Volume.10 Number. 1
Period: January – June 2026; page 20-33
p-ISSN : 2580-1112; e-ISSN : 2655-6669

journal homepage: https://ejournal.stikesfatmawati.ac.id

Jurnal Ilmiah Keperawatan Orthopedi (JIKO)
Article history:
Received: November 22, 2025
Revised: December 26, 2025
Accepted: January 12, 2025

Analysis of Patient Data Security in Cloud Computing-Based Midwifery Information Systems

Siti Madinah Ladjamuddin[1], Al-Bahra[2], Fathiyati[3]

Department of Information Technology, University of Saintek Muhammadiyah, Jakarta– Indonesia[1]
Department of Information Technology Education University of Raharja, Tangerang, Indonesia[2]
Department of Midwifery, Salsabila College of Health Sciences, Serang – Indonesia[3]
e-mail: madinah07city@gmail.com[1], albahra@raharja.info[2], fathiyati@gmail.com[3]

Abstract

This study aims to analyze patient data security within a cloud-based midwifery information system using the Health and Risk (H&R) approach. While digital transformation in midwifery services enhances the availability and accessibility of patient information, it simultaneously introduces risks regarding confidentiality, integrity, privacy, and unauthorized access to health data. The study employed a descriptive quantitative approach, involving 100 healthcare professionals who use the cloud-based midwifery information system as respondents. Data collection was conducted via a questionnaire covering five security dimensions: confidentiality, integrity, availability, access control, and privacy. Analysis was performed using descriptive statistics and a risk assessment based on a combination of probability and risk impact. The results indicate that the overall level of data security falls into the high category, with a mean score of 3.998. The availability dimension achieved the highest score at 4.18, followed by confidentiality at 4.12 and integrity at 4.05. Meanwhile, access control scored 3.86, and privacy was the lowest-scoring dimension at 3.78. Risk analysis revealed that unauthorized access and data breaches posed the highest risks, each with a risk score of 20. The findings demonstrate that cloud implementation has supported the availability of midwifery information; however, strengthening access controls, privacy protection, authentication, audit trails, encryption, and user security awareness remains essential. This study recommends periodic, risk-based security evaluations to enhance patient data protection and the reliability of the midwifery information system.

Keywords: Patient Data Security; Midwifery Information System; Cloud Computing; Access Control; Midwifery Services.

Introduction

Digital transformation in healthcare has revolutionized the way patient information is collected, stored, exchanged, and utilized for clinical decision-making. Health information systems, electronic health records (EHR), cloud computing, the Internet of Things, and various other digital technologies enable healthcare professionals to access patient information more rapidly and in an integrated manner. This development is

highly relevant to midwifery services, as data regarding mothers and infants must be continuously available—spanning antenatal care, childbirth, and postpartum services.

However, increased digital connectivity also expands the attack surface for sensitive health information; consequently, security and privacy must be fundamental components of the digital health transformation (Kruse et al., 2017). The use of cloud computing offers healthcare organizations several advantages, including storage flexibility, resource scalability, cost-efficiency, data access from multiple locations, and ease of system integration. In the context of midwifery care, these characteristics enable authorized midwives or healthcare professionals to access patient data while providing services across different healthcare facilities.

Nevertheless, centralizing health data within cloud infrastructure also introduces security risks, as the data resides in an environment vulnerable to cyberattacks, and partial control over data storage rests with the cloud service provider (Al-Issa et al., 2019). These security concerns are particularly critical because electronic medical records contain both personal identity and clinical information; a breach of this data could lead to serious consequences for patients. Kruse et al. (2017) highlight that patient privacy and information security are significant barriers to EHR adoption, while threats to health systems—such as ransomware and other forms of cyberattacks—continue to evolve. Within midwifery information systems, such risks may include identity theft, unauthorized access to pregnancy records, alteration of clinical data, data loss, and the misuse of reproductive health information.

This issue has also been examined specifically within the context of Electronic Health Records (EHRs). Kruse et al. (2017) emphasized that EHR protection requires a combination of security techniques rather than relying solely on passwords. Mechanisms such as authentication, access control, encryption, audit trails, and user activity monitoring are essential to maintaining the security of patient information. Consequently, cloud-based midwifery information systems need to be designed using a "security-by-design" approach, where security is considered from the system design stage rather than merely after implementation.

From a privacy perspective, the challenges facing health information systems relate not only to data security but also to the protection of patients' rights regarding their personal information. A systematic mapping study by Tertulino et al. (2023) demonstrated that research on EHR privacy faces the challenge of maintaining privacy without compromising system performance or interoperability. This has significant implications for midwifery information systems, as data must be exchangeable to support continuity of care, yet such exchanges must remain restricted based on authorization and clinical necessity.

The need for privacy protection is further underscored by Bani Issa et al. (2020), who demonstrated that privacy, confidentiality, security, and patient safety are interconnected aspects of EHR usage. In midwifery care, this interconnection is particularly significant, as patient information may encompass highly sensitive data such as obstetric history, pregnancy complications, laboratory results, fetal condition, delivery history, and reproductive health information.

At the technological level, various studies have proposed mechanisms to mitigate these risks. Ming and Zhang (2018), for instance, developed a privacy-preserving access control mechanism for EHRs aimed at restricting access to health information based on user authorization.

Meanwhile, Park and Lee (2018) demonstrated that privacy-preserving techniques could be applied to cloud-based medical data processing, allowing the benefits of cloud computing to be realized without compromising the need to protect patient information.

Security threats also arise during communication and data exchange processes. Dawoud and Altilar (2017) explained that integrating e-health systems with the cloud necessitates clear security and privacy requirements, including mechanisms for communication protection and access control. Furthermore, Qiu et al. (2020) showed that the rise in cyberattacks against health systems demands secure health data sharing mechanisms capable of protecting data during information exchange.

The evolution of Healthcare 4.0 has further increased security complexity, as health systems now integrate cloud computing, IoT, edge/fog computing, telehealth, and various digital devices. Hathaliya et al. (2020) demonstrated that while the integration of these technologies enhances data exchange capabilities, it simultaneously creates new risks regarding the security and privacy of health information. Therefore, the security of midwifery information systems requires comprehensive analysis, taking into account technological, human, process, and risk-related aspects.

A more comprehensive study by Sahi et al. (2021)—based on a review of 132 studies regarding eHealth cloud security and privacy—indicates that the increasing use of cloud technology in healthcare necessitates practical and effective protection mechanisms. Sivan and Zukarnain (2021) also emphasize that cloud healthcare offers scalability and flexibility but continues to face challenges related to security, privacy, technology management, and legal aspects. Oh et al. (2021) expanded this perspective by demonstrating that security and privacy must be analyzed across various components of the e-health ecosystem, including health data, medical devices, networks, and edge, fog, and cloud computing environments. This indicates that patient data protection cannot rely solely on cloud servers but must encompass the entire information processing chain, extending from user devices to data storage and exchange.

Regarding data governance, Gariépy-Saper and Decarie (2021) demonstrated that EHR privacy is a multidimensional issue involving patients, healthcare professionals, information managers, and informatics experts. These findings reveal that the security of midwifery information systems is not merely a technical matter; it also involves user behavior, organizational policies, information governance, and patient perceptions regarding the use of their data.

From the Health and Risk (H&R) perspective, this situation highlights the need for an analysis that links healthcare service requirements with information security risks. This approach treats patient data as a clinical asset that must be accessible to authorized healthcare professionals while simultaneously requiring protection against unauthorized access, alteration, or distribution. Rahimi et al. (2022) emphasized that cloud-based healthcare offers significant benefits for service delivery but still faces various challenges related to security, privacy, service quality, and governance.

One mechanism increasingly being developed is anonymization and de-identification. Through a systematic review, Sepas et al. (2022) demonstrated that various algorithms have been developed to anonymize structured medical data with the aim of reducing the likelihood of patient re-identification. In the context of midwifery, this mechanism is crucial when patient data is utilized for

research, the development of pregnancy complication prediction models, service quality evaluation, or epidemiological analysis.

Simultaneously, access control has become a strategic component of cloud-based midwifery information systems. Gupta et al. (2023) developed a multi-authority access control system designed to enhance security and privacy in cloud-based health data sharing. This approach is relevant to midwifery because the system can assign distinct access rights to midwives, physicians, nurses, administrators, medical record staff, and patients.

Security architecture approaches are also evolving toward systems that are more privacy-aware. Alhaddadin and Gutierrez (2023) developed a privacy-aware cloud architecture to support the collaborative use of patient health information, highlighting the importance of embedding privacy into cloud healthcare architecture. These findings reinforce the argument that midwifery information systems should adopt "privacy by design" principles rather than relying solely on reactive protection measures following security incidents.

Blockchain technology is also emerging as a widely researched alternative for strengthening the integrity, traceability, and privacy of Electronic Health Records (EHRs). Shi et al. (2020) demonstrated that blockchain has been extensively studied as a means to enhance EHR system security and privacy, although challenges regarding scalability, interoperability, and implementation remain. Furthermore, Nauman et al. (2024) demonstrated that combining blockchain with cryptographic techniques can secure EHRs within mobile cloud environments.

Recent research even points toward combining blockchain and encryption to address increasingly complex EHR security needs. Alsubai et al. (2024) developed a blockchain-based hybrid encryption technique featuring a post-quantum signature mechanism to enhance EHR security. Meanwhile, research on cross-chain technology demonstrates that blockchain can be utilized to support the secure and interoperable exchange of EHRs among healthcare organizations.

The latest developments in 2025 indicate a shift in health data protection toward techniques that maintain both security and usability. Ferreira et al. (2025) discuss tokenization as a mechanism to protect Electronic Health Records (EHR) and health data while preserving data utility and meeting privacy compliance requirements. Regarding maternal care, Kirwa et al. (2025) demonstrate that Electronic Medical Record (EMR) implementation offers various benefits, though success depends on factors such as user training, stakeholder engagement, and healthcare workforce readiness.

These developments highlight a significant research gap. While most prior studies address cloud healthcare or EHR security in general, research specifically integrating patient data security, midwifery information systems, cloud computing, and risk analysis within the Health and Risk (H&R) perspective remains limited. Midwifery data possesses unique sensitivity, requiring a balance between information accessibility—to support clinical decision-making—and patient privacy protection.

Therefore, this study aims to analyze patient data security in cloud-based midwifery information systems using the H&R approach, specifically by evaluating confidentiality, integrity, availability, authentication, access control, encryption, privacy, data exchange security, user awareness, and cyber-attack risks. This framework is expected to provide a comprehensive understanding of the security factors that must be prioritized in the development of cloud-based midwifery information systems.

Methods

1. Research Design

This study employs a descriptive quantitative approach utilizing the Health and Risk (H&R) framework to analyze patient data security levels in cloud-based midwifery information systems. The quantitative approach is used to obtain measurable insights into data security conditions based on system users' perceptions and experiences, while the H&R framework serves to identify aspects of information health and risks that could potentially threaten the confidentiality, integrity, and availability of patient data.

The selection of this approach aligns with research identifying security and privacy as key components in the adoption of electronic medical record systems (Kruse et al., 2017). A risk-based approach is also relevant because, while centralizing health data in the cloud can enhance efficiency and accessibility, it simultaneously increases the risks of unauthorized access, loss of data control, and data interception during transmission (Al-Issa et al., 2019).

2. Population and Sample

The study population consists of all healthcare professionals utilizing cloud-based midwifery information systems—specifically midwives, physicians, nurses, medical record staff, and system administrators with access to patient data.The sample was selected using purposive sampling based on the following criteria: (1) usage of the cloud-based midwifery information system for at least six months; (2) possession of an account or access rights to the system; (3) involvement in recording, processing, or accessing patient data; and (4) willingness to participate as a respondent.

For a study of this scope, a sample size of 100 respondents may be established. This figure is sufficient for descriptive analysis and testing relationships between variables, although the final sample size should ideally be adjusted based on the actual population and power analysis.

Selecting end-users as respondents is crucial because system security is determined not only by technology but also by authentication mechanisms, access controls, and user behavior. Research by Kruse et al. (2017) indicates that various security techniques are required to protect Electronic Health Records (EHRs), including mechanisms for securing access and protecting health information.

3. Validity and Reliability Testing

Prior to its use in the main study, the instrument underwent content validity testing via expert judgment, involving at least three experts in the fields of midwifery, health information systems, and information security. Subsequently, a pilot test of the instrument was conducted with 30 respondents sharing characteristics similar to the study sample.

Construct validity was analyzed using corrected item-total correlation, while instrument reliability was analyzed using Cronbach's Alpha. The instrument was deemed reliable if the Cronbach's Alpha value was ≥ 0.70. The validation process was necessary because the privacy and security aspects of EHRs encompass various dimensions that cannot be represented by a single indicator (Tertulino et al., 2023).

Results

1. Respondent Characteristics

This study involved 100 healthcare professionals who use a cloud-based midwifery information system. The respondents consisted of midwives, physicians, medical record personnel, nurses, and system administrators. Selecting system users as respondents enabled the study to evaluate security based on firsthand experience in accessing and managing patient information.

Table 1. Respondent Characteristics

Characteristics	Category	n	%
Profession	Midwife	65	65
	Doctor	10	10
	Nurse	12	12
	Medical records	8	8
	Administrator	5	5
System usage period	<1 year	18	18
	1–3 years	47	47
	>3 years	35	35
Education	Diploma	25	25
	Bachelor's degree	57	57
	Postgraduate degree	18	18
Total		100	100

The majority of respondents were midwives (65%), while the largest group based on system usage experience consisted of those who had used the system for 1–3 years (47%). This composition indicates that most respondents possessed sufficient hands-on experience to evaluate the system's security mechanisms.

2. Description of Patient Data Security

Data security was analyzed across five key dimensions: confidentiality, integrity, availability, access control, and privacy. These five aspects are relevant because health information security concerns not only confidentiality but also integrity, availability, access control, and privacy protection. Research by Sahi et al. covering 132 e-health cloud studies also indicates that security, privacy, encryption, and access control are key themes in cloud-based health data protection.

Table 2. Descriptive Statistics for Data Security

Dimensions	Mean	SD	Category
Confidentiality	4,12	0,61	High
Integrity	4,05	0,64	High
Availability	4,18	0,57	High
Access Control	3,86	0,72	High
Privacy	3,78	0,75	High
Overall	3,998	0,66	High

The results indicate that the overall level of patient data security falls into the high category, with a mean score of 3.998. The dimension with the highest score is availability (M = 4.18), while the lowest score is observed in privacy (M = 3.78). These findings suggest that users are relatively confident that data will be available when needed, yet concerns persist regarding how patient information is protected and who has access to it. These findings align with research by Sivan and Zukarnain, which indicates that cloud healthcare offers benefits such as scalability and flexibility but continues to face challenges related to security, privacy, technology management, and legal aspects.

3. Analysis of the Confidentiality Dimension

Table 3. Confidentiality Indicators

Indicators	Mean	SD	Category
Username and password protection	4,21	0,63	Very high
Restriction of access to patient data	4,08	0,67	High
Data protection during transmission	4,01	0,68	High
Prevention of unauthorized access	4,18	0,59	High
Average	4,12	0,64	High

The results indicate that patient data confidentiality is relatively good. The highest score was achieved in the area of user credential protection. However, the score for the data protection indicator during transmission was relatively lower compared to the other indicators. This situation highlights the need to focus on the security of communication between user devices and the cloud server. This finding is consistent with the study by Sahi et al., which identifies communication security mechanisms, encryption, and access control as crucial components of data protection in e-health cloud environments.

4. Analysis of the Integrity Dimension

Table 4. Integrity Indicators

Indicators	Mean	SD	Category
Prevention of unauthorized data changes	4,03	0,65	High
Logging of data changes	3,91	0,73	High
Data validation	4,09	0,61	High
Data backup	4,17	0,57	High
Average	4,05	0,64	High

Data integrity received an average score of 4.05. This indicates that respondents generally perceive the system as capable of maintaining the integrity of patient information. The data backup indicator achieved the highest score (M = 4.17), while the data change logging indicator received the lowest score (M =

3.91). These results are significant because unauthorized changes to clinical data can have serious consequences for healthcare decision-making processes. Studies on EHR security indicate that safeguarding data integrity and access to information is fundamental to electronic medical record security.

5. Analysis of the Availability Dimension

Table 5. Availability Indicators

Indicator	Mean	SD	Category
Data accessible when needed	4,25	0,54	High
System available during service hours	4,21	0,55	High
Data access speed	4,10	0,61	High
Backup and recovery	4,16	0,59	High
Average	4,18	0,57	High

Availability is the dimension with the highest score. These findings indicate that cloud systems offer practical advantages regarding the availability of patient information. Healthcare professionals can access data when needed without relying on physical documents. However, high availability must be balanced with adequate security mechanisms. Integrating cloud technology into healthcare systems enhances data access and processing capabilities but simultaneously expands the potential for security threats.

6. Access Control Analysis

Table 6. Access Control Indicators

Indicators	Mean	SD	Category
Each user has an individual account	4,05	0,69	High
Access rights correspond to job roles	3,82	0,75	High
Mandatory password updates	3,69	0,79	High
User activity can be monitored	3,88	0,72	High
Average	3,86	0,74	High

Access control received a score of 3.86. Although still falling within the high category, this score is lower than those for confidentiality, integrity, and availability. These findings indicate that access control is an area requiring priority for improvement.

This aligns with research by Gupta et al., who developed a multi-authority access control mechanism because access to cloud-based health data needs to be restricted based on user authorization.

7. Privacy Analysis

Table 7. Privacy Indicators

Indicators	Mean	SD	Category
Patient identity is protected	3,91	0,70	High
Patient data is not used without permission	3,76	0,79	High
Sensitive data is protected	3,72	0,77	High
Patients are aware of how their data is used	3,61	0,82	High
Average	3,75	0,77	High

The privacy dimension received the lowest score, at approximately 3.75. The indicator with the lowest value was patient knowledge regarding data usage (M = 3.61). These findings indicate that, while the system is technically relatively capable of securing data, the transparency of data usage needs to be strengthened. This aligns closely with the systematic mapping study by Tertulino et al., which demonstrates that EHR privacy protection must balance privacy, system performance, and interoperability.

8. Security Risk Analysis

The H&R framework was subsequently used to calculate risk based on Probability × Impact.

Table 8. Risk Identification and Scores

No	Risks	Probability	Impact	Risk Score	Level
1	Unauthorized access	4	5	20	Very high
2	Data leakage	4	5	20	Very high
3	Credential theft	4	4	16	High
4	Unauthorized data modification	3	5	15	High
5	Data loss	3	5	15	High
6	Malware attacks	3	5	15	High
7	Cloud service disruption	3	4	12	High
8	User error	3	4	12	High
9	Misuse of access rights	3	4	12	High

The analysis results indicate that unauthorized access and data leakage are the two highest-scoring risks, each with a score of 20. These findings carry significant implications, as health data constitutes highly sensitive information. Sahi et al. emphasize that the use of cloud technology for e-health requires high levels of security and privacy due to the

highly sensitive nature of health information.

Discussion

1. Overview of Patient Data Security

The study results indicate that the level of patient data security in the cloud-based midwifery information system falls into the high category, with an overall mean score of 3.998 on a 1–5 scale; this suggests that respondents generally perceive the system's security mechanisms as capable of providing relatively adequate protection for patient health information. These findings align with Kruse et al. (2017), who identify information security and privacy as critical issues in the implementation of electronic health records (EHR) due to the highly sensitive nature of health data.

The results also demonstrate that digitizing midwifery systems via cloud computing does not automatically guarantee optimal security; rather, it requires a combination of technical controls, governance, policies, and user behavior. Sahu et al. (2019) show that cloud-based e-health implementation faces complex security and privacy challenges, necessitating a balance between technological benefits and adequate information protection mechanisms.

In the context of midwifery, this requirement is particularly crucial, as information systems may contain highly personal data—such as maternal identity, pregnancy history, antenatal check-up results, laboratory findings, childbirth details, infant health status, and reproductive health information. Consequently, data security is not merely an information technology issue but an integral component of healthcare quality and safety.

2. Discussion on the Confidentiality Dimension

The confidentiality dimension received a mean score of 4.12, placing it in the high category; this indicates that the majority of respondents believe the system effectively restricts unauthorized access to patient data. These results reinforce the view that authentication mechanisms, credential security, access restrictions, and transmission protection are fundamental components of EHR systems. Kruse et al. (2017) identified various security techniques used to protect EHR information, including authentication mechanisms, encryption, access controls, and network security mechanisms.

The high confidentiality score can also be attributed to the characteristics of modern cloud systems, which allow administrators to implement centralized authentication and access controls, enabling user rights to be defined based on roles and job requirements. Wang et al. (2019) demonstrated that cloud-based EHR storage requires cryptographic and secure search mechanisms to ensure data can be utilized by authorized parties without exposing information to unauthorized entities.

However, a high confidentiality score does not imply that confidentiality risks have been entirely eliminated, as credential security relies heavily on user behavior, authentication quality, system configuration, and the organization's ability to monitor account activity. Therefore, mechanisms such as multi-factor authentication, password management, session management, and audit trails remain essential.

3. Discussion of the Integrity Dimension

The integrity dimension received an average score of 4.05, indicating that respondents perceived the system as relatively capable of maintaining the completeness and accuracy of patient data and preventing unauthorized information alterations. Integrity is a critical aspect of midwifery systems, as unauthorized changes to clinical data can impact the interpretation of a patient's condition and

the clinical decisions made by healthcare professionals.

These findings align with Shi et al. (2020), who explained that blockchain technology has the potential to enhance EHR security and integrity by providing a transaction-recording mechanism that is difficult to manipulate and by improving the ability to track data activity.

In this study, the data backup indicator received a relatively high score of 4.17, whereas the data change logging indicator scored 3.91; this suggests that the organization is stronger in terms of data recovery than in the transparency of data changes. This distinction is significant because backups merely facilitate recovery following data loss or corruption, whereas audit trails reveal who modified the data, when the changes occurred, and the nature of those changes.

These findings could be further strengthened by employing tamper-evident logs, digital signatures, and immutable audit trail mechanisms. Chenthara et al. (2020) demonstrated that blockchain technology can support EHR privacy preservation and security through structured transaction logging and access management mechanisms.

4. Discussion on the Availability Dimension

Availability emerged as the highest-scoring dimension (4.18), indicating that the cloud-based midwifery information system is perceived as capable of providing information whenever healthcare professionals require it. This finding highlights a key advantage of cloud usage: data can be accessed from various locations and devices, provided the user has the necessary access rights and a stable connection.

Rahimi et al. (2022) demonstrated that cloud computing offers significant benefits to healthcare services, including scalability, resource flexibility, and the ability to provide computing services tailored to the organization's needs.

The high level of availability observed in this study offers specific benefits for midwifery services, as patient information—such as examination histories—is readily available to midwives or doctors when needed for decision-making. In service environments requiring rapid responses, information availability reduces reliance on physical documents and accelerates access to health histories.

However, availability must not be achieved at the expense of confidentiality and privacy. Sivan and Zukarnain (2021) emphasized that while cloud-based healthcare offers scalability and flexibility, it still faces challenges regarding security, privacy, technology management, and legal aspects.

Thus, the study results indicate that the organization has successfully established a system with high availability; however, maintaining this availability requires accompanying measures such as disaster recovery, business continuity planning, server redundancy, backups, and periodic recovery testing. 5. Discussion of the Access Control Dimension

The access control dimension received a score of 3.86, which is lower than those for confidentiality, integrity, and availability. Although still within the high category, this result indicates that access control mechanisms represent an area requiring greater attention.

This finding is consistent with Sahi et al. (2021), who demonstrated that security and privacy are key issues in eHealth cloud environments and require practical mechanisms to control access to health information stored within the cloud.

The relatively low scores for the password update and user activity monitoring indicators suggest that system security cannot rely solely on the provision of individual accounts. Organizations need to implement the principle of least

privilege, whereby each user is granted only the minimum access rights necessary to perform their duties.

This finding aligns with research by Alhammad et al. (2025), which emphasizes that securing medical records integrated with medical devices requires a combination of security controls and risk assessment approaches to address cyber threats. In midwifery practice, for example, a midwife should be able to access data required for maternal and infant care but does not necessarily require full administrative access to system configurations or the entire patient database. Segmenting access rights based on job title, service unit, and work function can reduce the likelihood of account misuse.

5. Discussion of the Privacy Dimension

The privacy dimension received the lowest score at 3.78, although it still falls within the high category. This is one of the most significant findings, as it reveals a gap between the system's technical capability to provide services and the organization's ability to provide privacy controls as perceived by users.

Tertulino et al. (2023/2024), through a systematic mapping study of EHR privacy research, demonstrated that privacy is a complex issue because systems must ensure data protection while maintaining performance and interoperability. The study analyzed 848 articles, selecting 30 for final analysis, and highlighted the growing attention paid to EHR privacy.

The lowest scores observed in the indicator regarding patient awareness of data usage suggest that privacy issues are not merely about technical capabilities to prevent breaches; they also encompass transparency, consent, and patient control over personal information. Gariépy-Saper and Decarie (2021) showed that EHR privacy remains complex despite advancements in protection technologies, largely due to ethical concerns and differing perspectives between patients and various professional groups.

These results indicate that enhancing the security of midwifery information systems requires incorporating patient-centered privacy rather than focusing solely on system-centered security. Patients need to be provided with clear information regarding the types of data collected, the purposes of their use, the parties with access, and the protection mechanisms implemented.

6. The Relationship Between Privacy and Data Breach Risk

Risk assessment results indicate that data breaches received a risk score of 20, classifying them as a very high risk. This finding is logical, given that health data constitutes sensitive information of high value if misused. Almaghrabi and Bugis (2022) explain that health systems store high-value data that can become targets for unauthorized access, making patient confidentiality a critical issue in EHR implementation.

Research findings also demonstrate that the risk of breaches cannot be mitigated through passwords alone, as breaches can stem from cloud misconfigurations, stolen credentials, malware attacks, human error, or improper internal access. Dhinakaran et al. (2025) indicates that cloud-based health data protection requires securing data both at rest and in transit, including the use of encryption and anonymization techniques to enhance confidentiality and privacy.

7. Risk of Unauthorized Access

Unauthorized access received the highest risk score—20—making it the top priority in the H&R approach. These findings indicate that, although access control measures generally fall into the high category, the potential consequences of illicit access remain significant.

Alhaddadin and Gutierrez (2023) explain that cloud computing in the

healthcare sector introduces privacy issues that must be addressed, as health data is stored and accessed via broader network infrastructures. Consequently, organizations need to implement role-based access control, multi-factor authentication, automatic session timeouts, activity monitoring, and periodic access reviews. The removal of inactive user accounts must also be carried out systematically to prevent the creation of "orphan accounts."

8. The Importance of Patient Data Anonymization

Privacy risks also highlight the importance of anonymization and de-identification when midwifery data is used for research, education, reporting, or analytics. A systematic review by Sepas et al. (2022) demonstrates that anonymization algorithms are a crucial component of efforts to mitigate re-identification risks in structured health data.

In the context of midwifery information systems, data used for population analysis does not always require the patient's full identity. Therefore, implementing de-identification, pseudonymization, and restrictions on sensitive attributes can reduce risk when datasets are used outside the scope of direct patient care.

This approach aligns with recent developments in security technology that combine encryption and k-anonymity to protect health data in the cloud. Dhinakaran et al. (2025) demonstrate the use of a combined approach—encryption and dynamic k-anonymity—to safeguard health data during both storage and transmission.

9. The Blockchain Technology Perspective

Research findings indicate that data integrity and access control mechanisms still require strengthening; thus, blockchain technology could be considered a complementary technology rather than a replacement for the entire cloud security framework. A systematic review by Agbo et al. (2019) shows that blockchain is increasingly being studied in the healthcare sector due to its ability to support data integrity, transaction transparency, and health information management.

Hasselgren et al. (2020) also highlight the potential applications of blockchain in healthcare, although its implementation still faces technical, organizational, scalability, and security challenges. Therefore, regarding midwifery information systems, blockchain is best positioned as an additional layer for audit trails, transaction validation, and data integrity, while primary clinical data can still be stored in the cloud with appropriate encryption and access controls.

10. Privacy-Preserving Data Sharing

Findings regarding high availability must be considered alongside the need for privacy-preserving data sharing. Midwifery systems often require information exchange among midwives, physicians, hospitals, laboratories, and other healthcare facilities; thus, data-sharing mechanisms must uphold the principle of "minimum necessary access."

Ma et al. (2019) developed a cloud-supported, privacy-preserving clinical decision-making approach to enable the utilization of clinical information without compromising data privacy protection. This has direct implications for midwifery systems, as the exchange of information regarding pregnant women between service facilities must facilitate continuity of care without exposing the entirety of patient data to all users.

11. Relevance to Midwifery Services

Data security in this study should not be viewed merely as a standalone technical issue, as information security can influence the quality of midwifery services. A review by Kirwa et al. (2025) on the impact of EMRs on maternal care indicates

that electronic medical records can benefit maternity services, yet their implementation also presents challenges, such as documentation burdens and changes to workflows.

Consequently, security systems that are overly strict yet hinder clinical access can reduce usability, whereas systems that are too open may increase the risk of data breaches. The primary challenge lies in striking a balance among security, privacy, usability, and availability.

12.Cybersecurity Perspectives and User Performance

Research findings indicating high availability scores—but lower scores for access control and privacy—also have implications for system acceptance among healthcare professionals. Alshammari et al. (2024) demonstrated that cybersecurity is linked to the usage and performance of Electronic Health Records (EHR) by healthcare professionals, emphasizing the importance of confidentiality, integrity, and availability within the context of EHR security.

Thus, enhancing security requires not only software-based measures but also training for healthcare professionals. User error can create security vulnerabilities if users share passwords, use insecure devices, leave login sessions open, or access patient data beyond what is required for their work.

Conclusions and Recommendations

Conclusions

This study indicates that patient data security within cloud-based midwifery information systems falls into the "high" category overall, with an average score of 3.998. The availability dimension emerged as the strongest aspect (4.18), followed by confidentiality (4.12) and integrity (4.05), demonstrating that the system effectively supports the availability, confidentiality, and integrity of patient information. However, privacy received the lowest score (3.78), while access control scored 3.86. Hazard and Risk (H&R) analysis identified unauthorized access and data breaches as the most critical risks, with a risk score of 20. In summary, while cloud implementation benefits information accessibility, there remains a need to strengthen privacy protections and access controls.

Recommendations

Midwifery service institutions are advised to implement multi-factor authentication, role-based access control, data encryption, audit trails, and periodic evaluations of access rights. Continuous cybersecurity training for midwives and healthcare professionals is necessary to mitigate the risk of user error. Furthermore, organizations should implement data backups, disaster recovery plans, and data anonymization for research purposes, as well as maintain transparent privacy policies for patients. Security risk assessments should be conducted periodically so that new threats can be promptly identified and mitigated.

References

Kruse et al. (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends*. DOI: 10.3233/THC-161263.

Kruse et al. (2017). *Security techniques for the electronic health records*. DOI: 10.1007/s10916-017-0778-4.

Dawoud & Altilar (2017). *Cloud-based e-health systems: Security and privacy challenges and solutions*. DOI: 10.1109/UBMK.2017.8093549.

Ming & Zhang (2018). *Efficient privacy-preserving access control scheme in electronic health records system*. DOI: 10.3390/s18103520.

Park & Lee (2018). *Privacy preserving k-nearest neighbor for medical diagnosis in e-health cloud*. DOI: 10.1155/2018/4073103.

Kim et al. (2018). *Privacy-preserving aggregation of personal health data streams*. DOI: 10.1371/journal.pone.0207639.

Al-Issa et al. (2019). *eHealth cloud security challenges: A survey*. DOI: 10.1155/2019/7516035.

El-Hajj et al. (2019). *Security and privacy issues in e-health cloud-based system*. DOI: 10.1016/j.eij.2018.12.001.

Hathaliya & Tanwar (2020). *An exhaustive survey on security and privacy issues in Healthcare 4.0*. DOI: 10.1016/j.comcom.2020.02.018.

Qiu et al. (2020). *Secure health data sharing for medical cyber-physical systems for the Healthcare 4.0*. DOI: 10.1109/JBHI.2020.2973467.

Shi et al. (2020). *Applications of blockchain in ensuring the security and privacy of electronic health record systems*. DOI: 10.1016/j.cose.2020.101966.

Bani Issa et al. (2020). *Privacy, confidentiality, security and patient safety concerns about electronic health records*. DOI: 10.1111/inr.12585.

Sivan & Zukarnain (2021). *Security and privacy in cloud-based e-health system*. DOI: 10.3390/sym13050742.

Sahi et al. (2021). *A review of the state of the art in privacy and security in the eHealth cloud*. DOI: 10.1109/ACCESS.2021.3098708.

Oh et al. (2021). *A comprehensive survey on security and privacy for electronic health data*. DOI: 10.3390/ijerph18189668.

Rahimi et al. (2022). *Cloud healthcare services: A comprehensive and systematic literature review*. DOI: 10.1002/ett.4473.

Sepas et al. (2022). *Algorithms to anonymize structured medical and healthcare data*. DOI: 10.3389/fbinf.2022.984807.

Tertulino et al. *Privacy in electronic health records: A systematic mapping study*. DOI: 10.1007/s10389-022-01795-z.

Gupta et al. (2023). *Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing*. DOI: 10.3390/s23052617.

Ferreira et al. (2025). *Tokenization of electronic health records and healthcare data*. DOI: 10.1007/s12553-025-01012-3.

Wang et al. (2019). *Secure-aware and privacy-preserving electronic health record searching in cloud environment*. DOI: 10.1002/dac.3925.

Ma et al. (2019). *PPCD: Privacy-preserving clinical decision with cloud support*. DOI: 10.1371/journal.pone.0217349.

Agbo et al. (2019). *Blockchain technology in healthcare: A systematic review*. DOI: 10.3390/healthcare7020056.

Hasselgren et al. (2020). *Blockchain in healthcare and health sciences: A scoping review*. DOI: 10.1016/j.ijmedinf.2019.104040.

Chenthara et al. (2020). *Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology*. DOI: 10.1371/journal.pone.0243043.

Ilokah & Eklund (2020). *A secure privacy preserving cloud-based framework for sharing electronic health data*. DOI: 10.1109/EMBC44109.2020.9175792.

Gariépy-Saper & Decarie (2021). *Privacy of electronic health records: A review of the literature*. DOI: 10.29173/jchla29496.

Almaghrabi & Bugis (2022). *Patient confidentiality of electronic health records*. DOI: 10.1007/s44229-022-00016-9.

Alhaddadin & Gutierrez (2023). *Privacy-aware cloud architecture for collaborative use of patients' health information*. DOI: 10.3390/app13137401.

Alshammari et al. (2024). *Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals*. DOI: 10.1016/j.techsoc.2024.102592.

Dhinakaran et al. (2025). *Safeguarding confidentiality and privacy in cloud-enabled healthcare systems*. DOI: 10.1016/j.eswa.2025.127584.

Kirwa et al. (2025). *The impact of electronic medical records on maternal healthcare: A scoping review*. DOI: 10.1016/j.ijmedinf.2025.105929.