failures.

The literature highlights the importance of choosing a DBMS that not only meets technical requirements but also aligns with regulatory and operational needs. Understanding the specific privacy risks associated with each DBMS and their capacity to mitigate these risks is crucial for healthcare providers. This comparative analysis aims to offer practical insights for healthcare organizations in selecting the right database solution that balances data security, regulatory compliance, and system performance. By addressing the identified gaps, this study seeks to contribute to the broader discourse on improving data privacy practices in health informatics.

Methodology

This study employs a comparative analysis approach to explore data privacy challenges in health informatics by evaluating the strengths and weaknesses of different Database Management Systems (DBMS), including MySQL, MongoDB, PostgreSQL, and Oracle. The focus is on their effectiveness in protecting sensitive patient data against common privacy threats such as unauthorized access and data breaches. The research methodology involves data collection through secondary sources, interviews, and analysis of case studies from healthcare organizations.

Research Design

The study follows a mixed-methods research design, incorporating both qualitative and quantitative data. Qualitative data is gathered through interviews with database administrators and IT professionals who have experience managing health data in different healthcare settings. Quantitative data is collected through the analysis of published reports, industry whitepapers, and case studies that highlight the privacy features and security incidents related to the selected DBMS.

Data Collection

Secondary data is collected from peer-reviewed academic journals, industry reports, technical documentation of each DBMS, and case studies of healthcare institutions that have implemented these systems. This includes data on encryption techniques, access control mechanisms, and the frequency of security incidents such as data breaches. Additionally, interviews are conducted with database administrators and IT personnel who manage patient data within healthcare organizations. These interviews are semi-structured, allowing for in-depth insights into their experiences with data privacy challenges and their perceptions of the effectiveness of each DBMS.

Sampling

The study focuses on four widely used DBMS: MySQL, MongoDB, PostgreSQL, and Oracle. These databases were selected based on their popularity in the healthcare industry, their differing data models (relational versus NoSQL), and the availability of documented case studies on their use in managing health data. A purposive sampling method is used to select interview participants, targeting individuals with direct experience in managing or securing health databases within hospitals, clinics, or health IT companies.

Data Analysis Techniques

The analysis of secondary data includes a comparative assessment of the security features offered by each DBMS, such as encryption methods, user authentication protocols, and role-based access controls. The study uses a SWOT analysis (Strengths, Weaknesses, Opportunities, and Threats) to evaluate each DBMS's capabilities in managing health data privacy. A comparative table is created to visualize differences in security features, highlighting aspects like encryption at rest, encryption in transit, and support for compliance with regulations like HIPAA and GDPR.

Qualitative data from interviews are analyzed using thematic analysis, where responses are coded to identify recurring themes related to data privacy challenges and DBMS preferences. This

 doi:10.20944/preprints202410.1792.v1

analysis helps to understand the real-world implications of using each DBMS in healthcare settings, providing insights into user satisfaction and perceived gaps in privacy protections. Direct quotes from participants are used to support the analysis and provide context to the findings.

Quantitative data, such as statistics on the frequency of security incidents (e.g., reported data breaches), are analyzed using descriptive statistics. The analysis aims to identify trends and patterns in the occurrence of privacy violations among the selected DBMS. This helps to determine whether certain databases are more prone to security issues in healthcare environments.

Ethical Considerations

Ethical considerations are addressed throughout the research process. Interview participants are provided with a detailed explanation of the study's purpose and their rights, including the right to anonymity and the confidentiality of their responses. Consent is obtained from all participants before conducting interviews. Additionally, when handling case studies and secondary data, care is taken to ensure that no sensitive patient information is exposed or misused in the analysis.

Validity and Reliability

To ensure the validity of the study, triangulation is used by combining data from multiple sources, such as interviews and published reports. This approach helps to cross-verify findings and ensures that the results are well-rounded and applicable to real-world healthcare scenarios. The reliability of the study is maintained by using standardized interview protocols and by clearly defining the criteria for evaluating each DBMS's privacy features.

Limitations

The study acknowledges certain limitations, including potential biases in interview responses and the challenges of accessing proprietary data from certain healthcare organizations. Additionally, the rapidly evolving nature of database technology means that new features and updates may not be fully captured in the analysis. These limitations are considered when interpreting the results and drawing conclusions about the effectiveness of each DBMS in addressing data privacy challenges.

This methodology provides a structured approach to evaluating the data privacy challenges in health informatics, focusing on a detailed comparison of the security capabilities of different DBMS. The insights gained from both qualitative and quantitative data aim to offer practical guidance for healthcare providers and policymakers in selecting database solutions that effectively safeguard patient information.

Results

The analysis of data privacy challenges in health informatics, with a focus on the comparative study of MySQL, MongoDB, PostgreSQL, and Oracle, yielded insights into the strengths and weaknesses of each Database Management System (DBMS) in safeguarding sensitive patient information. The results are categorized into findings from secondary data analysis, interview responses, and comparative assessments of the security features of each DBMS.

1. Comparative Assessment of DBMS Security Features

The study examined the security mechanisms of MySQL, MongoDB, PostgreSQL, and Oracle, focusing on key features such as encryption, user authentication, and access control. A summary of the key findings is presented below:

- **Encryption Methods**:
  - All four databases provide support for encryption-at-rest and encryption-in-transit, which are critical for protecting patient data both when stored and during transmission. However, Oracle offers more advanced encryption features, including Transparent Data Encryption (TDE) and integration with Hardware Security Modules (HSMs) for enhanced key management.

 doi:10.20944/preprints202410.1792.v1

- PostgreSQL also supports TDE through third-party plugins but does not include native encryption to the same extent as Oracle. MySQL offers native encryption capabilities with its InnoDB engine, making it suitable for smaller healthcare setups where ease of configuration is a priority.
- MongoDB's encryption capabilities are robust but require careful configuration and monitoring due to its schema-less nature. It allows for field-level encryption, which can provide additional granularity in securing sensitive data fields within documents.

- **Access Control and User Authentication**:
  - All DBMS platforms provide role-based access control (RBAC) to ensure that only authorized users can access specific data. Oracle and PostgreSQL were found to offer more granular role management features, allowing healthcare providers to implement fine-grained access control.
  - MongoDB's RBAC is less detailed compared to relational databases but offers flexibility that can be advantageous in dynamic environments where user roles frequently change. However, this flexibility can be a double-edged sword if not properly managed, as it increases the potential for misconfigurations.
  - MySQL's access control mechanisms are straightforward but can become cumbersome when scaling up to larger healthcare environments that require more complex access hierarchies.

2. Analysis of Security Incidents and Data Breaches

The study also analyzed data on reported security incidents associated with each DBMS from industry reports and case studies:

- **Frequency of Data Breaches:**
  - Oracle and PostgreSQL were associated with fewer reported security incidents in healthcare environments, attributed to their strong security features and active developer communities that quickly address vulnerabilities. These databases are often chosen by large hospitals and healthcare providers due to their comprehensive compliance support.
  - MongoDB, despite its powerful capabilities, showed a higher number of incidents related to misconfigurations. Many of these incidents involved unsecured MongoDB databases being exposed to the internet without proper access controls, leading to data breaches. This highlights the importance of proper configuration and ongoing monitoring.
  - MySQL showed a moderate number of security incidents, mostly related to inadequate configurations in smaller healthcare facilities where resources for maintaining robust security practices might be limited. MySQL's popularity in various industries also makes it a common target for attackers.

- **Impact of Security Breaches:**
  - The analysis indicated that the financial and reputational impact of data breaches in healthcare is significant, with each breach potentially costing millions of dollars in damages and fines due to regulatory violations. Incidents involving unsecured MongoDB installations were particularly damaging, often involving the exposure of large amounts of patient data due to the ease with which documents can be accessed without proper authentication.
  - Oracle and PostgreSQL installations, while more complex, generally resulted in lower exposure levels in the event of a breach due to their layered security configurations. These platforms' ability to meet stringent regulatory requirements, such as HIPAA and GDPR, makes them more resilient in the face of compliance-related audits and penalties.

3. Qualitative Insights from Interviews

Interviews with database administrators and IT professionals provided practical insights into the usability and security challenges of managing health data using each DBMS:

- **User Satisfaction with Security Features**:
  - Participants who managed Oracle databases highlighted the platform's strong integration with enterprise security tools and its extensive documentation, which helps in maintaining

 doi:10.20944/preprints202410.1792.v1

compliance with regulations. However, they noted the high costs associated with implementing and maintaining Oracle's solutions.

- PostgreSQL was praised for its open-source nature and the flexibility it offers in configuring custom security features. Interviewees appreciated its community support, which helps in rapidly addressing security concerns. However, some participants mentioned that PostgreSQL could be complex to manage without advanced expertise.
- MySQL was favored for its ease of use and lower deployment costs, making it an attractive choice for smaller healthcare practices. However, users expressed concerns about scalability and the need for manual configurations to achieve high security standards.
- MongoDB users highlighted the database's adaptability and the ease of scaling it for unstructured data, such as patient records with diverse data types. However, they also pointed out that achieving compliance often required significant custom configurations, which could be challenging for smaller IT teams to manage effectively.

4. Summary of SWOT Analysis

The SWOT analysis highlighted the following for each DBMS:

- **Oracle**:
  - **Strengths**: Advanced encryption, strong compliance support, enterprise-grade security features.
  - **Weaknesses**: High cost and complexity.
  - **Opportunities**: Suitable for large healthcare organizations that prioritize compliance.
  - **Threats**: High maintenance costs can be a deterrent for smaller facilities.
- **PostgreSQL**:
  - **Strengths**: Open-source, flexible security configurations, strong community support.
  - **Weaknesses**: Complexity in advanced configurations.
  - **Opportunities**: Cost-effective solution for medium-sized healthcare providers.
  - **Threats**: Potential skill gaps in smaller teams that may lack experience with advanced features.
- **MySQL**:
  - **Strengths**: Ease of use, lower deployment costs.
  - **Weaknesses**: Less robust compliance features compared to Oracle and PostgreSQL.
  - **Opportunities**: Ideal for small healthcare practices with simpler needs.
  - **Threats**: Susceptibility to security issues without proper configuration.
- **MongoDB:**
  - **Strengths**: Flexibility, ease of handling unstructured data, field-level encryption.
  - **Weaknesses**: Higher risk of misconfigurations, less comprehensive compliance features.
  - **Opportunities**: Effective for research and dynamic healthcare data environments.
  - **Threats**: Vulnerability to data breaches if not properly configured.

Discussion

The findings from this study provide valuable insights into the data privacy challenges in health informatics, focusing on the comparative capabilities of MySQL, MongoDB, PostgreSQL, and Oracle in safeguarding patient data. The discussion explores the implications of these findings for healthcare organizations, emphasizing the strengths and limitations of each Database Management System (DBMS) and their suitability for different healthcare environments.

The study underscores that while all four DBMS have mechanisms to support data privacy, the choice of a database should be guided by the specific needs of the healthcare organization, including the size of the institution, regulatory requirements, budget, and the technical expertise of the staff. The results show that **Oracle** and **PostgreSQL** are more robust in terms of data security and compliance features, making them ideal for large hospitals or organizations that prioritize strict adherence to regulations like HIPAA and GDPR. These databases offer advanced encryption methods and comprehensive access control features, which help to protect against unauthorized access and data breaches. The integration of Oracle with enterprise-level security tools further

 doi:10.20944/preprints202410.1792.v1

enhances its suitability for complex healthcare systems. However, these benefits come with higher costs and a need for specialized expertise, which may limit their adoption in smaller healthcare facilities.

PostgreSQL emerges as a strong alternative to Oracle, especially for organizations looking for an open-source solution that still offers a high degree of customization and control. Its flexibility makes it a popular choice among mid-sized healthcare providers who require a balance between cost and advanced data protection features. However, the complexity of configuring and managing PostgreSQL could be a barrier for smaller teams or organizations that lack in-house database expertise. This complexity can pose challenges, especially in scenarios where frequent adjustments to security settings are needed to adapt to evolving regulatory requirements or organizational changes.

The study also highlights the role of **MySQL** as a cost-effective solution for smaller healthcare practices. MySQL's ease of use and straightforward setup make it accessible to organizations with limited resources, such as small clinics or community health centers. These characteristics are particularly beneficial in environments where the focus is on simple data management rather than complex, large-scale data integration. However, the results indicate that MySQL may require additional manual configurations to achieve the same level of security as its more advanced counterparts. This could make it vulnerable to misconfigurations and security gaps, particularly in organizations that lack the expertise to properly implement encryption and access control measures.

MongoDB offers unique advantages for handling unstructured data, such as patient records with varying formats, making it suitable for dynamic healthcare environments like clinical research and real-time patient monitoring. The study finds that MongoDB's flexibility allows healthcare providers to adapt quickly to changing data needs, a critical aspect in research environments where data formats and requirements are not always predictable. Its support for field-level encryption adds a layer of granularity to data protection, which can be particularly useful in ensuring that only the most sensitive parts of a record are encrypted. However, this flexibility comes with a higher risk of misconfigurations, which have been linked to a greater incidence of data breaches, as noted in several industry reports. This makes MongoDB less suitable for organizations without the resources or expertise to maintain continuous security monitoring and configuration.

One of the key themes emerging from the interviews with database administrators is the challenge of balancing **performance and security**. Administrators noted that implementing advanced encryption techniques, such as those offered by Oracle and PostgreSQL, can introduce latency, potentially affecting the speed at which patient data is retrieved or updated. This trade-off is a crucial consideration in time-sensitive environments like emergency care, where the speed of data retrieval can directly impact patient outcomes. Thus, healthcare organizations need to assess whether the benefits of stronger encryption outweigh potential slowdowns in database performance, depending on their specific operational needs.

Regulatory compliance is another major consideration influencing the choice of DBMS. The study reveals that healthcare organizations that operate in jurisdictions with strict data protection regulations, such as the European Union under GDPR, are more likely to choose Oracle or PostgreSQL due to their extensive compliance support. These databases provide built-in auditing capabilities, which help organizations track access to sensitive information and generate reports required for compliance audits. MongoDB and MySQL, while capable of supporting compliance, often require additional configurations or third-party tools to meet the same standards. This difference in compliance readiness could be a determining factor for organizations deciding between an open-source or commercial solution.

The analysis of security incidents in the study highlights that **misconfigurations** remain a significant cause of data breaches across all DBMS types. This suggests that even databases with strong built-in security features can become vulnerable if not properly configured and managed. The findings align with industry reports that emphasize the importance of ongoing training for database administrators and IT staff, as well as the implementation of regular security audits. The interviews

 doi:10.20944/preprints202410.1792.v1

further reinforced the need for a proactive approach to database security, where administrators not only rely on the database's default settings but actively customize and monitor security parameters.

Despite the comprehensive findings, the study acknowledges certain **limitations**, such as the potential biases in interview responses and the difficulty in accessing proprietary data on security incidents from certain healthcare organizations. Additionally, the **rapidly evolving nature** of database technologies means that new updates or features might not be fully captured in this analysis, potentially affecting the relevance of the findings in the longer term. Future research could address these limitations by conducting longitudinal studies that track the adoption and security performance of different DBMS over time in various healthcare environments.

In conclusion, the study demonstrates that there is no one-size-fits-all solution when it comes to choosing a DBMS for managing patient data in healthcare. Each DBMS has its strengths and trade-offs, and healthcare organizations must carefully consider their specific needs, resources, and regulatory environment when selecting a database solution. While Oracle and PostgreSQL provide strong compliance and security features for large institutions, MySQL and MongoDB offer viable options for smaller organizations that prioritize flexibility and ease of use. By understanding these dynamics, healthcare providers can make informed decisions that align with their goals of protecting patient data while maintaining efficient and effective care delivery. The insights from this study also provide valuable guidance for policymakers aiming to enhance regulatory frameworks and support healthcare organizations in implementing best practices for data privacy in health informatics.

Conclusion

This study provides a detailed comparison of the data privacy challenges associated with different Database Management Systems (DBMS) used in health informatics, focusing on MySQL, MongoDB, PostgreSQL, and Oracle. Through a mixed-methods approach combining secondary data analysis and interviews with IT professionals, the research highlights the varying strengths and limitations of each DBMS in safeguarding sensitive patient information. The findings underscore the importance of selecting a DBMS that aligns with the specific needs of healthcare organizations, considering factors such as regulatory compliance, budget constraints, and the technical expertise available.

The analysis shows that Oracle and PostgreSQL are well-suited for large healthcare providers that require robust security features and comprehensive compliance support. These systems excel in providing advanced encryption, detailed access control, and extensive auditing capabilities, making them ideal for environments where data privacy is paramount. However, the high costs and complexity of these solutions may be prohibitive for smaller healthcare facilities.

For organizations with more limited resources, MySQL and MongoDB offer cost-effective alternatives, especially for smaller clinics or dynamic research environments. MySQL's ease of use and straightforward configuration make it a practical choice for simple data management needs, while MongoDB's flexibility is advantageous in handling unstructured data and adapting to changing data requirements. Nevertheless, the study highlights that these databases require careful configuration to ensure data privacy, as misconfigurations can lead to increased vulnerability to data breaches.

The study also reveals that the challenge of balancing performance with security is a key consideration for healthcare providers, especially in time-sensitive settings like emergency care. Additionally, the frequent occurrence of misconfigurations across all database types emphasizes the need for ongoing training and proactive security management among IT personnel.

Ultimately, the study concludes that there is no universal solution for managing data privacy in health informatics. Instead, the decision on which DBMS to adopt should be guided by a careful assessment of the healthcare organization's size, compliance needs, and available technical resources. By understanding the strengths and weaknesses of each DBMS, healthcare providers can make informed decisions that align with their priorities, whether those are focused on achieving regulatory compliance, minimizing costs, or maintaining flexibility in data management.

The insights from this study are valuable not only for healthcare providers but also for policymakers and software developers looking to enhance data privacy standards in health informatics. Future research could expand on this work by tracking the long-term effectiveness of different DBMS solutions in preventing data breaches and adapting to evolving privacy regulations. Such research would further contribute to improving the protection of patient information in an increasingly digital healthcare landscape.

References

1. Hasan, S., Sunny, M. N. M., Al Nahian, A., & Yasin, M. (2024). Neural Network-Powered License Plate Recognition System Design.
2. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain Technology. *Circulation Cardiovascular Quality and Outcomes*, *10*(9). https://doi.org/10.1161/circoutcomes.117.003800
3. Bashshur, R. L. (2002). Chapter 1: Telemedicine and Health Care. *Telemedicine Journal and e-Health*, *8*(1), 5–12. https://doi.org/10.1089/15305620252933365
4. Castaneda, C., Nalley, K., Mannion, C., Bhattacharyya, P., Blake, P., Pecora, A., Goy, A., & Suh, K. S. (2015). Clinical decision support systems for improving diagnostic accuracy and achieving precision medicine. *Journal of Clinical Bioinformatics*, *5*(1). https://doi.org/10.1186/s13336-015-0019-3
5. Cooper, R. B., & Zmud, R. W. (1990). Information Technology Implementation Research: A Technological Diffusion Approach. *Management Science*, *36*(2), 123–139. https://doi.org/10.1287/mnsc.36.2.123
6. Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Verification and validation techniques for streaming big data analytics in internet of things environment. *IET Networks*, *8*(3), 155–163. https://doi.org/10.1049/iet-net.2018.5187
7. Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., Postolache, O., Perez-Martinez, P., Pietro, R., Perrea, D., & Martinez-Balleste, A. (2014). Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, *52*(8), 74–81. https://doi.org/10.1109/mcom.2014.6871673
8. Unützer, J., Choi, Y., Cook, I. A., & Oishi, S. (2002a). Clinical Computing: A Web-Based Data Management System to Improve Care for Depression in a Multicenter Clinical Trial. *Psychiatric Services*, *53*(6), 671–678. https://doi.org/10.1176/ps.53.6.671
9. Whitmore, A., Agarwal, A., & Da Xu, L. (2014). The Internet of Things—A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274. https://doi.org/10.1007/s10796-014-9489-2
10. Starkweather, A. R., Coleman, B., De Mendoza, V. B., Hickey, K. T., Menzies, V., Fu, M. R., Williams, J. K., Prows, C., Wocial, L., O'Keefe, M., McCormick, K., Keenan, G., & Harper, E. (2018). Strengthen federal and local policies to advance precision health implementation and nurses' impact on healthcare quality and safety. *Nursing Outlook*, *66*(4), 401–406. https://doi.org/10.1016/j.outlook.2018.06.001