impact International Journals and Publications

© IIJP 2026 | Volume 2, Issue 3, pp. 1972-1983 | ISSN: 2636-4484

ASSESSMENT OF ROLE-BASED ACCESS CONTROL FOR ELECTRONIC HEALTH RECORDS AT UNIVERSITY OF PORT HARCOURT TEACHING HOSPITAL

***Idimie T. Ayaowei[1], Wagbara Evelyn[2], Kurokeyi E.J. Teddy[3], Nwankwo B. Chidinma[4], Amos K. Omietimi[5] & Mamman S. Safinatu[6]**

[1&3]Department of Health Information Management, Bayelsa Medical University, Yenagoa, Bayelsa State

[2]Department of Health Information Management, University of Port Harcourt Teaching Hospital, Rivers State.

[4]Department Health Care Administration & Hospital Management, Bayelsa Medical University, Yenagoa. Bayelsa State, Nigeria.

[5]Department of Medical Social Works, Bayelsa Medical University, Yenagoa

[6]Department of Health Information Management, School of Allied Medical Sciences, Bayelsa State College of Technology, Otuogidi Ogbia

****Corresponding author:** idimie.ayaowei@bmu.ed.ng*

ARTICLE INFO
Article No.: 0563
Accepted Date: 17/08/2026
Published Date: 11/09/2026
Type: Research

ABSTRACT

This study investigates Assessment Access Control for Electronic Health Records (EHRs) at the University of Port Harcourt Teaching Hospital (UPTH), Rivers State, South South, Nigeria. Amidst a critical transition from paper-based to digital records, the absence of a formal access control framework presents significant risks to patient confidentiality and institutional compliance. The research employed a quantitative, descriptive cross-sectional survey design, collecting data from 156 clinical and administrative staff through a structured questionnaire. The analysis aimed to evaluate existing access mechanisms. The findings reveal a generally negative perception of the existing access control mechanisms. A majority of respondents disagreed or strongly disagreed (64.7%, n=101) with a low mean score of 2.18 (SD=1.09), with 54.5% (n=85) of staff disagreeing or strongly disagreeing that the current system provides adequate protection, reflected in a mean score of 2.41 (SD=1.13). Staff perceived the technical infrastructure as inadequate to support an advanced system. The ability to audit who has accessed a patient's record was also perceived as weak, as 70.5% (n=110) disagreed or strongly disagreed that this was easy to determine (Mean=2.01, SD=1.02). Similarly, financial and human resources were deemed insufficient, with particularly low confidence in funding and user training provisions and administrative processes were also poor. The study concludes that, its practical implementation is contingent upon substantial and strategic investment in the hospital's foundational infrastructure and organisational resources. This research provides an evidence-based roadmap for UPTH and a valuable framework for other healthcare institutions in similar contexts navigating the complexities of secure EHR adoption.

Keywords*:* Role−Based Access Control System, Electronic Health Records, University of Port Harcourt Teaching Hospital..

© IIJP 2026 | Volume 2, Issue 3, pp. 1972-1983 | ISSN: 2636-4484

Introduction

The global system for Electronic Health Records (HER) adoption has been driven by a confluence of factors, including governmental policy, technological advancement, and a growing recognition of the system-wide benefits. In developed nations, landmark initiatives like the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 in the United States catalysed a rapid and widespread migration from paper to digital systems, incentivising healthcare providers to adopt and demonstrate 'meaningful use' of certified EHR technology (Blumenthal & Tavenner, 2010). The promised advantages were manifold: enhanced care coordination through seamless information exchange, a reduction in medical errors stemming from illegible prescriptions or incomplete histories, improved chronic disease management, and the creation of vast data repositories to fuel clinical research and public health surveillance (Jha et al., 2009). Indeed, the capacity of EHRs to aggregate longitudinal data has unlocked new frontiers in population health management and evidence-based practice, transforming the scale at which medical knowledge can be generated and applied (Classen et al., 2020). This digital transformation, however, casts a long shadow, for with the immense power to collect and disseminate data comes an equally immense responsibility to protect it. The very attributes that make EHRs powerful—their accessibility, interoperability, and persistence—also render them uniquely vulnerable. Unlike a paper file locked in a cabinet, an electronic record can be copied, transmitted, and accessed from multiple points, often simultaneously, creating an expanded threat surface (Keshta & Odeh, 2021). The information contained within an EHR is among the most sensitive personal data imaginable, encompassing not only medical diagnoses and treatments but also genetic information, psychiatric notes, and lifestyle details. The unauthorised disclosure of such information can lead to profound personal consequences, including discrimination, social stigma, and emotional distress (Fernández-Alemán *et al*., 2013).

The shortcomings of these traditional models highlighted the need for a more sophisticated approach, one that could mirror the functional structure of a healthcare organisation. This need gave rise to Role-Based Access Control (RBAC), a model first formalised in the 1990s and subsequently standardised by the US National Institute of Standards and Technology (NIST) (Sandhu et al., 2000; Ferraiolo et al., 2001). The genius of RBAC lies in its elegant decoupling of users from permissions. Instead of assigning permissions directly to individuals, permissions are assigned to abstract 'roles' that correspond to specific job functions (e.g., 'Physician', 'Nurse', 'Pharmacist', 'Billing Clerk'). Users are then assigned to one or more of these roles. A user's effective permissions at any given time are the sum of the permissions associated with their assigned role(s) (Manor, 2024). This structure offers profound advantages for a healthcare setting. It naturally enforces the principle of least privilege, simplifies administration (as managing role memberships is far easier than managing thousands of individual permission sets), and provides a robust framework for implementing critical security policies like the separation of duties, which prevents a single individual from performing conflicting actions, such as both prescribing and dispensing a controlled substance (Nyame & Qin, 2020). Because of its scalability, administrative efficiency, and alignment with organisational structures, RBAC has emerged as the de facto industry standard for managing access to enterprise systems, including EHRs (Carvalho Junior & Bandiera-Paiva, 2018).The privacy of patient information is a deeply held cultural and ethical value, and any perception that a new electronic system might compromise this confidentiality could severely undermine its adoption and effectiveness (Alshahrani et al., 2021).

Therefore, as Nigerian teaching hospitals stand on the precipice of this digital transformation, the question of access control moves from a theoretical concern to an immediate and practical imperative.

Statement of the Problem

The core problem this research addresses is the profound risk posed by the absence of a formal, structured, and enforceable access control framework for the hospital's emerging EHR environment. The University of Port Harcourt Teaching Hospital (UPTH) stands as a vital healthcare institution in Nigeria's Niger Delta region, serving as a primary referral centre for a vast and diverse population. With numerous specialised departments, a large cadre of multidisciplinary staff, and a high volume of patient encounters, the hospital's information management systems are central to its mission of providing quality care, training, and research. Historically, UPTH, like many of its counterparts in Nigeria, has relied heavily on a paper-based system for patient records. This legacy system, while familiar, is beset by systemic inefficiencies and security vulnerabilities. Records are frequently misplaced, become illegible over time, or are difficult to retrieve in a timely manner, particularly during emergencies, directly impacting the quality and continuity of patient care (Solvang *et al.,* 2024). From a security perspective, the physical folders offer minimal protection; they lack robust audit trails, making it nearly impossible to track who has accessed a patient's information, and are susceptible to unauthorised viewing, theft, or damage. In response to these challenges and in alignment with national e-health objectives, UPTH is navigating the critical transition towards a comprehensive Electronic Health Record (EHR) system. This transition represents a significant step towards modernising healthcare delivery, but it simultaneously introduces a new and formidable set of challenges related to information security. The core problem this research addresses is the profound risk posed by the absence of a formal, structured, and enforceable access control framework for the hospital's emerging EHR environment. Without such a framework, the default state is often one of overly permissive access, where any authenticated user can potentially view, alter, or extract any patient's record, regardless of their professional role or legitimate need-to-know. This situation creates a security vacuum that manifests in several critical and interconnected problems.

First, there is an acute and immediate threat to patient privacy and confidentiality. In an environment with ill-defined access controls, a billing clerk could potentially access a patient's sensitive psychiatric notes, or a laboratory technician could view the HIV status of a colleague. Such breaches violate the fundamental ethical duty of confidentiality owed to every patient and can cause irreparable harm, including social stigmatisation and discrimination (Tertulino et al., 2023). This risk is amplified by the significant threat posed by insiders—be they malicious actors seeking to exploit data for personal gain or simply curious employees—who can abuse their legitimate access privileges in ways that are difficult to detect in an unstructured system (Marquis, 2024). Also, there is lack of a robust access control system exposes UPTH to significant legal and regulatory jeopardy. The purpose of the study specifically determines staff perceptions of the existing access control mechanisms for Electronic Health Records in University of Port Harcourt Teaching Hospital (UPTH). The study provide answer to the following research question: What are the existing access control mechanisms for Electronic Health Records (EHRs) in UPTH South-South, Nigeria?

Literature Review

While the provided literature does not contain studies conducted specifically at the University of Port Harcourt Teaching Hospital (UPTH), it offers robust evaluations of access control mechanisms in comparable healthcare settings. These findings establish a valuable

framework for assessing the potential state and challenges of access control at UPTH. By examining the methodologies and outcomes of these general studies, it is possible to infer the key criteria, common failings, and alternative models that would be pertinent to an evaluation at the hospital.

A pivotal study by Helms and Williams (2011) provides a direct model for such an evaluation. The researchers aimed to assess the state of practice in EHR access control by examining four open-source EHR systems against a robust set of 25 criteria derived from the Health Insurance Portability and Accountability Act (HIPAA), meaningful use certification requirements, and National Institute of Standards and Technology (NIST) best practices. Their methodology involved a criteria-based evaluation of each system's access control features. The findings were stark, revealing significant deficiencies in the implementation of established security principles. Critically, the study demonstrated that all four EHR systems failed to properly implement a separation of duties (SoD) component, a fundamental principle for preventing fraud and error. Furthermore, two of the systems did not utilise the best practice of 'permission-role review', which is essential for maintaining and auditing access rights. The conclusion drawn was that open-source EHR system designers were not implementing robust access control mechanisms, leaving patient data inadequately protected. This study's methodology and criteria offer a direct blueprint for evaluating the existing mechanisms at UPTH, while its findings highlight that a failure to enforce core principles like SoD is a common vulnerability that should be a primary focus of any internal assessment.

Expanding on the evaluation of specific mechanisms, a formal analysis by Carvalho Junior and Bandiera-Paiva (2021) investigated the security implications of different interpretations of the RBAC standard's session control function (RC-16). Their research sought to highlight how a loosened implementation of this function could undermine the enforcement of Dynamic Mutually Exclusive Roles (DMER), a key feature for maintaining SoD. The study employed a rigorous formal methods approach, using Z notation for formal description and Coloured Petri Nets (CPN) for simulation and analysis of system behaviour under two different interpretations of the standard. The findings demonstrated that a relaxed interpretation, which allows a user to select a subset of their assigned roles to activate within a session, could enable a user to circumvent DMER constraints by activating non-conflicting roles one at a time across different sessions. The authors concluded that such a loosened implementation creates a significant security vulnerability, potentially allowing corporate security policies to be broken and enabling collusion or fraud. For an evaluation at UPTH, this study underscores the importance of not just verifying the presence of an access control feature, but meticulously examining its implementation logic to ensure it robustly enforces security policies as intended, especially concerning dynamic session management and SoD.

A systematic literature review conducted by Cobrado et al. (2024) offers a broader evaluation of the access control landscape, synthesising findings from 20 journal articles to categorise solutions according to the Identification, Authentication, Authorization, and Accountability (IAAA) framework. The study aimed to analyse existing access control solutions for EHRs and identify prominent research gaps. Using the 2020 PRISMA guidelines, the researchers analysed methodologies across the IAAA spectrum. A significant finding was the prominence of Attribute-Based Access Control (ABAC) as the most popular authorisation mechanism in the reviewed literature, suggesting a trend away from simpler RBAC models towards more flexible and granular control. The analysis revealed that unique IDs were the most common identification method (used in 12 studies), digital signatures were a frequent

authentication method (10 studies), and access control logs were the primary accountability mechanism (2 studies). The study concluded that major gaps exist in current implementations, including a lack of multi-factor authentication, inadequate emergency access protocols, and insufficient accountability mechanisms. This research provides a structured IAAA framework that UPTH could use to evaluate its own systems, suggesting that an effective evaluation must assess the maturity of mechanisms across all four IAAA categories and consider whether more dynamic models like ABAC might be better suited to its needs than traditional RBAC alone.

Furthering the evaluation by comparing different models, Atlam et al, (2025) presents a conceptual showdown between RBAC, ABAC, and Relationship-Based Access Control (ReBAC). The aim was to delineate the use cases, strengths, and weaknesses of each model to guide developers in choosing the appropriate framework. The analysis characterised RBAC as simple and scalable but prone to 'role explosion' and lacking flexibility for granular requirements. In contrast, ABAC was presented as highly dynamic and capable of fine-grained control by using attributes of users, resources, and the environment, though its implementation is more complex and resource-intensive. ReBAC was highlighted for its unique strength in managing complex hierarchies and nested relationships, such as defining that a user who owns a folder also owns all files within it. Atlam et al, (2025) concluded that no single model is universally superior and that many modern applications benefit from a hybrid approach, often starting with RBAC and evolving to incorporate ABAC or ReBAC as complexity grows. For UPTH, this evaluation is critical; it suggests that assessing its current system should involve determining where the limitations of its existing model lie and whether the institution's complex hierarchical and contextual access needs might be better served by ABAC, ReBAC, or a hybrid model.

The foundational work of Sandhu et al. (1996) provides a structured framework for evaluating the sophistication of any RBAC implementation. The authors aimed to systematically categorise the diverse components of RBAC by proposing a family of four reference models. The methodology involved defining a conceptual framework progressing in complexity: RBAC0 (the base model with users, roles, permissions, and sessions), RBAC1 (which adds role hierarchies), RBAC2 (which adds constraints like separation of duties), and RBAC3 (which consolidates both hierarchies and constraints). This framework establishes that true RBAC is more than just grouping users; it involves centrally managed relationships between users, roles, and permissions, and can support advanced principles like least privilege and SoD. The authors concluded that this family of models provides a clear reference for comparing and evaluating different systems. This work is directly relevant for UPTH, as it provides a standardised benchmark. An evaluation of the hospital's current system could determine where it falls on this spectrum, for instance, whether it is a simple RBAC0 implementation or if it supports more advanced features like hierarchies (RBAC1) and constraints (RBAC2), which are critical for a complex healthcare environment.

Finally, a systematic review by Kruse et al. (2017) categorises security techniques for EHRs into three safeguard themes derived from HIPAA: administrative, physical, and technical. The study's objective was to analyse and discuss prominent security techniques to establish a foundation for further research. By reviewing 25 articles from databases like PubMed and CINAHL, the researchers synthesised observations into these three categories. Administrative safeguards included policies, risk assessments, and training. Physical safeguards involved controlling physical access to hardware like servers and workstations. Technical safeguards, the most frequently mentioned category (45% of occurrences), included firewalls, cryptography, and access controls like RBAC. The authors concluded that a multi-layered approach incorporating robust techniques across all three themes is imperative for securing EHRs. This framework implies

that a thorough evaluation of access control at UPTH cannot be conducted in isolation. It must be part of a holistic assessment that examines how technical controls like RBAC are supported by, and integrated with, the hospital's administrative policies and physical security measures to ensure comprehensive protection of patient information. By weaving these theoretical threads together, the study can produce a richer and more holistic analysis. The literature confirms that while RBAC is a mature and preferred model (de Carvalho Junior & Bandiera-Paiva, 2018), its successful introduction is less about the model itself and more about the meticulous, context-sensitive, and theoretically informed process of its implementation. This process is precisely what the current research sets out to define and facilitate for the University of Port Harcourt Teaching Hospital.

Research Methodology

A quantitative, descriptive cross-sectional survey design. It was precisely a study aimed to capture: the current state of access control mechanisms, the existing technical infrastructure, enforceable access control framework for the hospital's emerging EHR environment. In this study, data were collected from all full-time clinical and administrative staff employed at the University of Port Harcourt Teaching Hospital who had direct or indirect interaction with patient health records. The target population comprised full-time clinical and administrative staff employed in UPTH, totalling to 4,500 individuals. A multi-stage sampling technique was employed in this study, this included all health information personnel - medical doctors, nurses, and pharmacists, and administrative staff of the hospital, (Source: Staff Nominal Roll in each of the hospitals, 2023), and a sample size of 170 was determined using the Cochran's formula for large populations. Therefore, out the 170-sample size, questionnaires were sent out for data collection and 156 questionnaires were retrieved and used for the study. Content validity was ensured through a multi-faceted process. The initial draft of the questionnaire was subjected to a comprehensive review by a panel of five experts, comprising two senior health information management professionals from UPTH, one senior IT administrator from the hospital, and two academics with expertise in health informatics and research methodology. The primary method for assessing reliability was to evaluate the instrument's internal consistency. This was achieved by calculating Cronbach's alpha coefficient for the Likert-scaled sections of the questionnaire (e.g., the TAM constructs and factor perception scales). The calculation was first performed on the data collected during the pre-testing phase. The instrument was considered to have acceptable reliability if the Cronbach's alpha value was 0.70 or higher, a widely accepted threshold in social science research. The ethical integrity of this research was a foundational priority, and a comprehensive protocol was followed to safeguard the rights, dignity, and welfare of all participants. The cornerstone of this protocol was the acquisition of formal ethical approval from the University of Port Harcourt Teaching Hospital's Institutional Review Board (IRB) before any research activities commenced. This external review ensured the study complied with all national and institutional guidelines for research involving human subjects. Beyond this formal approval, several key ethical principles were meticulously observed throughout the research process. Informed consent was treated not as a mere formality but as an ongoing process of communication. Every potential participant was provided with a detailed information sheet, written in clear and accessible English, outlining the study's purpose, the nature of their involvement, potential (though minimal) risks, and the benefits of the research. It explicitly stated that participation was entirely voluntary and that they had the right to withdraw at any time without any negative consequences to their employment or professional standing. Written consent was obtained on a separate form before the questionnaire was administered

Results

© IIJP 2026 | Volume 2, Issue 3, pp. 1972-1983 | ISSN: 2636-4484

Research Question One: What are the existing access control mechanisms for Electronic Health Records (EHRs) in UPTH South-South, Nigeria?

Table 1: Staff Perceptions of Existing Access Control Mechanisms (N=156)

Statement	SD	D	N	A	SA	Mean	SD
1. The current system is efficient and saves time.	41 (26.3)	60 (38.5)	31 (19.9)	20 (12.8)	4 (2.6)	2.18	1.09
2. The current system adequately protects patient confidentiality.	35 (22.4)	50 (32.1)	38 (24.4)	29 (18.6)	4 (2.6)	2.41	1.13
3. It is easy to determine who has accessed a patient's record.	55 (35.3)	55 (35.3)	29 (18.6)	14 (9.0)	3 (1.9)	2.01	1.02
4. The process for granting access to new staff is straightforward.	32 (20.5)	57 (36.5)	35 (22.4)	28 (17.9)	4 (2.6)	2.39	1.11
5. I am confident that only authorized individuals can access sensitive information.	42 (26.9)	54 (34.6)	29 (18.6)	25 (16.0)	6 (3.8)	2.27	1.15
6. The current system clearly defines what information different staff can see.	38 (24.4)	55 (35.3)	36 (23.1)	23 (14.7)	4 (2.6)	2.33	1.08
7. Accessing records from different departments is a seamless process.	63 (40.4)	51 (32.7)	24 (15.4)	15 (9.6)	3 (1.9)	1.95	0.99
8. Revoking access for staff who have left or changed roles is done promptly.	21 (13.5)	44 (28.2)	59 (37.8)	25 (16.0)	7 (4.5)	2.63	1.06
9. The risk of unauthorized personnel viewing patient records is low.	40 (25.6)	54 (34.6)	31 (19.9)	26 (16.7)	5 (3.2)	2.29	1.12
10. The current system creates significant administrative work.	5 (3.2)	14 (9.0)	25 (16.0)	78 (50.0)	34 (21.8)	3.89	1.05
11. I frequently encounter difficulties when trying to access patient information.	6 (3.8)	18 (11.5)	30 (19.2)	71 (45.5)	31 (19.9)	3.76	1.10
12. Overall, I am satisfied with the security and access control features.	60 (38.5)	52 (33.3)	25 (16.0)	16 (10.3)	3 (1.9)	1.98	1.04

This objective was addressed by assessing staff perceptions of the current system for accessing patient records. Respondents rated their level of agreement with twelve statements on a five-point Likert scale, ranging from 'Strongly Disagree' to 'Strongly Agree'. The descriptive statistics for these items, including frequencies, percentages, mean, and standard deviation, are presented in Table 1.

The findings reveal a generally negative perception of the existing access control mechanisms. For the statement regarding efficiency and time-saving (1), a majority of respondents disagreed or strongly disagreed (64.7%, n=101), with a low mean score of 2.18 (SD=1.09). Similarly, there were significant concerns about patient confidentiality (2), with 54.5% (n=85) of staff disagreeing or strongly disagreeing that the current system provides adequate protection, reflected in a mean score of 2.41 (SD=1.13). The ability to audit who has accessed a patient's record was also perceived as weak (3), as 70.5% (n=110) disagreed or strongly disagreed that this was easy to determine (Mean=2.01, SD=1.02).

Perceptions of administrative processes were also poor. The process for granting access to new staff members (4) was not considered straightforward by 57.0% (n=89) of respondents (Mean=2.39, SD=1.11). Confidence that only authorised individuals can access sensitive patient information was low (5), with 61.5% (n=96) expressing disagreement or strong disagreement (Mean=2.27, SD=1.15). The system's ability to clearly define what information different staff can see (6) was also rated negatively by a majority (59.6%, n=93), yielding a mean score of 2.33 (SD=1.08). Accessing records across different departments was not seen as a seamless process (7), with a substantial 73.1% (n=114) disagreeing or strongly disagreeing (Mean=1.95, SD=0.99).

On the issue of revoking access for staff who have left or changed roles (8), respondents were divided, though leaning towards negative. While 37.8% (n=59) were neutral, 41.7% (n=65) disagreed or strongly disagreed that this was done promptly (Mean=2.63, SD=1.06). Staff perceived the risk of unauthorised viewing of patient records as high, with 60.2% (n=94) disagreeing with the statement that the risk is low (9), resulting in a mean of 2.29 (SD=1.12).

For the reverse-coded items, the findings further support the overall dissatisfaction. A large majority (71.8%, n=112) agreed or strongly agreed that the current system creates significant administrative work (10), with a high mean of 3.89 (SD=1.05). Furthermore, 65.4% (n=102) of staff reported that they frequently encounter difficulties when trying to access needed patient information (11), with a corresponding mean of 3.76 (SD=1.10).

Given these widespread negative perceptions, it is unsurprising that the overall satisfaction with the security and access control features of the current system (12) was very low. A combined 71.8% (n=112) of participants disagreed or strongly disagreed that they were satisfied, leading to one of the lowest mean scores of 1.98 (SD=1.04). A composite score for satisfaction with the existing system, created by averaging scores for items 1-9 and 12 (with 10 and 11 reverse-coded), yielded an overall mean of 2.31 (SD=0.88), indicating a general level of dissatisfaction among the staff.

Discussion.

An examination of the existing access control mechanisms for electronic health records (EHRs) at the University of Port Harcourt Teaching Hospital (UPTH) revealed a predominantly critical and unfavourable assessment from the staff. The findings indicated widespread discontent across multiple dimensions of the access-control environment. Staff expressed strong dissatisfaction with the system's efficiency, finding it cumbersome rather than time-saving. Significant concerns were also raised regarding the protection of patient confidentiality. Core properties of a secure access system, such as the ability to audit user actions, were found to be profoundly lacking; most participants reported that it was exceptionally difficult to determine who had accessed a patient’s record. Furthermore, inter-departmental data retrieval was widely regarded as non-seamless, and overall satisfaction with the system's security and controls was exceptionally low. This sentiment was reinforced by staff reports of a heavy administrative burden

and frequent difficulties in retrieving necessary information, pointing to systemic friction in daily workflows.

This pattern of findings provides evidence that the current mechanisms fail to adequately support effective healthcare delivery while safeguarding sensitive information. The results suggest a significant misalignment between the system's technological design and the dynamic requirements of the hospital environment. When audit trails are opaque, accountability becomes performative rather than operative, weakening both deterrence and the capacity to remediate improper access. The practical implications are significant; such deficiencies can lead to inefficient clinical workarounds, exacerbate errors, delay treatments, and compromise patient confidentiality. These deficits—poorly defined permission scopes, fragile processes for granting and revoking access, and inadequate operational visibility—are precisely the issues that a Role-Based Access Control (RBAC) model is designed to address.

The observed negative perceptions are consistent with findings from other health systems where EHRs predate the disciplined application of modern access-control standards. Concerns over confidentiality echo explorations of vulnerabilities in health databases where off-the-shelf software can heighten breach risks (Basil et al., 2022). The difficulty in auditing access aligns with systematic analyses that categorize authorization as a critical but often underdeveloped component (Cobrado et al., 2024). Research on audit logs shows that when access trails are underused, clinical teams lose trust in the system's ability to protect privacy (Kannampallil & Adler-Milstein, 2022). The low confidence in restricting unauthorized views is similar to findings on patient engagement, where privacy issues impede effective control (Alomar et al., 2024). Furthermore, challenges with inter-departmental access parallel examinations of cross-organizational sharing, where technical hurdles create friction (Høstgaard et al., 2024).

However, the findings also diverge from some established scholarship, often due to contextual nuances. The intensity of dissatisfaction with cross-department access and auditing appears more acute at UPTH. One reason may be the infrastructural context; in settings with intermittent networks and power, users often develop workaround practices that erode the coherence of access policies. Literature on EHR adoption in sub-Saharan Africa repeatedly points to infrastructural unreliability as a determinant of weak security practices, which may magnify the negative user experience compared to better-resourced systems (Odekunle et al., 2017). Another point of divergence is regulatory salience. In jurisdictions with strongly institutionalized privacy laws, users encounter more visible monitoring. While Nigeria's legal framework has evolved with the 2023 Data Protection Act, health-sector compliance remains uneven, and the absence of routine privacy monitoring likely weakens confidence in access governance (DataGuidance, 2020).

In summary, the results reveal a system that has not effectively encoded the principles of least privilege and accountability in a way that frontline users can recognize and trust. The experience of administrative load and opaque auditing signals a governance gap that modern RBAC implementations are designed to close (Ferraiolo et al., 2007). The concordance between this study's data and prior work on RBAC and audit logging reinforces the conclusion that the perceived inefficiencies are symptoms of a structural authorization problem.

Conclusion

A consolidated view of the research findings presents a verdict on the assessment of Role-Based Access Control system at the University of Port Harcourt Teaching Hospital that is both important and conditional. The evidence suggests that while the initiative is overwhelmingly feasible from a human-factor and organisational-need perspective, its success is severely constrained by profound deficits in the institution's technical and resource foundations. The study

therefore arrives at the position that the introduction of an RBAC system is not a question of 'if' but of 'how' and, more critically, 'when'. The pathway to successful implementation is not through the immediate procurement of a software solution, but through a deliberate and strategic process of foundational capacity building that directly addresses the weaknesses identified by the hospital's own staff. It is recommended that a formal, multi-year "EHR Security and Infrastructure Modernisation Plan" be developed and approved within the next twelve-month fiscal planning cycle by management of the hospital, also hospital management should at information security relating patient records management for efficient service delivery.

References

Alshahrani, A., Jamal, A., & Tharkar, S. (2021). How private are the electronic health records? Family physicians' perspectives towards electronic health records privacy. Journal of Health Informatics in Developing Countries, 15(1).

Alomar, D., Almashmoum, M., Eleftheriou, I., Whelan, P., & Ainsworth, J. (2024). The impact of patient access to electronic health records on health care engagement: Systematic review. Journal of Medical Internet Research, 26, e56473. https://doi.org/10.2196/56473

Atlam, H. F., & Yang, Y. (2025). Enhancing healthcare security: A unified RBAC and ABAC risk-aware access control approach. Future Internet, 17(6), 262. https://doi.org/10.3390/fi17060262

Basil, N. N., Ambe, S., Ekhator, C., & Fonkem, E. (2022). Health records database and inherent security concerns: A review of the literature. Cureus, 14(10), e30168. https://doi.org/10.7759/cureus.30168

Blumenthal, D., & Tavenner, M. (2010). The "meaningful use" regulation for electronic health records. *New England Journal of Medicine, 363*(6), 501–504.

Carvalho Junior, M. A. de, & Bandiera-Paiva, P. (2021). Implications of loosened Role-based Access Control session control implementation for the enforcement of Dynamic Mutually Exclusive Roles properties on Health Information Systems. *Informatics in Medicine Unlocked, 26*, 100780.

Classen, D. C., Holmgren, A. J., Co, Z., Newmark, L. P., Seger, D., Danforth, M., & Bates, D. W. (2020). National trends in the safety performance of electronic health record systems from 2009 to 2018. *JAMA Network Open, 3*(5), e205547.

Cobrado, U. N., Sharief, S., Regahal, N. G., Zepka, E., Mamauag, M., & Velasco, L. C. (2024). Access control solutions in electronic health records systems: A systematic review. Informatics in Medicine Unlocked, 49, 101552. https://doi.org/10.1016/j.imu.2024.101552

Data Guidance (2020). Nigerian Data Protection Regulation 2019: Implementation Framework. https://www.dataguidance.com/sites/default/files/ndpr_implementation_framework_november_2020.pdf?utm_source=chatgpt.com

Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics, 46*(3), 541–562.

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2007). Role-based access control (2nd ed.). 418–418. https://csrc.nist.gov/pubs/book/2007/01/rolebased-access-control/final

Helms, E., & Williams, L. (2011). Evaluating access control of open source electronic health record systems. In Proceedings of the 3rd Workshop on Software Engineering in Health Care (pp. 63-70).

Høstgaard, A. M., Nøhr, C., & Jensen, S. (2024). Healthcare professionals' cross-organizational access to electronic health records: A scoping review. International Journal of Medical Informatics, 189, Article 105688. https://doi.org/10.1016/j.ijmedinf.2024.105688

Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., Shields, A., Rosenbaum, S., & Blumenthal, D. (2009). Use of electronic health records in U.S. hospitals. *New England Journal of Medicine, 360*(16), 1628–1638.

Kannampallil, T., & Adler-Milstein, J. (2022). Using electronic health record audit log data for research: insights from early efforts. Journal of the American Medical Informatics Association : JAMIA, 30(1), 167–171. https://doi.org/10.1093/jamia/ocac173

Keshta, I., & Odeh, A. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal, 22*(2), 177-183.

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41(8), 127. https://doi.org/10.1007/s10916-017-0778-4

Manor, G. L. (2024, February 7). Best practices to implement role-based access control (RBAC) for developers. Permit.io.

Nyame, G., & Qin, Z. (2020). Precursors of Role-Based Access Control Design in KMS: A Conceptual Framework. Information, 11(6), 334.

Odekunle, F. F., Odekunle, R. O., & Shankar, S. (2017). Why sub-Saharan Africa lags in electronic health record adoption and possible strategies to increase its adoption in this region. International Journal of Health Sciences, 11(4), 59–64. https://pmc.ncbi.nlm.nih.gov/articles/PMC5654179/

Sandhu, R., Ferraiolo, D. F., & Kuhn, D. R. (2000). The NIST model for role-based access control: Toward a unified standard. In *Proceedings of the fifth ACM workshop on Role-based access control* (pp. 47–63). Association for Computing Machinery

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). Role-based access control models. *IEEE Computer, 29*(2), 38–47.

Solvang, O. S., Cassidy, S., Granja, C., & Solvoll, T. (2024). Healthcare professionals' cross-organizational access to electronic health records: A scoping review. International Journal of Medical Informatics, 183, 105688.