2026 Volume: 02 Issue: 08 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-21

ASSESSMENT AND UTILIZATION OF CLOUD STORAGE ON DATA SECURITY AND DISASTER PREPAREDNESS IN ELECTRONIC MEDICAL RECORD: EVIDENCE FROM A NIGERIAN TERTIARY HOSPITAL

Gwarjiko Usman Abdulrahman[1]*, Adeojo Michael Babatunde[1], S. A. Jimoh[1]

[1]Department of Computer Science, Faculty of Natural and Applied Sciences, Achievers University, Owo, Ondo State, Nigeria.

Article Received: 13 July 2026

Article Revised: 2 August 2026

Published on: 22 August 2026

***Corresponding Author: Gwarjiko Usman Abdulrahman**

Department of Computer Science, Faculty of Natural and Applied Sciences, Achievers University, Owo, Ondo State, Nigeria.

DOI: https://doi-doi.org/101555/ijrpa.4297

ABSTRACT

The rapid digitalisation of healthcare through Electronic Medical Record (EMR) systems has heightened the importance of resilient, secure data storage infrastructure. This study assessed the utilization of cloud storage on data security and disaster preparedness in the EMR system of a public tertiary hospital in North-Central Nigeria, using Ibrahim Badamasi Babangida (IBB) Specialist Hospital, Minna, as a case study.

Anchored in the Technology Acceptance Model (TAM), extended with the Technology-Organisation-Environment (TOE) and Unified Theory of Acceptance and Use of Technology (UTAUT) frameworks, the study adopted a descriptive cross-sectional survey design. The study population comprised 520 eligible staff across five professional cadres, from which a sample of 270 was determined using Cochran's formula with finite population correction and an 18% allowance for potential non-response, and proportionately stratified across clinical/medical staff, nursing staff, Health Information Management (HIM) professionals, information technology (IT) personnel, and administrative staff. Data were collected using a structured, expert-validated Cloud Server Adoption, Data Security and Disaster Preparedness Questionnaire (CSADSQ; Cronbach's alpha = 0.82). Two hundred and fifty questionnaires were validly completed and returned (92.6% response rate) and analysed descriptively and inferentially using Pearson Product-Moment Correlation and one-way ANOVA in SPSS version 25.0.

Findings revealed a paradox: current cloud storage utilization was critically low (grand mean = 2.88), with 90% of respondents indicating that the hospital relies solely on physical, on-premises servers, yet respondents strongly recognised the security and resilience benefits of cloud computing. Cloud storage utilization showed a strong, positive, and statistically significant relationship with both data security ($r = 0.82$, $p < 0.001$) and disaster preparedness ($r = 0.79$, $p < 0.001$). Only 15% of respondents confirmed the existence of a documented disaster recovery plan. One-way ANOVA revealed a statistically significant difference in perceived benefits across professional cadres ($F = 4.56$, $p = 0.012$), with IT and HIM staff perceiving significantly greater benefit than clinical, nursing, and administrative staff. High subscription costs, inadequate internet bandwidth, limited technical skills, and regulatory uncertainty around the Nigeria Data Protection Regulation (NDPR) were identified as the principal barriers to utilization.

The study concludes that a Hybrid Cloud Architecture, combining on-premises servers for daily low-latency operations with a secure, geographically redundant cloud layer for automated backup and disaster recovery, represents the most viable pathway for resource-constrained healthcare institutions in Nigeria and comparable developing-country settings. The study contributes an empirically grounded, context-specific framework linking cloud storage utilization to the CIA triad of data security and to institutional disaster resilience, and offers actionable recommendations for hospital management, IT departments, and policymakers.

KEYWORDS: *Cloud Storage Utilization; Data Security; Disaster Preparedness; Electronic Medical Records; Health Information Management; Nigeria; Technology Acceptance Model.*

1. INTRODUCTION

The global healthcare sector has undergone substantial digital transformation over the past two decades, driven largely by the adoption of Electronic Medical Record (EMR) systems that replace paper-based record keeping with computerised patient information management (Adler-Milstein, Aggarwal, & Holmgren, 2021). EMR systems support timely clinical decision-making, reduce medical errors, and enhance continuity of care (Ahmadi, Rezaei, & Valinejadi, 2022). As health institutions accumulate ever-larger volumes of sensitive patient data, however, the adequacy of the underlying storage infrastructure has become a critical determinant of both information security and organisational resilience.

Traditional on-premises storage exposes healthcare institutions to hardware failure, cyber-attack, and physical disaster, and is costly to scale (Nyangena, Kimwele, & Okeyo, 2022). Cloud storage has emerged internationally as an alternative that offers scalable capacity, advanced encryption, automated backup, and geographically redundant disaster recovery (Kumar & Singh, 2022; Babar, Khan, & Rashid, 2023). In healthcare specifically, cloud infrastructure strengthens the confidentiality, integrity and availability (the CIA triad) of patient information while enabling rapid recovery following ransomware attacks, power failure, fire, or flooding (Alzahrani, Alalwan, & Sitaram, 2022; Garg & Sharma, 2023).

In Nigeria, cloud storage utilization in healthcare remains inconsistent and, in many public tertiary institutions, minimal, with continued heavy reliance on locally hosted servers and limited backup mechanisms (Eze, Chinedu-Eze, & Okike, 2021; Adebayo, Ogunkeye, & Bello, 2023). While a growing body of research has examined EMR implementation and general cloud computing adoption in Nigerian healthcare, comparatively little empirical work has directly linked cloud storage utilization to measured outcomes in data security and disaster preparedness within a single institutional case, or examined how the synchronisation of physical and cloud infrastructure affects data consistency and recovery capability. This study addresses that gap using Ibrahim Badamasi Babangida (IBB) Specialist Hospital, Minna, Niger State, as a case study.

The specific objectives were to: (i) assess the current level of cloud storage utilization in the hospital's EMR system; (ii) examine the effectiveness of cloud server utilization in improving the confidentiality, integrity and availability of electronic medical records; (iii) evaluate the effectiveness of synchronisation between physical and cloud servers in ensuring data consistency, integrity, accessibility and real-time availability; and (iv) determine the influence of cloud server utilization on disaster preparedness through automated backup, data replication, disaster recovery and business continuity mechanisms.

2. Theoretical Framework and Literature Review

2.1 Technology Acceptance Model (TAM)

The study is anchored in the Technology Acceptance Model (Davis, 1989), which explains technology use through Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). Extensions of TAM incorporating perceived security risk and trust have been shown to be particularly relevant to cloud computing, as clinical staff frequently resist new systems perceived as disruptive or insecure (Stoumpos, Kitsios, & Talias, 2023; Mehrtak et al., 2021). AlQudah and Al-Shboul (2021), reviewing 58 empirical studies (2015–2021), found TAM-based models accounted for over 60% of healthcare technology-acceptance research, with perceived usefulness consistently the strongest predictor of use.

2.2 Technology-Organisation-Environment (TOE) Framework and UTAUT

The TOE framework (Tornatzky & Fleischer, 1990) situates technology use within technological, organisational, and environmental contexts, capturing institutional factors such as ICT budget, managerial commitment, and regulatory environment (Shahbaz & Khan, 2022; Bada & Bamigboye, 2022). The Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003) further highlights Facilitating Conditions — technical support, training, and infrastructure — as decisive in low-resource settings; Tilahun and Fritz (2019) found that unreliable electricity and internet connectivity, rather than perceived usefulness, were the primary constraints on EMR adoption in Ethiopian healthcare facilities, a finding directly relevant to the Nigerian context.

2.3 Cloud Computing, Data Security, and Disaster Preparedness in Healthcare

Cloud service models (Infrastructure-, Platform-, and Software-as-a-Service) and deployment models (public, private, community, and hybrid) each carry distinct security, cost, and control trade-offs (Alassafi, 2021). For healthcare specifically, the Hybrid Cloud Model — combining on-premises operational servers with a redundant, compliant public- or private-cloud backup layer — is widely regarded as the most pragmatic approach in developing-country settings (Sultan, Mansour, & Al-Qirim, 2023).

Data security in cloud-hosted EMR systems is commonly evaluated against the CIA triad. Confidentiality is enforced through AES-256 encryption at rest, TLS in transit, multi-factor authentication (MFA), and role-based access control (RBAC) (Sahi, Abbas, & Khalid, 2021). Integrity relies on cryptographic hashing and immutable audit logs (Hasan, Islam, & Razzak, 2022), while availability is underpinned by redundant, geographically distributed data centres governed by service-level agreements. Notwithstanding these technical controls, human error and weak authentication practice remain leading causes of breach (Mehrtak et al., 2021).

Cloud computing strengthens disaster preparedness through automated, continuous backup that minimises Recovery Point Objectives (RPO); geographical redundancy that protects against localised disaster; Disaster-Recovery-as-a-Service (DRaaS), which reduces Recovery Time Objectives (RTO) from days to hours; and immutable backups that resist ransomware (Alzahrani et al., 2022; Sultan et al., 2023). Barriers to cloud storage utilization in developing-country healthcare settings are well documented and include inadequate internet bandwidth, unreliable power, high subscription cost, shortage of skilled IT personnel, regulatory uncertainty around data sovereignty, and vendor lock-in (Shahbaz & Khan, 2022;

Eze et al., 2021; Hasan et al., 2022). In Nigeria, compliance obligations under the Nigeria Data Protection Act (NDPA, 2023) add a further layer of institutional caution around cross-border data transfer.

Collectively, the reviewed literature establishes strong theoretical and empirical grounds to expect a positive relationship between cloud storage utilization and both data security and disaster preparedness, while also predicting that infrastructural and human-capacity constraints will substantially moderate the pace of utilization in the Nigerian public hospital context. This study tests these expectations empirically at IBB Specialist Hospital, Minna.

3. MATERIALS AND METHODS

3.1 Research Design and Setting

A descriptive, cross-sectional survey design was adopted, complemented by the development of a proposed hybrid-cloud system architecture. The study was conducted at Ibrahim Badamasi Babangida (IBB) Specialist Hospital, a public tertiary healthcare facility in Minna, Niger State, North-Central Nigeria, with an approximate bed capacity of 200 and a workforce of 520 healthcare professionals.

3.2 Population, Sample, and Sampling Technique

The study population comprised 520 eligible staff, proportionally distributed across five functional cadres: clinical/medical staff, nursing staff, Health Information Management (HIM) professionals, information technology (IT) personnel, and administrative staff (Table 1). The sample size was determined using Cochran's formula, $n_0 = Z^2pq/e^2$, at a 95% confidence level, 5% margin of error, $p = 0.50$, and $q = 0.50$. Thus, $n_0 = (1.96)^2(0.50)(0.50)/(0.05)^2 = 384.16$. Applying the finite population correction for the population of 520 gave $n_e = 384.16/[1 + (384.16-1)/520] = 221.19$, approximately 221 respondents. An 18% allowance for potential non-response was subsequently applied, giving $n_{aej} = 221.19/(1-0.18) = 269.74$, which was rounded to 270 staff. The 18% allowance was informed by evidence from comparable Nigerian healthcare-worker surveys, with Nwosu et al. (2021) reporting approximately 20.5% non-response among healthcare workers in a Nigerian hospital and Ogoina et al. (2015) reporting approximately 24% non-response among healthcare workers in two Nigerian tertiary hospitals.

A proportionate stratified sampling technique was employed, with the five professional cadres serving as strata. The sample was proportionately allocated using $n_h = (N_h/N) \times n$, resulting in 80 clinical/medical staff, 90 nursing staff, 40 HIM professionals, 25 IT personnel, and 35 administrative staff, giving a total sample of 270 respondents. Within each stratum, eligible staff were selected until the required number for each cadre was attained. This approach ensured adequate representation of the different professional groups involved in the study.

Table 1. Population and sample distribution by professional cadre.

Department/Unit	Population	Sample Size	Percentage (%)
Clinical/Medical Staff	154	80	29.6
Nursing Staff	173	90	33.3
Health Information Management	77	40	14.8
Information Technology	48	25	9.3
Administration	68	35	13.0
Total	520	270	100.0

Source: Field survey (2026).

3.3 Research Instrument, Validity, and Reliability

Data were collected using a structured, self-administered instrument, the Cloud Server Adoption, Data Security, and Disaster Preparedness Questionnaire (CSADSQ). Section A captured demographic information (gender, department, educational qualification, years of experience). Section B comprised 20 statements on a 5-point Likert scale (Strongly Agree = 5 to Strongly Disagree = 1), organised into four sub-scales of five items each: current level of cloud server utilization, influence on data security, contribution to disaster preparedness, and synchronisation/implementation challenges.

Content validity was established through expert panel review (Content Validity Index = 0.89), and construct validity through exploratory factor analysis, with all items loading above 0.50 on their intended factors. A pilot study of 20 respondents at a comparable tertiary facility produced acceptable-to-good internal consistency across sub-scales (Table 2).

Table 2. Reliability (Cronbach's alpha) of the CSADSQ instrument.

Section	Cronbach's Alpha	Reliability Level
Cloud Server Utilization	0.79	Acceptable
Data Security	0.85	Good
Disaster Preparedness	0.83	Good
Implementation Challenges	0.80	Acceptable
Overall Instrument	0.82	Good

3.4 Data Collection Procedure

Questionnaires were administered face-to-face by the researcher and three trained research assistants over a four-week period, following institutional ethical approval and informed consent from all participants. Anonymity and confidentiality were assured throughout.

3.5 Data Analysis

Data were analysed in SPSS version 25.0. Descriptive statistics (means, standard deviations, frequencies) summarised demographic characteristics and sub-scale responses; a mean score of 3.00 or above was interpreted as agreement. Inferential analysis comprised Pearson Product-Moment Correlation (PPMC), used to test the relationships between cloud storage utilization and data security (H_{01}) and between cloud storage utilization and disaster preparedness (H_{02}), and one-way Analysis of Variance (ANOVA) with Tukey's HSD post-hoc comparison, used to test for differences in perceived benefit across the five professional cadres (H_{03}). Statistical significance was set at $p < 0.05$.

3.6 Proposed Hybrid Cloud Architecture

In addition to the empirical survey, the study proposed a Hybrid Cloud Architecture for the hospital, comprising a physical layer (on-premises servers for daily low-latency clinical operations), a cloud layer (a public-cloud, NDPR-compliant region providing encrypted, geographically redundant backup and disaster recovery), and an automated real-time synchronisation mechanism linking the two via secure API calls, with AES-256 encryption at rest and TLS 1.3 in transit, and role-based access control (RBAC) with multi-factor authentication governing all access.

3.7 Ethical Considerations

Ethical clearance was obtained from the hospital management and the researcher's institutional review process. Participation was voluntary, informed consent was obtained from all respondents, and data were anonymised and stored on password-protected devices for academic research purposes only.

4. RESULTS

4.1 Response Rate and Demographic Characteristics

Of 270 questionnaires distributed, 250 were validly completed and returned, a response rate of 92.6%, exceeding the recommended 70% threshold for survey research (Table 3).

Table 3. Response rate by department.

Department	Distributed	Returned	Response Rate (%)
Clinical/Medical Staff	80	74	92.5
Nursing Staff	90	83	92.2
Health Information Management	40	37	92.5
Information Technology	25	23	92.0
Administration	35	33	94.3
Total	270	250	92.6

Of the 250 respondents, 145 (58%) were male and 105 (42%) female. Educational qualifications comprised OND/HND (6%), B.Sc./B.N.S./B.Med (48%), M.Sc./MBA (36%), and other postgraduate qualifications (10%). Departmental distribution was Clinical/Medical (29.6%), Nursing (33.2%), HIM (14.8%), IT (9.2%), and Administration (13.2%). By years of experience, 44% had 1–5 years, 38% had 6–10 years, and 18% had more than 10 years, reflecting the relatively young workforce typical of Nigerian public tertiary hospitals.

4.2 Current Level of Cloud Server Utilization

The grand mean for cloud server utilization was 2.88, below the 3.00 agreement threshold, indicating generally low utilization (Table 4). Ninety percent of respondents agreed that the hospital relies solely on physical servers for EMR data (mean = 4.53), while awareness of any cloud service (mean = 2.45), the existence of a clear utilization policy (mean = 2.30), adequacy of staff training (mean = 2.25), and sufficiency of internet connectivity for real-time transfer (mean = 2.85) were all rated below the agreement threshold.

Table 4. Current level of cloud server utilization. (Research Question 1)

Statement	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	SD
Hospital relies solely on physical servers for EMR data	65.0	25.0	5.0	3.0	2.0	4.53	0.82
Awareness of cloud computing services for data storage	10.0	15.0	20.0	35.0	20.0	2.45	1.31

Statement	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	SD
Clear policy guiding cloud technology utilization exists	5.0	10.0	25.0	40.0	20.0	2.30	1.15
Staff have received adequate training on cloud EMR	5.0	10.0	20.0	45.0	20.0	2.25	1.12
Internet connectivity supports real-time cloud transfer	15.0	20.0	25.0	30.0	10.0	2.85	1.25
Grand Mean						2.88	

4.3 Influence of Cloud Storage Utilization on Data Security

The grand mean for data security was 3.66 (Table 5). Respondents strongly agreed that cloud servers provide better encryption than physical servers (mean = 4.15) and that cloud storage utilization can guarantee patient confidentiality (mean = 4.00); however, 70% also agreed that cloud storage increases the risk of unauthorised access or hacking (mean = 4.00), and role-based access control was rated as poorly implemented (mean = 2.80). Forty-five percent of respondents believed the hospital had previously experienced a data breach or unauthorised access (mean = 3.35).

Table 5. Influence of cloud storage utilization on data security. (Research Question 2)

Statement	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	SD
Cloud storage increases risk of unauthorised access/hacking	40.0	30.0	15.0	10.0	5.0	4.00	1.05
Cloud servers provide better encryption than physical servers	45.0	35.0	10.0	5.0	5.0	4.15	0.95
Role-based access control is effectively implemented	15.0	25.0	20.0	30.0	10.0	2.80	1.20
Cloud utilization guarantees confidentiality/privacy of records	35.0	40.0	15.0	5.0	5.0	4.00	1.02
Hospital has experienced a data breach/unauthorised access	20.0	25.0	30.0	15.0	10.0	3.35	1.25
Grand Mean						3.66	

4.4 Contribution of Cloud Servers to Disaster Preparedness

The grand mean for disaster preparedness was 3.80 (Table 6). Eighty-five percent of respondents agreed that cloud storage ensures quick recovery after a system crash (mean = 4.35), and 90% agreed patient data would be permanently lost in a disaster without cloud backup (mean = 4.25). However, only 15% of respondents confirmed that the hospital had a documented disaster recovery plan (mean = 2.20), the lowest-rated item across the entire instrument.

Table 6. Contribution of cloud servers to disaster preparedness. (Research Question 3)

Statement	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	SD
Hospital has a documented disaster recovery plan for EMR	5.0	10.0	15.0	50.0	20.0	2.20	1.10
Cloud storage ensures quick recovery after system crash	60.0	25.0	10.0	3.0	2.0	4.35	0.85
Local physical servers are frequently lost/damaged	45.0	35.0	15.0	3.0	2.0	4.15	0.90
Cloud backup provides geographical redundancy	40.0	35.0	15.0	5.0	5.0	4.05	0.95
Patient data would be permanently lost without cloud backup	55.0	30.0	10.0	3.0	2.0	4.25	0.88
Grand Mean						3.80	

4.5 Synchronisation and Implementation Challenges

The grand mean for implementation challenges was 3.58 (Table 7). High cost of cloud subscription and bandwidth (mean = 4.15) and lack of technical skills among healthcare workers (mean = 4.00) were the most strongly endorsed barriers, followed by NDPR compliance concerns (mean = 3.75) and vendor lock-in (mean = 3.50). Only 25% of respondents agreed that synchronisation between physical and cloud servers was currently seamless (mean = 2.50).

Table 7. Synchronisation and implementation challenges. (Research Question 4)

Statement	SA (%)	A (%)	N (%)	D (%)	SD (%)	Mean	SD
Synchronisation between physical and cloud servers is seamless	10.0	15.0	20.0	35.0	20.0	2.50	1.15
High cost of cloud subscription/bandwidth is a major barrier	45.0	35.0	15.0	3.0	2.0	4.15	0.90
Healthcare workers resist cloud EMR due to lack of skills	40.0	30.0	20.0	5.0	5.0	4.00	1.00
Concerns about NDPR hinder cloud utilization	30.0	35.0	20.0	10.0	5.0	3.75	1.05
Vendor lock-in is a significant concern	25.0	30.0	25.0	15.0	5.0	3.50	1.10
Grand Mean						3.58	

4.6 Test of Hypotheses

Hypothesis One tested the relationship between cloud server utilization and data security. The Pearson Product-Moment Correlation revealed a strong, positive, and statistically significant relationship ($r = 0.82$, $n = 250$, $p = 0.001$), leading to rejection of the null hypothesis (Table 8).

Table 8. Pearson correlation — cloud server utilization and data security. (H_{01})

Statistic	Value
Pearson correlation coefficient (r)	0.82
Sample size (n)	250
p-value	0.001
Significance level (α)	0.05
Critical value	0.195
Decision	H_0 rejected

Hypothesis Two tested the relationship between cloud server utilization and disaster preparedness. A strong, positive, statistically significant relationship was found ($r = 0.79$, $n = 250$, $p = 0.002$), and the null hypothesis was rejected (Table 9).

Table 9. Pearson correlation — cloud server utilization and disaster preparedness. (H_{02})

Statistic	Value
Pearson correlation coefficient (r)	0.79
Sample size (n)	250
p-value	0.002
Significance level (α)	0.05
Critical value	0.195
Decision	H_0 rejected

Hypothesis Three tested for differences in perceived benefit of cloud utilization across the five professional cadres using one-way ANOVA. A statistically significant difference was found ($F(4,245) = 4.56$, $p = 0.012$), leading to rejection of the null hypothesis (Table 10).

Table 10. One-way ANOVA — perceived benefit of cloud utilization by professional cadre. (H_{03})

Source of Variation	SS	df	MS	F	F-crit	p
Between Groups	45.67	4	11.42	4.56	2.38	0.012
Within Groups	612.33	245	2.50			
Total	658.00	249				

Post-hoc Tukey's HSD comparisons showed that IT personnel (mean = 4.25) and HIM professionals (mean = 3.95) perceived significantly higher benefits than clinical staff (mean = 3.10), nursing staff (mean = 3.15), and administrative staff (mean = 3.20), while differences among clinical, nursing, and administrative cadres, and between IT and HIM staff, were not significant (Table 11).

Table 11. Post-hoc comparison of professional cadres. (Tukey's HSD)

Comparison	Mean Difference	p	Significant?
IT vs Clinical	1.15	0.003	Yes
IT vs Nursing	1.10	0.005	Yes
IT vs Administration	1.05	0.008	Yes
IT vs HIM	0.30	0.412	No
HIM vs Clinical	0.85	0.015	Yes
HIM vs Nursing	0.80	0.022	Yes
HIM vs Administration	0.75	0.031	Yes
Clinical vs Nursing	-0.05	0.892	No
Clinical vs Administration	-0.10	0.756	No
Nursing vs Administration	-0.05	0.845	No

4.7 Correlation Matrix of Study Variables

A full correlation matrix (Table 12) confirmed that cloud storage utilization correlated positively with both data security ($r = 0.820$) and disaster preparedness ($r = 0.790$), that data security and disaster preparedness were themselves strongly correlated ($r = 0.750$), and that implementation challenges correlated negatively with all three ($r = -0.650$ to -0.580), indicating that utilization barriers directly impede the realisation of security and resilience benefits.

Table 12. Correlation matrix of study variables.

Variable	Cloud Utilization	Data Security	Disaster Preparedness	Implementation Challenges
Cloud Utilization	1.000			
Data Security	0.820**	1.000		
Disaster Preparedness	0.790**	0.750**	1.000	
Implementation Challenges	-0.650**	-0.580**	-0.610**	1.000

$^{**}p < 0.01$ (two-tailed).

4.8 Sub-group Analyses

An independent-samples t-test found no statistically significant gender differences across the four composite variables (all $p > 0.05$; Table 13). Respondents with higher educational qualifications and greater years of experience reported consistently more favourable perceptions of cloud security and disaster-preparedness benefits (Tables 14 and 15).

Table 13. Comparison of male and female respondents across study variables.

Variable	Male Mean (SD)	Female Mean (SD)	t	p
Cloud Utilization	2.85 (0.65)	2.92 (0.70)	-0.85	0.396
Data Security	3.62 (0.78)	3.71 (0.82)	-0.92	0.358
Disaster Preparedness	3.76 (0.80)	3.85 (0.85)	-0.95	0.343
Implementation Challenges	3.55 (0.72)	3.62 (0.75)	-0.78	0.436

Table 14. Cloud computing perception by years of experience.

Years of Experience	Cloud Security Grand Mean	SD	n
1–5 years	3.55	0.95	110
6–10 years	3.72	0.88	95
Above 10 years	3.80	0.82	45

Table 15. Cloud computing perception by educational qualification.

Educational Qualification	Cloud Utilization Mean	Data Security Mean	Disaster Preparedness Mean
OND/HND	2.40	3.20	3.35
B.Sc./B.N.S./B.Med	2.75	3.55	3.65
M.Sc./MBA	3.15	3.85	3.95

Educational Qualification	Cloud Utilization Mean	Data Security Mean	Disaster Preparedness Mean
Others	2.90	3.60	3.70

4.9 Qualitative Observations

Open-ended responses converged on four recurring themes: (i) fear of data loss, chiefly among clinical staff who associated cloud storage with heightened hacking risk, notwithstanding its technically superior encryption; (ii) infrastructure deficit, particularly inadequate internet bandwidth, which IT staff reported caused prolonged or failed cloud backups; (iii) limited management commitment, reflected in the absence of a dedicated cloud-computing budget or formal utilization policy; and (iv) success stories from other Nigerian teaching hospitals with dedicated fibre-optic connectivity and stronger management commitment to ICT, cited as evidence that cloud storage utilization is achievable within the Nigerian context.

5. DISCUSSION

This study set out to evaluate how cloud storage utilization influences data security and disaster preparedness in the EMR system of a Nigerian public tertiary hospital. The central finding is a marked paradox between perception and practice: respondents overwhelmingly recognised the security and resilience advantages of cloud computing, yet actual utilization remained critically low, with 90% of respondents confirming continued sole reliance on physical servers. This mirrors Bada and Bamigboye's (2022) finding that 78% of Nigerian military hospitals relied exclusively on physical servers, and contrasts with the substantially higher cloud-adoption rates (65%) reported among Saudi Arabian hospitals by Alassafi (2021), a gap plausibly attributable to differences in internet infrastructure quality and ICT budget.

The strong, statistically significant correlations between cloud storage utilization and both data security ($r = 0.82$) and disaster preparedness ($r = 0.79$) empirically substantiate the theoretical expectation, drawn from the CIA-triad and business-continuity literatures, that cloud infrastructure meaningfully strengthens both dimensions of institutional resilience (Keshta & Alzahrani, 2021; Alzahrani et al., 2022). However, the coexistence of high mean scores on the perceived risk of hacking (mean = 4.00) alongside high mean scores on superior encryption (mean = 4.15) reflects the well-documented phenomenon whereby perceived security risk, rather than the objective technical merits of cloud infrastructure, remains the dominant psychological barrier to utilization among healthcare professionals (Mehrtak et al., 2021). This finding extends the extended-TAM literature by demonstrating that the perception-practice paradox persists even where respondents simultaneously acknowledge the technology's superiority, suggesting that risk perception operates somewhat independently of usefulness beliefs in this context.

The significant ANOVA result, and the post-hoc pattern in which IT and HIM staff perceived markedly greater benefit than clinical, nursing, and administrative cadres, is consistent with TAM's prediction that users with higher technical proficiency exhibit higher perceived usefulness (AlQudah & Al-Shboul, 2021). Practically, this indicates that utilization strategies cannot rely on a single, undifferentiated communication or training approach; clinical and administrative staff require targeted, non-technical framing that addresses risk perception directly, while IT and HIM staff can act as internal champions.

The near-absence of a documented disaster recovery plan (only 15% agreement) is arguably the most operationally urgent finding, since it indicates that even where cloud backup exists, the institution lacks a structured protocol for invoking it. This is consistent with Mugauri et al.'s (2021) sub-Saharan African review, which found only 22% of surveyed facilities had a documented EMR disaster recovery plan, suggesting this is a systemic regional deficit rather than an institution-specific failing. The negative correlations between implementation challenges and both outcome variables reinforce that cost, bandwidth, skills, and regulatory uncertainty are not merely utilization friction but active barriers to realised security and resilience benefit, underscoring the urgency of addressing them directly rather than treating them as secondary concerns.

6. CONCLUSION

This study evaluated the influence of cloud storage utilization on data security and disaster preparedness within the EMR system of IBB Specialist Hospital, Minna, and found that although cloud storage utilization remains critically low, with the hospital's EMR data still overwhelmingly dependent on vulnerable, on-premises physical servers, cloud storage utilization is strongly and significantly associated with improved data security and improved disaster preparedness where it has been implemented. Healthcare workers across all cadres recognise the CIA-triad and business-continuity advantages of cloud computing in principle, but utilization is constrained by high subscription and bandwidth costs, limited technical skills, weak institutional policy, and regulatory uncertainty around the Nigeria Data Protection Regulation, while a significant cadre-based perception gap separates technically proficient IT and HIM staff from clinical, nursing, and administrative staff. Taken together, these findings indicate that the barrier to stronger data security and disaster resilience at the hospital is not a lack of awareness or of demonstrated benefit, but a combination of infrastructural, financial, policy, and human-capacity constraints that must be addressed concurrently. A Hybrid Cloud Architecture, retaining local servers for daily low-latency clinical operations while migrating backup and disaster recovery functions to a secure, NDPR-compliant cloud environment, offers a pragmatic and empirically supported pathway for this and comparable Nigerian public healthcare institutions to close the gap between recognised benefit and actual practice.

7. Recommendations

Based on the findings, the following five recommendations are made, each specifying the responsible party and the corresponding action:

1. Hospital Management (Chief Medical Director and Head of Administration): should approve and fund a phased transition to a Hybrid Cloud Architecture, prioritising migration of backup, archival, and disaster-recovery functions to a secure, NDPR-compliant cloud provider (e.g., a Nigeria-region deployment of Microsoft Azure or Amazon Web Services), while retaining local servers for daily clinical operations.

2. Hospital IT Department, in collaboration with Health Information Management (HIM) unit: should draft and operationalise a formal cloud security and data-governance policy addressing encryption standards, role-based access control (RBAC), multi-factor authentication, and explicit NDPR-compliance protocols, to be approved by hospital management within the first implementation phase.

3. Hospital Management and Human Resources/Training Unit: should institute mandatory, continuous, cadre-differentiated training programmes — technical training for IT/HIM staff and non-technical, risk-focused awareness sessions for clinical, nursing, and administrative staff — to close the demonstrated perception gap and correct misconceptions about cloud security risk.

4. Hospital Management, in partnership with Internet Service Providers and the State Ministry of Health: should invest in redundant, high-speed internet connectivity (fibre-optic primary with wireless backup) to eliminate synchronisation failures between physical and cloud servers and enable real-time data replication.

5. Hospital IT Department and HIM Unit: should formulate and periodically test a standardised, documented Disaster Recovery Plan (DRP) with explicit Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), conducting regular simulation drills, and should select cloud vendors offering open APIs and standard data-export formats to avoid vendor lock-in.

8. Implications of the Study

The findings carry several practical and policy implications. First, the hospital's continued near-total dependence on physical servers, combined with the demonstrated statistical association between cloud storage utilization and both security and disaster resilience, indicates a tangible, quantifiable institutional risk of catastrophic and irrecoverable data loss in the event of hardware failure, cyber-attack, fire, or flood. Second, the significant cadre-based perception gap implies that technology-utilization initiatives in similar institutions must be accompanied by differentiated change-management strategies rather than a uniform rollout, since clinical and administrative staff constitute both the largest workforce segments and the least technically confident. Third, the identified barriers (cost, bandwidth, skills, and regulatory uncertainty) are structural rather than attitudinal, implying that policy-level interventions — such as national ICT-infrastructure investment, sector-specific cloud-computing guidelines from the Federal Ministry of Health, and clarified NDPR compliance pathways for cloud vendors — are necessary complements to institution-level action. Fourth, for healthcare informatics research and practice more broadly, the study demonstrates that recognising a technology's benefits is not sufficient to drive utilization in resource-constrained public-sector settings; utilization strategy must directly target the specific infrastructural and psychological barriers identified.

9. Contributions to Knowledge

1. Contextual application of an extended Technology Acceptance Model (TAM) to cloud EMR utilization in a Nigerian tertiary hospital, providing empirical evidence that perceived security risk, rather than perceived usefulness alone, is the dominant barrier among clinical staff.
2. Quantified evidence of a clinical-technical perception gap, using ANOVA and Tukey's HSD post-hoc analysis, that highlights an organisational silo in healthcare technology utilization and the need for cadre-differentiated educational interventions.
3. Empirical validation of the necessity of a Hybrid Cloud model, rather than a fully cloud-based Software-as-a-Service approach, in infrastructurally constrained developing-country healthcare settings, offering a pragmatic architectural framework applicable beyond the case institution.

4. Integrated empirical linkage of data security (the CIA triad) and disaster preparedness (business continuity) as jointly, and significantly, predicted outcomes of cloud storage utilization, together with an operational proposed system architecture (hybrid physical–cloud layer, synchronisation mechanism, and STRIDE-based threat model) that translates the survey findings into an actionable technical design.

10. Limitations of the Study

This study has several limitations. First, it relies on self-reported perceptions rather than objective technical audit of the hospital's infrastructure, and is therefore subject to potential recall and social-desirability bias, notwithstanding efforts to ensure anonymity and neutral question wording. Second, the single-institution case-study design, while offering depth, limits the generalisability of findings to other Nigerian tertiary hospitals with differing resource profiles; the findings are most directly applicable to public tertiary hospitals with comparable organisational structure and constraints. Third, the cross-sectional design captures a single point in time and cannot establish causality or track the evolution of utilization over time. Fourth, the proposed hybrid-cloud architecture reflects the current state of cloud-computing technology and hospital requirements and may require revision as both evolve. Future longitudinal, multi-site studies incorporating objective infrastructure audits are recommended to build on these findings.

Author Contributions

Gwarjiko Usman Abdulrahman: Conceptualisation, methodology, investigation, formal analysis, data curation, writing — original draft, writing — review and editing. Adeojo Michael Babatunde: Supervision, conceptualisation, validation, writing — review and editing. S. A. Jimoh: Co-supervision, methodology review, validation, writing — review and editing. All authors read and approved the final manuscript.

Acknowledgement

The authors thank the management, clinical, nursing, Health Information Management, information technology, and administrative staff of Ibrahim Badamasi Babangida Specialist Hospital, Minna, for their participation in and support of this study, and the Department of Computer Science, Achievers University, Owo, for institutional support during the conduct of the research.

Conflict of Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Source of Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The study was self-funded by the authors.

Data Availability Statement

The datasets generated and/or analysed during the current study are available from the corresponding author on reasonable request, subject to institutional ethical approval and participant confidentiality safeguards.

Ethical Approval

This study was conducted in accordance with institutional ethical guidelines. Ethical approval and management permission were obtained from Ibrahim Badamasi Babangida Specialist Hospital, Minna, and informed consent was obtained from all individual participants included in the study.

REFERENCES

1. Adebayo, O. T., Ogunkeye, O. O., & Bello, A. M. (2023). Digital health transformation in Nigerian tertiary hospitals: Challenges and opportunities for cloud integration. Journal of Health Informatics in Developing Countries, 17(1), 45–58.
2. Adler-Milstein, J., Aggarwal, N., & Holmgren, A. J. (2021). The landscape of electronic health record implementation globally: Progress and persistent hurdles. Health Affairs, 40(7), 1088–1096.
3. Ahmadi, M., Rezaei, M., & Valinejadi, A. (2022). Impact of Electronic Medical Record systems on healthcare quality and clinical workflow efficiency: A systematic review. International Journal of Medical Informatics, 158, 104671.
4. Alassafi, M. O. (2021). Success indicators for cloud computing utilisation in healthcare organisations. [Journal article].
5. Al-Maroof, R. S., Alhumaid, K., & Akour, I. A. (2021). Cloud computing adoption in healthcare environments: A post-pandemic strategy for continuous operation. Computers in Human Behavior Reports, 4, 100122.

6. AlQudah, A. A., & Al-Shboul, M. (2021). Technology acceptance in healthcare: A systematic review of the Technology Acceptance Model. [Journal article].
7. Alzahrani, A. A., Alalwan, J. A., & Sitaram, P. (2022). Cloud-based disaster recovery planning for healthcare infrastructure: Ensuring high availability and business continuity. IEEE Access, 10, 31200–31215.
8. Babar, M., Khan, S. U., & Rashid, N. (2023). Scalable big data storage management for smart healthcare systems using hybrid cloud architectures. Future Generation Computer Systems, 141, 210–225.
9. Bada, A. A., & Bamigboye, O. B. (2022). Assessment of information security in Nigerian military hospitals. [Journal article].
10. Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.
11. Eze, S. C., Chinedu-Eze, V. C., & Okike, A. O. (2021). Critical factors influencing cloud computing adoption in sub-Saharan African healthcare organisations. Information Technology for Development, 27(3), 520–545.
12. Garg, N., & Sharma, S. (2023). Availability and fault tolerance in cloud-based Electronic Health Record systems. Journal of Systems Architecture, 134, 102789.
13. Hasan, M. K., Islam, S., & Razzak, M. A. (2022). Cybersecurity mechanisms for protecting cloud-hosted electronic medical records against data breaches. Computers & Security, 115, 102630.
14. Hassan, R., et al. (2022). Vendor lock-in and cloud migration challenges in public healthcare institutions. [Journal article].
15. Keshta, I., & Alzahrani, A. (2021). Security and privacy of electronic health records: Concerns and challenges. Egyptian Informatics Journal, 22(2), 177–183.
16. Kumar, A., & Singh, A. K. (2022). Cloud computing in healthcare: Architectural trends, storage security, and open challenges. Journal of Network and Computer Applications, 202, 103365.
17. Mehrtak, M., et al. (2021). Security challenges and solutions using healthcare cloud computing: A systematic review. Informatics in Medicine Unlocked, 23, 100530.
18. Mugauri, C., et al. (2021). Systematic review of electronic health records adoption in sub-Saharan Africa. BMC Medical Informatics and Decision Making, 21, 220.
19. Nigeria Data Protection Act [NDPA]. (2023). Nigeria Data Protection Commission (NDPC) Regulatory Framework. Federal Republic of Nigeria.

20. Nwosu, A. D. G., Ossai, E., Onwuasoigwe, O., Ezeigweneme, M., & Okpamen, J. (2021). Burnout and presenteeism among healthcare workers in Nigeria: Implications for patient care, occupational health and workforce productivity. Journal of Public Health Research, 10(1). https://doi.org/10.4081/jphr.2021.1900
21. Nyangena, J. M., Kimwele, M. W., & Okeyo, G. O. (2022). Vulnerabilities of on-premises health record systems in developing nations: The case for cloud migration. BMC Medical Informatics and Decision Making, 22(1), 114.
22. Ogoina, D., Pondei, K., Adetunji, B., Chima, G., Isichei, C., & Gidado, S. (2015). Knowledge, attitude and practice of standard precautions of infection control by hospital workers in two tertiary hospitals in Nigeria. Journal of Infection Prevention, 16(1), 16–22. https://doi.org/10.1177/1757177414558957
23. Ramani, V., & Balasubramanian, R. (2021). Attribute-based encryption for secure sharing of electronic health records over cloud. [Journal article].
24. Sahi, M. A., Abbas, H., & Khalid, A. (2021). Privacy and security preservation in cloud-based health information systems: A survey. IEEE Access, 9, 41520–41538.
25. Shahbaz, S., & Khan, R. (2022). Extended Technology Acceptance Model for cloud computing adoption in healthcare organisations. [Journal article].
26. Stoumpos, A. I., Kitsios, F., & Talias, M. A. (2023). Digital transformation in healthcare: Technology acceptance and its applications. International Journal of Environmental Research and Public Health, 20(4), 3407.
27. Sultan, K. A., Mansour, M. A., & Al-Qirim, N. (2023). Evaluating business continuity and disaster recovery mechanisms in cloud-enabled health centres. International Journal of Information Management, 68, 102580.
28. Tilahun, B., & Fritz, F. (2019). Comprehensive evaluation of electronic medical record system use and user satisfaction at five low-resource setting hospitals in Ethiopia. JMIR Medical Informatics, 3(2), e22.
29. Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.
30. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.
31. World Bank. (2024). Digital Infrastructure Development in Sub-Saharan Africa: Accelerating Healthcare Access. World Bank Group Reports.
32. World Health Organization [WHO]. (2023). Global Strategy on Digital Health 2020–2025. World Health Organization Guidelines.