Online at: https://researchtrendsjournal.com **ISSN No:** 2584-282X

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 2; Issue 3; 2024; Page No. 176-182

Received: 17-02-2024
Accepted: 29-03-2024

Securing patient data: An empirical evaluation of role-based access control in healthcare environments

[1]Taduri Suneetha and [2]Dr. Amit Singhal

[1]Research Scholar, Department of Computer Science & Engineering, Monad University, Hapur, Uttar Pradesh, India
[2]Professor, Department of Computer Science & Engineering, Monad University, Hapur, Uttar Pradesh, India

Corresponding Author: Taduri Suneetha

Abstract

Role-Based Access Control (RBAC) has become one of the most widely adopted methods for safeguarding electronic health records (EHRs) in contemporary healthcare environments. By assigning permissions to roles rather than individuals, RBAC aims to streamline access privileges and mitigate risks associated with inappropriate data exposure. This paper presents an in-depth examination of RBAC within the healthcare sector, highlighting its theoretical underpinnings, practical applications, benefits, and limitations. The study employs a mixed-methods approach, combining a systematic literature review, expert interviews, and a survey of healthcare information technology professionals to gauge the efficacy of RBAC implementations. Findings reveal that while RBAC significantly enhances data security and compliance with regulations, its effectiveness can be undermined by organisational challenges such as poorly defined roles, lack of ongoing training, and insufficient policy enforcement. Moreover, rapid technological evolution and the growing need for cross-institutional data sharing introduce complexities that traditional RBAC systems may struggle to address. This paper proposes strategies to refine RBAC models, including dynamic role assignment, integration with emerging technologies like blockchain, and the importance of a robust organisational culture that prioritises security. Ultimately, the study underscores that a well-implemented RBAC framework, when combined with complementary security measures and comprehensive governance, can substantially reduce the risk of data breaches and bolster patient trust in digital healthcare systems.

Keywords: Role-based access control, electronic health records, data security, healthcare IT, patient privacy, access management, RBAC implementation

Introduction

The digital transformation of healthcare has revolutionised the way patient information is stored, accessed, and managed. With the advent of Electronic Health Records (EHRs), healthcare providers can more efficiently track patient histories, share data across departments, and improve overall patient outcomes. However, the transition to digital platforms has also introduced significant security challenges, as large volumes of sensitive data become vulnerable to unauthorised access, data breaches, and malicious attacks (Alotaibi & Federico, 2017) [2]. In light of these concerns, healthcare organisations are under growing pressure to implement robust security frameworks that protect patient privacy and maintain data integrity.

Role-Based Access Control (RBAC) is one such framework that has gained considerable traction for its potential to balance the competing demands of accessibility and security. Unlike discretionary or mandatory access control models, RBAC assigns permissions to roles rather than individuals, thereby streamlining the management of user privileges (Ferraiolo *et al*., 1995) [5]. Within a healthcare setting, these roles might include physicians, nurses, administrative staff, and specialised personnel, each requiring different levels of access to patient information. By mapping privileges to predefined roles, RBAC can theoretically reduce the risk of human error, facilitate compliance with data protection regulations, and create a clearer, more auditable trail of user activity (Kraemer & Carayon, 2017) [9].

Despite its widespread adoption, questions remain about the real-world efficacy of RBAC in healthcare environments. For example, the fluid nature of healthcare roles-where

responsibilities can overlap or shift due to staff rotations, departmental changes, or emergencies-can introduce complexities in defining and maintaining strict role boundaries (Lai *et al*., 2019) [12]. Additionally, rapid technological innovations such as telemedicine platforms, mobile health applications, and the increasing reliance on cloud-based services mean that traditional RBAC systems must adapt to accommodate emerging security threats and new forms of data sharing (Kulkarni *et al*., 2020) [10]. Organisational culture, employee training, and the robustness of supporting policies also play a vital role in determining whether RBAC frameworks truly achieve their intended objectives.

This paper seeks to provide a comprehensive exploration of RBAC's effectiveness in protecting EHRs within contemporary healthcare settings. The research objectives are threefold:

1. To examine the theoretical foundations and current implementations of RBAC in healthcare.
2. To evaluate the practical challenges and limitations that organisations face when deploying RBAC for EHR protection.
3. To propose potential enhancements and complementary measures that could strengthen RBAC-based security models.

By combining a thorough literature review with empirical data collected from IT professionals, healthcare administrators, and industry experts, this study aims to offer both academic and practical insights. The hope is that healthcare organisations, policymakers, and researchers can use these findings to refine their security strategies and mitigate the growing threats to patient data.

In the following sections, the paper will first present a critical review of existing literature on RBAC and its application in healthcare contexts. It will then outline the methodology used to collect and analyse data, including a survey and interviews. The subsequent sections will present the results, followed by an in-depth discussion of the findings. Finally, the conclusion will summarise the key takeaways and suggest avenues for future research in this rapidly evolving domain.

Literature Review

1. Overview of Role-Based Access Control

Role-Based Access Control was first formally introduced in the 1990s as a means to simplify and standardise the assignment of user privileges (Ferraiolo *et al*., 1995) [5]. In essence, RBAC revolves around the concept that access permissions should be tied to a role, which reflects a particular job function or responsibility, rather than an individual's identity. This separation of identity from privilege allocation is intended to reduce administrative overhead and enhance security by minimising opportunities for privilege abuse (Sandhu *et al*., 1996) [14].

2. RBAC in Healthcare Contexts

Healthcare is a prime setting for RBAC due to the diverse array of roles within hospitals, clinics, and research institutions. Physicians, nurses, administrative staff, technicians, and researchers often require different levels of access to EHRs (Johnson *et al*., 2018) [8]. The granular control provided by RBAC allows organisations to define which roles can read, write, or modify specific types of data. For instance, a nurse may have read-only access to certain patient records, while a specialist consultant might have permission to both view and update records related to a specific condition.

3. Advantages of RBAC for EHR Security

- **Streamlined Permission Management:** RBAC significantly reduces the complexity of assigning permissions on an individual basis, especially in large healthcare systems with thousands of employees (Thomas & Sandhu, 1997) [15].
- **Regulatory Compliance:** With robust audit trails and clear delineation of user privileges, RBAC can facilitate compliance with regulations such as HIPAA in the United States, GDPR in Europe, and other regional data protection laws (Kraemer & Carayon, 2017) [9].
- **Scalability:** As healthcare organisations grow or merge, RBAC can scale more easily than discretionary access control (DAC), since new employees are simply assigned to existing roles with pre-defined privileges (Alhaqbani & Fidge, 2008) [1].
- **Enhanced Accountability:** By tying actions to specific roles and logging all user activity, it becomes easier to investigate breaches or unauthorised access incidents (Hu *et al*., 2012) [6].

4. Limitations and Challenges of RBAC

- **Role Explosion:** In some organisations, the number of roles can proliferate to unmanageable levels, undermining the very simplicity RBAC aims to achieve (Cram *et al*., 2016) [4]. This occurs when highly specialised roles are created for niche tasks, resulting in an administrative burden.
- **Dynamic Role Requirements:** Healthcare environments are inherently dynamic. Staff rotations, temporary assignments, and emergency scenarios can make rigid role definitions difficult to maintain (Lai *et al*., 2019) [12].
- **Contextual Access Needs:** A purely role-based model may not adequately capture context, such as time-bound access for emergency care or location-based restrictions. Some researchers have proposed context-aware RBAC models to address these limitations (Zhang *et al*., 2019) [17].
- **Lack of Organisational Support:** Effective RBAC implementation requires robust organisational policies, ongoing training, and executive buy-in. Without these, even the best technical framework may fail in practice (Kraemer & Carayon, 2017) [9].

Emerging Trends and Extensions of RBAC

Attribute-Based Access Control (ABAC)

An emerging approach that often competes or complements RBAC is Attribute-Based Access Control (ABAC). In ABAC, permissions are granted based on attributes such as user characteristics, resource types, and environmental conditions (Hu *et al*., 2015) [7]. This model can offer more flexibility but may also be more complex to implement and maintain.

Context-Aware and Risk-Adaptive RBAC

Researchers are increasingly exploring how RBAC can be adapted to account for situational factors. For example, a risk-adaptive RBAC model might grant elevated privileges to a user in an emergency context but restrict them otherwise (Ni *et al*., 2021) [13]. This ensures that healthcare providers can quickly respond to urgent situations without compromising overall data security.

Blockchain Integration

Blockchain technology has been proposed as a potential solution for decentralised access management. In theory, blockchain could store access policies and transaction logs, ensuring transparency and tamper resistance (Kuo *et al*., 2017) [11]. However, practical adoption in healthcare is still in its early stages, with scalability and regulatory compliance posing significant challenges.

Regulatory Considerations

The handling of patient data is heavily regulated worldwide. In the UK and Europe, the General Data Protection Regulation (GDPR) mandates strict guidelines for data processing, consent, and breach notification. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) outlines rules for patient privacy and security. RBAC implementations must align with these regulations by ensuring only authorised personnel can access patient data and that audit logs are maintained for compliance purposes (Wiederhold *et al*., 2019) [16]. Failure to comply can result in substantial fines and damage to organisational reputation.

Research Gaps

While RBAC is well-established, several gaps remain in the literature:

- **Empirical Evaluations:** Many studies discuss RBAC conceptually, but fewer offer detailed empirical evaluations of its performance in real-world healthcare settings (Cram *et al*., 2016) [4].
- **Longitudinal Studies:** The long-term sustainability and effectiveness of RBAC implementations are under-researched, particularly in large-scale healthcare networks (Ni *et al*., 2021) [13].
- **Integration with Emerging Technologies:** As telemedicine, Internet of Medical Things (IoMT), and AI-driven diagnostics grow, the adaptability of RBAC to these new paradigms requires further investigation (Kuo *et al*., 2017) [11].

This review highlights that while RBAC remains a cornerstone for securing EHRs, it must evolve to address dynamic healthcare contexts and emerging technologies. The following sections outline the methodology and empirical findings of this study, which aims to contribute to the ongoing discourse by providing a detailed, data-driven assessment of RBAC's efficacy and proposing practical improvements.

Materials and Methods

1. Research Design

A mixed-methods approach was employed to capture both quantitative and qualitative perspectives on RBAC implementation in healthcare. This design aimed to provide a more comprehensive understanding of the strengths, weaknesses, and contextual factors influencing RBAC efficacy.

1. **Literature Review:** A systematic review of academic databases (e.g., PubMed, IEEE Xplore, ScienceDirect) was conducted to identify existing research on RBAC in healthcare. Keywords included "RBAC," "Role-Based Access Control," "Electronic Health Records," and "Healthcare Security."
2. **Surveys:** A structured survey was distributed to 150 healthcare IT professionals across hospitals, clinics, and research institutions in the UK. The survey contained Likert-scale and open-ended questions focusing on RBAC usage, perceived benefits, and encountered challenges.
3. **Interviews:** Semi-structured interviews were conducted with 20 participants, including hospital administrators, data protection officers, and healthcare security consultants. Interviews aimed to delve deeper into issues uncovered by the survey and to gather real-life experiences and case studies.
4. **Document Analysis:** Organisational policies, role definitions, and access control logs from three participating hospitals were analysed to cross-verify self-reported practices and identify any discrepancies.

2. Sampling Strategy

- **Survey Participants:** Convenience sampling was used initially, reaching out to professional networks of healthcare IT staff. This was followed by snowball sampling, where participants were asked to recommend colleagues. Efforts were made to include a diverse range of institutions, from small private clinics to large public hospitals.
- **Interview Participants:** Purposive sampling was employed to ensure that interviewees represented various roles: IT managers, chief information officers, data protection officers, and frontline clinical staff.

3. Data Collection

- **Survey Administration:** The survey was administered online via a secure platform. Participants were provided with an information sheet and a consent form. Data collection took place over four weeks, and a 62% response rate was achieved (93 out of 150).
- **Interviews:** Interviews were conducted either face-to-face or via secure video conferencing platforms, typically lasting 30–45 minutes. All interviews were recorded with consent and transcribed verbatim.
- **Policy and Log Analysis:** Organisational documents related to role definitions and access protocols were collected in digital form. Access control logs were anonymised and reviewed to identify patterns of usage and any recorded breaches.

4. Data Analysis

- **Quantitative Data:** Survey data were analysed using SPSS (version 28). Descriptive statistics summarised key variables such as the prevalence of RBAC, perceived ease of administration, and satisfaction with security outcomes. Inferential statistics (e.g., chi-square

tests) were conducted to explore relationships between organisational size, type, and RBAC efficacy.
- **Qualitative Data:** Interview transcripts were coded using thematic analysis (Braun & Clarke, 2006) [3]. An initial coding framework was developed based on the research questions and then refined as new themes emerged. The final themes were cross-checked by a second researcher to enhance reliability.
- **Document Analysis:** Organisational policies were examined to see if they aligned with best practices outlined in the literature. Access logs were statistically examined for anomalies, such as frequent access attempts outside standard role boundaries.

Ethical Considerations

Ethical approval was obtained from the relevant institutional review boards before data collection commenced. Participants were informed about the purpose of the study, and confidentiality was maintained by anonymising responses. Any potentially identifying information, particularly from interview transcripts, was removed during transcription. Data were stored in encrypted files, accessible only to the research team.

Limitations of the Methodology
- **Sampling Bias:** Reliance on convenience and snowball sampling may limit the generalisability of findings, although efforts were made to include a diverse range of institutions.
- **Self-Reported Data:** Surveys and interviews are subject to social desirability bias, where respondents may overstate compliance or success. Triangulation with document analysis helped mitigate this issue.
- **Time Constraints:** The cross-sectional nature of this study provides only a snapshot. Longitudinal research would offer deeper insights into how RBAC efficacy evolves over time.

By integrating both quantitative and qualitative data, this study aims to provide a robust evaluation of RBAC's role in protecting EHRs. The subsequent sections detail the results of the survey and interviews, followed by a discussion that synthesises these findings in the context of existing literature.

Results

1. Survey Findings

Out of the 93 respondents:
- **RBAC Adoption:** 81% reported that their organisation had implemented an RBAC system for EHR access. The remaining 19% either used alternative models (like ABAC) or had no formal access control system beyond basic authentication.
- **Perceived Effectiveness:** 72% of RBAC users agreed or strongly agreed that RBAC effectively prevented unauthorised access, while 15% were neutral and 13% disagreed.
- **Administrative Burden:** 56% found RBAC "moderately easy" or "very easy" to administer, whereas 44% cited significant difficulties, particularly when roles needed frequent updates.
- **Training and Awareness:** Only 38% stated that staff received ongoing training about role definitions and data security protocols. Lack of training emerged as a common concern.

A chi-square test revealed a statistically significant relationship ($p<0.05$) between organisation size and perceived administrative burden, suggesting that larger institutions with more complex role structures found RBAC more challenging to maintain.

2. Interview Insights

Thematic analysis of the 20 interviews revealed several recurring themes:
- **Role Clarity:** Many interviewees emphasised that RBAC's success hinged on clearly defined roles. However, in practice, roles often overlapped, and staff members sometimes performed tasks outside their nominal roles.
- **Emergency Overrides:** Clinicians expressed frustration with the rigidity of RBAC, particularly in emergency scenarios where rapid access to patient data was crucial. Some organisations implemented "break-glass" policies, but these were not always well-monitored.
- **Cultural Factors:** Interviewees stressed that a security-conscious culture was as important as technical measures. In organisations where leadership prioritised data protection, RBAC was more consistently applied.
- **Integration Challenges:** Several participants highlighted difficulties integrating RBAC with newer technologies, such as telehealth platforms, which often required separate access control systems.

3. Document and Log Analysis
- **Policy Alignment:** Two of the three hospitals analysed had comprehensive RBAC policies aligned with best practices. The third had outdated documentation, leading to inconsistent role assignments.
- **Access Log Patterns:** Frequent instances of "role creep" were observed, where employees retained privileges from previous roles. Additionally, there were sporadic instances of unauthorised access attempts, though no major breaches were reported.

Table 1: Below provides a concise summary of key findings from the three data collection methods.

Data Collection Method	Key Findings
Survey (n=93)	81% use RBAC; 72% find it effective; 44% face admin burden
Interviews (n=20)	Importance of clear roles, break-glass policies, culture
Document & Log Analysis	Role creep, outdated policies, minimal major breaches

Overall, the results paint a mixed picture of RBAC's effectiveness. While most organisations acknowledged its importance in securing EHRs, real-world implementation challenges, particularly around dynamic roles and cultural adoption, frequently hindered its potential.

Findings and Discussion

1. Alignment with Literature

The results corroborate earlier research indicating that RBAC can significantly enhance data security by offering structured, role-based privileges (Sandhu *et al*., 1996; Kraemer & Carayon, 2017) [14, 9]. The high adoption rate (81%) among surveyed organisations underscores RBAC's perceived value in healthcare. This aligns with literature suggesting that RBAC is often the "go-to" model due to its intuitive mapping of clinical job functions to access privileges (Thomas & Sandhu, 1997) [15].

However, the interviews and document analysis reveal substantial implementation hurdles, echoing the concerns raised by Lai *et al*. (2019) [12] about the dynamic nature of healthcare roles. Role explosion and overlap were particularly prevalent in large institutions, supporting Cram *et al*. (2016) [4], who warn of the administrative burden that can accompany granular role definitions.

2. Role Definition and Maintenance

A critical insight is that effective RBAC depends on meticulously defining roles, responsibilities, and associated privileges. While many surveyed organisations had RBAC policies, the interviews revealed that these policies were not always updated to reflect staff changes or departmental reorganisation. This finding aligns with the concept of "role creep," where employees accumulate privileges from previous roles, potentially leading to security vulnerabilities (Ni *et al*., 2021) [13].

Implication: Organisations need a clear governance structure to periodically review and update role definitions. Automated tools that alert administrators to potential role conflicts or unnecessary privileges could help mitigate role creep.

3. Emergency Scenarios and Break-Glass Policies

The interviews highlighted the tension between security and accessibility in emergency contexts. Clinicians sometimes felt that RBAC impeded patient care by restricting quick data access. Although "break-glass" mechanisms were in place at several institutions, these were not uniformly monitored, raising the risk of misuse (Lai *et al*., 2019) [12].

Implication: A well-defined, audited break-glass policy is essential. Technology solutions could include automated logging and real-time alerts whenever emergency privileges are invoked, ensuring accountability and post-event review.

4. Organisational Culture and Training

A recurring theme was the importance of organisational culture. Where leadership emphasised data security and provided regular training, RBAC was more effectively implemented and adhered to. Conversely, in institutions where security was seen as a low priority, staff often circumvented controls or failed to follow protocols.

Implication: Technical solutions like RBAC can only be as effective as the people managing and using them. Regular training, clear communication, and leadership commitment are vital for fostering a security-oriented culture (Kraemer & Carayon, 2017) [9].

5. Integration with Emerging Technologies

Many respondents noted the difficulty of integrating RBAC with newer technologies such as telemedicine platforms and mobile health applications. Some telehealth solutions used proprietary access control systems that did not easily map onto existing RBAC frameworks. This challenge reflects broader concerns about the interoperability of healthcare systems (Kuo *et al*., 2017) [11].

Implication: As healthcare continues to digitise, RBAC must evolve to support a broader range of devices and platforms. Future research should explore hybrid models that combine RBAC with other approaches like ABAC or blockchain-based solutions, enabling more flexible and context-aware access control.

6. Recommendations for Strengthening RBAC

Based on the study's findings, the following recommendations are proposed:

1. **Dynamic Role Assignment:** Incorporate real-time context into role assignment. For instance, a nurse in the emergency department might temporarily gain elevated privileges during a specific shift, automatically reverting to a standard level of access afterward.
2. **Regular Audits and Role Reviews:** Implement quarterly or semi-annual reviews of role definitions and user privileges. This process can be supported by automated scripts that flag anomalies, such as roles with overlapping privileges or users retaining old permissions.
3. **Comprehensive Training:** Provide mandatory training sessions for all staff, focusing on the rationale behind RBAC, how to use the system properly, and the consequences of data breaches.
4. **Robust Break-Glass Mechanisms:** Develop well-defined emergency override procedures, coupled with automated monitoring and real-time alerts to ensure accountability.
5. **Integration Frameworks:** Encourage vendors of telemedicine and mobile health platforms to adopt standardised access control protocols, facilitating easier integration with existing RBAC systems.
6. **Policy and Cultural Reinforcement:** Leadership should consistently emphasise the importance of data security, ensuring that it is embedded in organisational values and daily practices.

7. Theoretical and Practical Implications

- **Theoretical:** The study enriches the academic discourse by providing empirical data on RBAC's real-world efficacy. It supports the argument that RBAC alone may not suffice in rapidly evolving healthcare contexts, suggesting the need for adaptive or hybrid models (Ni *et al*., 2021).
- **Practical:** Healthcare administrators can leverage these findings to refine existing RBAC frameworks. The recommendations serve as actionable steps that can be customised to organisational size, culture, and technological maturity.

8. Limitations and Future Research

- **Cross-Sectional Nature:** The study offers only a

snapshot of current RBAC implementations. Longitudinal research could track how RBAC evolves over time and in response to organisational changes.
- **Geographical Scope:** While the focus on UK healthcare institutions provides valuable insights, the findings may not be fully generalisable to other regions with different regulatory landscapes.
- **Technological Advances:** As new technologies like AI-driven diagnostics and advanced IoT devices proliferate, future studies should investigate how RBAC can adapt to these emerging paradigms (Kulkarni *et al*., 2020) [10].

In summary, RBAC remains a cornerstone for securing EHRs, but its success hinges on careful role definition, ongoing maintenance, and a supportive organisational culture. With healthcare undergoing rapid digital transformation, there is a pressing need to evolve RBAC frameworks to be more dynamic, context-aware, and integrated with emerging technologies.

Conclusion

This study set out to evaluate the effectiveness of Role-Based Access Control (RBAC) for protecting electronic health records in modern healthcare settings. The findings, drawn from surveys, interviews, and document analysis, reveal that RBAC can substantially improve data security by providing a structured framework for assigning and managing user privileges. However, the research also highlights persistent challenges, including role explosion, dynamic role requirements, and difficulties in integrating RBAC with emerging telehealth and mobile technologies.

A key takeaway is that successful RBAC implementation is not solely a technical endeavour. Organisational culture, leadership commitment, and continuous training play equally important roles in ensuring that staff adhere to access policies and understand the rationale behind them. Where such elements are lacking, even well-designed RBAC systems may fail to achieve their intended outcomes. Moreover, emergency scenarios demand flexible yet secure override mechanisms, underscoring the need for break-glass policies that balance urgent access with accountability.

The recommendations provided-ranging from dynamic role assignment to regular audits-offer practical guidance for healthcare administrators seeking to fortify their RBAC frameworks. As healthcare continues to evolve, future research should explore adaptive or hybrid models that can respond to the complexities of telemedicine, IoT devices, and AI-driven diagnostics. In doing so, RBAC can remain a vital component of healthcare security, ensuring that sensitive patient information is accessed appropriately and responsibly.

Ultimately, by strengthening RBAC implementations and addressing the challenges identified in this study, healthcare organisations can better protect patient privacy, maintain regulatory compliance, and uphold public trust in the digitised healthcare landscape.

References

1. Alhaqbani B, Fidge C. Access control requirements for processing electronic health records. In: Proceedings of the 5th Australasian Workshop on Grid Computing and e-Research (AusGrid 2008), Wollongong, Australia; c2008. p. 23-32.
2. Alotaibi YK, Federico F. The impact of health information technology on patient safety. Saudi Medical Journal. 2017;38(12):1173-1180.
3. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;3(2):77–101.
4. Cram WA, Proudfoot JG, D'Arcy J. Organizational information security policies: a review and research framework. European Journal of Information Systems. 2016;25(6):605-641.
5. Ferraiolo DF, Kuhn R, Chandramouli R. Role-based access control (RBAC): Features and motivations. In: Proceedings of the 11th Annual Computer Security Applications Conference, New Orleans, LA; c1995. p. 241-248.
6. Hu VC, Ferraiolo DF, Kuhn R, Schnitzer A, Sandlin K, Miller R, *et al*. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. NIST Special Publication 800-162. Gaithersburg: National Institute of Standards and Technology; c2012.
7. Hu VC, Kuhn R, Ferraiolo DF. Attribute-based access control. Computer. 2015;48(2):85-88.
8. Johnson ME, Stoudemire S, Gofman M. Comparing role-based and attribute-based access control in healthcare and finance. Journal of Information Privacy and Security. 2018;14(1):3-18.
9. Kraemer S, Carayon P. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technology and Health Care. 2017;25(6):1-10.
10. Kulkarni S, Smith A, Martin T. Leveraging artificial intelligence to enhance healthcare data security. BMC Medical Informatics and Decision Making. 2020;20(1):278.
11. Kuo TT, Kim HE, Ohno-Machado L. Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association. 2017;24(6):1211-1220.
12. Lai AM, Ramesh A, Mahan M, Chokshi SK. Improving the impact of health information technology implementation: a qualitative study. BMJ Open. 2019;9(9):e030528.
13. Ni Q, Lin D, Bertino E. Privacy-aware role-based access control. ACM Transactions on Information and System Security. 2021;24(3):16.
14. Sandhu R, Coyne E, Feinstein H, Youman C. Role-based access control models. Computer. 1996;29(2):38-47.
15. Thomas R, Sandhu R. Task-based authorization controls (TBAC): A family of models for active and enterprise-oriented authorization management. In: Database Security XI: Status and Prospects. Boston: Springer; c1997. p. 166-181.
16. Wiederhold G, Gupta A, Memon N. Challenges in ensuring cybersecurity for healthcare: the case for a new regulatory framework. Health Affairs. 2019;38(11):1840-1847.
17. Zhang L, Yu H, Chen D. Context-aware access control model for patient healthcare monitoring in smart homes. Sensors. 2019;19(2):276.

18. Johnson C, Jones A. A study on the evolution of healthcare data security in the digital era. Health Informatics Journal. 2020;26(3):1612-1625.
19. Brown T, O'Sullivan M, Anderson P. Evaluating the role of RBAC in hospital data protection: a multi-case study. International Journal of Medical Informatics. 2021;152:104479.
20. Smith G, Johnson D. Enhancing RBAC with dynamic contextual rules in emergency medicine. Journal of Healthcare Engineering. 2021;2021:8812539.
21. Lee H, Park E, Kim J. Healthcare data breach trends and implications for hospital security policies. Journal of Medical Internet Research. 2022;24(4):e30834.
22. Miller T, Roberts A. Telemedicine expansion and the implications for RBAC: a survey of US hospitals. Telemedicine and e-Health. 2022;28(7):977-984.
23. Ahmad A, Maynard SB, Shanks G. A case analysis of information systems and security incident responses. International Journal of Information Management. 2015;35(6):717-723.
24. Martin KE, Nissenbaum H. Privacy interests in public records: An empirical investigation. Harvard Journal of Law & Technology. 2017;31(1):111-167.
25. ISO/IEC. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: International Organization for Standardization; c2022.
26. NIST. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53 Rev. 5. Gaithersburg: National Institute of Standards and Technology; c2020.
27. Office for National Statistics. Cyber security breaches survey. London: UK Government; c2021.
28. Eze E, Gleasure R, Heavin C. Exploiting the digital patient experience: a critical analysis of telehealth. Information Systems Frontiers. 2020;22(2):247-266.
29. NHS Digital. Data Security and Protection Toolkit: Guidance for Healthcare Providers. London: Department of Health and Social Care; c2023.
30. Park J, Park Y. Comparative analysis of RBAC and ABAC in cloud-based EHR systems. Computers & Security. 2023;123:102959.