Patients' Perceptions of Electronic Medical Record Confidentiality in Primary Care: A Cross-Sectional Study

Shona'a Surya Alay'ya[1]*, Arifatun Nisaa[2], Julia Pertiwi[2]

[1]Medical Records and Health Information Study Program, Faculty of Public Health and Health Sciences, University Veteran Bangun Nusantara Sukoharjo, Indonesia.
[2]Records and Health Information Study Program, Faculty of Public Health and Health Sciences, University Veteran Bangun Nusantara Sukoharjo, Indonesia.

Email: shonaaalayya@gmail.com*

Submitted: 23 February 2026 Reviewed: 28 July 2026 Accepted: 11 August 2026

ABSTRACT

Background: Electronic Medical Records (EMRs) have become an essential component of digital healthcare transformation, but their implementation also raises concerns regarding the confidentiality and protection of patients' personal health information. This study aimed to analyze patients' perceptions of EMR data confidentiality at Baki Community Health Center based on five dimensions: knowledge and understanding, service experience, trust in healthcare professionals, privacy policies and education, and data confidentiality. **Methods:** This descriptive quantitative study used a cross-sectional design involving 96 outpatients selected through quota sampling. The questionnaire consisted of 18 Likert-scale items distributed across five dimensions and was adapted from previous studies concerning electronic medical record confidentiality, health information privacy, patient trust, service experience, privacy policies, and data protection. The instrument was pilot-tested on 30 respondents. Item validity was assessed using Pearson Product-Moment correlation, while internal consistency was evaluated using Cronbach's Alpha. Descriptive statistics were used to present frequencies, percentages, and responses across the five dimensions. **Results:** All 18 items showed acceptable validity (item-total correlations 0.584–0.824, above the 0.361 critical value), with overall Cronbach's Alpha of 0.887 and dimension range 0.798–0.833, indicating satisfactory internal consistency. Respondents generally reported positive perceptions of EMR confidentiality across all five dimensions, particularly on protection of personal health information, though awareness of privacy policies and confidentiality rights still needs improvement. **Conclusion:** Patients at Baki Community Health Center generally reported positive perceptions regarding EMR data confidentiality. However, these findings reflect patients' perceptions and should not be interpreted as objective evidence of the technical or organizational security performance of the EMR system. Strengthening patient education and communication regarding privacy policies, data access, and confidentiality rights is recommended to improve patients' understanding and confidence in EMR management.

Keywords: Confidentiality; Electronic Health Records; Patients; Primary Health Care; Privacy

INTRODUCTION

The rapid advancement of information technology has accelerated the digital transformation of healthcare services through the implementation of Electronic Medical Records (EMRs). In Indonesia, the implementation of EMRs has been mandated for all healthcare facilities since 2023 as part of the national strategy to improve healthcare quality, service efficiency, and health information integration [3]. EMRs enable healthcare providers to store, retrieve, and manage patient information electronically, thereby facilitating timely clinical decision-making, improving continuity of care, and supporting evidence-based healthcare delivery [4–8]. Despite these advantages, digitalization also introduces significant challenges related to information security and the confidentiality of patients' personal health information. Personal information contained in EMRs, including patient identity, medical history, laboratory results, diagnoses, and treatment records, must be protected from unauthorized access in accordance with the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 [2].

Community Health Centers (*Puskesmas*), as primary healthcare facilities, play a strategic role in delivering promotive, preventive, curative, and rehabilitative healthcare services. The implementation of EMRs in *Puskesmas* is expected to improve administrative efficiency, enhance data accuracy, facilitate information

exchange, and strengthen coordination among healthcare professionals [19,33]. However, successful implementation depends not only on technological readiness but also on patients' confidence that their personal health information is managed securely and confidentially. Maintaining the confidentiality of patient information is therefore essential for preserving public trust and ensuring the quality of healthcare services [15,27,32].

The confidentiality of EMR data is a shared responsibility between healthcare providers and patients. Healthcare professionals are required to ensure that patient information is accessed only by authorized personnel, while patients are encouraged to protect their personal credentials and avoid disclosing sensitive health information to unauthorized individuals [2,17,32]. Inadequate awareness regarding data protection may increase the risk of privacy breaches, unauthorized disclosure, and misuse of personal health information. Consequently, improving patients' understanding of health information confidentiality has become an important component of successful EMR implementation [9,10,28].

Patients' perceptions regarding EMR data confidentiality are influenced by multiple factors, including their knowledge of medical record confidentiality, previous experiences with healthcare services, trust in healthcare professionals, and their understanding of institutional privacy policies. Positive perceptions of data security are associated with increased trust, greater willingness to disclose accurate health information, and stronger engagement in healthcare services. Conversely, concerns regarding unauthorized access or misuse of health information may reduce patient trust and negatively affect healthcare utilization [11,13,20,23,29].

Several previous studies have emphasized the importance of protecting patient information within electronic health systems. Wulandari et al. reported that patients at Hidayah Boyolali Hospital generally demonstrated positive perceptions regarding EMR data confidentiality, which contributed to increased trust in healthcare services [35]. Likewise, studies on patient confidentiality have shown that effective legal protection and information security practices are fundamental to safeguarding patients' privacy rights and strengthening public confidence in digital healthcare systems [2,7,15,32]. Other studies have primarily examined legal frameworks, cybersecurity, interoperability, or technical aspects of EMR implementation, particularly within hospital settings [7,16–19,22,24].

State of the Art. Previous studies on electronic medical record confidentiality have predominantly focused on hospital settings, technical information security, legal protection, cybersecurity, and healthcare professionals' perspectives. Evidence regarding patients' perceptions of EMR confidentiality in primary healthcare settings remains comparatively limited. This distinction is important because patients' interactions with EMRs in primary healthcare may differ from those in hospitals in terms of service flow, patient characteristics, frequency of visits, and direct communication with healthcare personnel. In addition, previous studies have often examined confidentiality as a single concept or focused on specific aspects of privacy and security rather than examining patients' perceptions across multiple dimensions simultaneously. This study addresses this gap by examining patients' perceptions of EMR confidentiality in a primary healthcare setting through five complementary dimensions: knowledge and understanding, service experience, trust in healthcare professionals, privacy policies and education, and data confidentiality. These dimensions capture not only whether patients perceive their information as confidential, but also whether they understand confidentiality principles, experience secure and convenient services, trust healthcare professionals, and are aware of institutional privacy policies and their rights. Therefore, the study provides a more comprehensive patient-centered perspective on EMR confidentiality in primary healthcare [7,9–11,15,25,35].

Novelty. This study provides a comprehensive assessment of patients' perceptions of EMR data confidentiality within a primary healthcare setting by simultaneously evaluating five dimensions: knowledge and understanding, service experience, trust in healthcare professionals, privacy policies and education, and data confidentiality. Unlike previous studies that mainly investigated legal aspects, technical security, or hospital-based implementation, this study focuses on *Puskesmas*, thereby providing evidence that may support the development of patient-centered information security strategies in Indonesian primary healthcare facilities.

Therefore, this study aimed to analyze patients' perceptions of the importance of Electronic Medical Record data confidentiality at Baki Community Health Center based on five dimensions: knowledge and understanding, service experience, trust in healthcare professionals, privacy policies and education, and data confidentiality. The findings are expected to provide evidence-based recommendations for strengthening patient education, improving communication regarding privacy policies, and enhancing information security practices to support the secure and sustainable implementation of Electronic Medical Records in Indonesian primary healthcare facilities.

METHODS

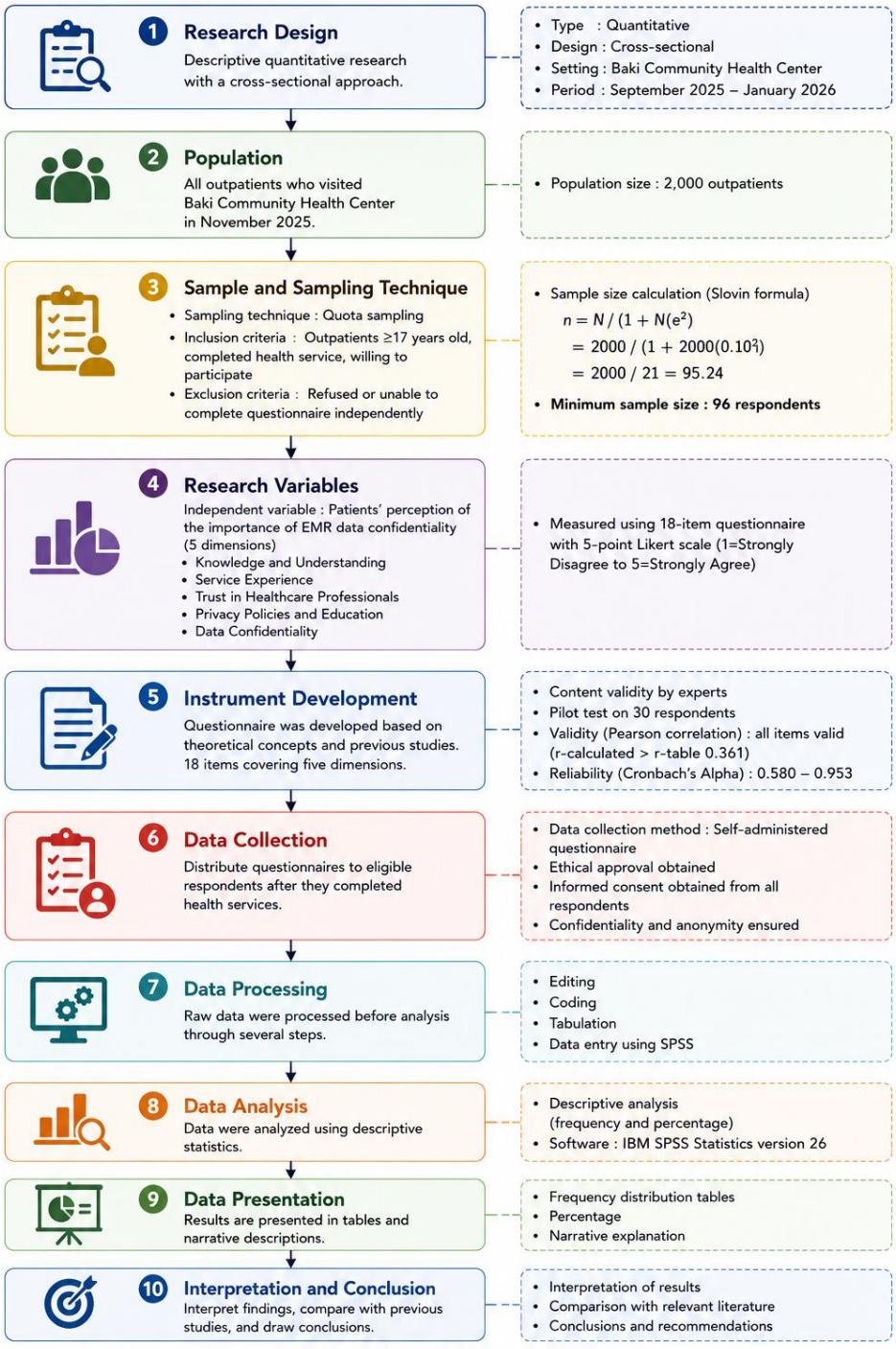

Figure 1. Research Method Flowchart

The research procedure conducted in this study is illustrated in Figure 1 (Research Method Flowchart). The study began with determining the research design, which employed a descriptive quantitative method with a cross-sectional approach. This design was selected to describe patients' perceptions regarding the importance of Electronic Medical Record (EMR) data confidentiality at a single point in time.

The study population consisted of 2,000 outpatients who visited Baki Community Health Center (Puskesmas Baki) during November 2025. The minimum sample size was calculated using the Slovin formula with a 10% margin of error, resulting in 96 respondents. Participants were selected using a quota sampling technique. Eligible

participants were outpatients aged 18 years or older who had completed their healthcare services and voluntarily agreed to participate in the study.

The research variables focused on patients' perceptions of the importance of EMR data confidentiality, which were measured through five dimensions: knowledge and understanding, service experience, trust in healthcare professionals, privacy policies and education, and data confidentiality.

Table 1. Item Validity and Internal Consistency of the Questionnaire by Dimension

Dimension	Item	Source/Adaptation	r-count range	Cronbach's Alpha
Knowledge and Understanding	4	Adapted from previous studies on EMR confidentiality and patient health information privacy	0.612–0.781	0.821
Service Experience	3	Adapted from previous studies on EMR service experience, usability, and perceived data security	0.645–0.793	0.806
Trust in Healthcare Professionals	4	Adapted from previous studies on patient trust, professional competence, and confidentiality practices	0.584–0.768	0.814
Privacy Policy and Education	4	Adapted from previous studies on privacy policies, patient rights, and health information education	0.603–0.752	0.798
Data Confidentiality	3	Adapted from previous studies on medical record confidentiality and electronic health information protection	0.671–0.824	0.833
Overall	**18**	—	0.584–0.824	0.887

The questionnaire consisted of 18 items distributed across five dimensions: knowledge and understanding (4 items), service experience (3 items), trust in healthcare professionals (4 items), privacy policy and education (4 items), and data confidentiality (3 items). The questionnaire items were adapted from previous studies addressing electronic medical record confidentiality, health information privacy, patient trust, service experience, privacy policies, and data protection. A pilot test was conducted among 30 respondents who met the study criteria but were not included in the main sample. Item validity was assessed using the Pearson Product-Moment correlation test. With 30 respondents, the critical r-value was 0.361 at a significance level of 5%. The item-total correlation coefficients ranged from 0.584 to 0.824, with all items exceeding the critical value, indicating acceptable item validity.

Reliability was assessed using Cronbach's Alpha. The Cronbach's Alpha coefficients for the five dimensions ranged from 0.798 to 0.833, while the overall questionnaire demonstrated a Cronbach's Alpha of 0.887. These results indicate satisfactory internal consistency of the questionnaire, measured on a five-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). The questionnaire was developed based on theoretical concepts, the Indonesian Ministry of Health Regulation Number 24 of 2022 concerning Electronic Medical Records, and previous studies related to information privacy, data security, and electronic health records. Prior to the main survey, the questionnaire was tested on 30 respondents to evaluate its validity and reliability. The validity test was performed using the Pearson Product-Moment correlation, while internal consistency was assessed using Cronbach's Alpha. All questionnaire items were found to be valid, and the reliability coefficients indicated acceptable to excellent internal consistency.

After data collection, the completed questionnaires underwent editing, coding, data entry, and tabulation. Data processing and statistical analysis were conducted using IBM SPSS Statistics version 26. Descriptive statistical analysis, including frequency distributions and percentages, was performed to describe respondents' characteristics and their perceptions regarding EMR data confidentiality across the five research dimensions.

The research findings were subsequently presented in the form of tables, figures, and narrative descriptions. The results were interpreted by comparing the findings with relevant theories, previous empirical studies, and applicable regulations concerning Electronic Medical Records and patient data confidentiality to formulate evidence-based conclusions and recommendations.

This study utilized a structured questionnaire as the primary research instrument. The study materials consisted of patients' responses regarding their perceptions of EMR data confidentiality. The research tool was a validated and reliable questionnaire developed from established theoretical frameworks and previous empirical

studies. The research design, sampling procedures, data collection techniques, measured variables, and statistical analyses were clearly defined to ensure methodological rigor and reproducibility.

Ethical principles were strictly observed throughout the research process. All respondents received adequate information regarding the objectives and procedures of the study before participating. Written informed consent was obtained from each respondent, and participation was entirely voluntary. Respondents were assured that all collected information would remain confidential, anonymous, and used exclusively for research purposes.

Ethical Considerations

This study employed a descriptive cross-sectional survey using an anonymous questionnaire and did not collect participants' names or other personally identifiable information. Participation was voluntary, and respondents were informed that all information provided would be kept confidential and used solely for research purposes. The study involved only the completion of a questionnaire regarding patients' perceptions of electronic medical record data confidentiality.

RESULTS

Characteristics of Respondents

Gender

Based on Table 2, among the 96 respondents included in this study, 26.0% were male, while 74.0% were female.

Table 2. Characteristics of Respondents by Gender

Gender	Frequency	Percentage (%)
Male	25	26,0
Female	71	74,0
Total	**96**	**100**

(Source: Primary data)

Age

Based on Table 3, the largest proportion of respondents was in the 18–30 years age group, accounting for 37.5% of the total respondents.

Table 3. Distribution of Respondents by Age

Age	Frequency	Percentage (%)
> 17 years	0	0
18-30 years	36	37,5
31-40 years	24	25,0
41-50 years	32	33,3
>50 years	4	4,2
Amount	**96**	**100**

Education

Based on Table 4, the majority of respondents had completed senior high school/vocational high school (SMA/SMK) as their highest level of education, accounting for 46.9% of the total respondents.

Table 4. Characteristics of Respondents Based on Education

Education	Frequency	Percentage (%)
SD/unfinished	23	24,0
SMP	6	6,3
SMA/SMK	45	46,9
D3	4	4,2
S1	18	18,8
>S1 (S2/S3)	0	0
Amount	**96**	**100**

A total of 96 respondents participated in this study. The demographic characteristics of the respondents are presented according to gender, age, and educational level. Based on Table 2, female respondents constituted the majority of the sample, accounting for 71 respondents (74.0%), while 25 respondents (26.0%) were male. Based on Table 3, the largest proportion of respondents was in the 18–30 years age group, comprising 36 respondents (37.5%). This was followed by respondents aged 41–50 years with 32 respondents (33.3%), 31–40 years with 24 respondents (25.0%), and those aged over 50 years with 4 respondents (4.2%). No respondents were younger than

18 years because the study only included participants aged 17 years and above who met the inclusion criteria. Based on Table 4, the highest educational attainment among respondents was senior high school/vocational high school (SMA/SMK), representing 45 respondents (46.9%). This was followed by respondents with elementary school or incomplete elementary education (23 respondents; 24.0%), bachelor's degree (18 respondents; 18.8%), junior high school (6 respondents; 6.3%), and diploma (D3) (4 respondents; 4.2%). None of the respondents had completed postgraduate education.

Item Analysis of the Knowledge and Understanding Dimensions

The Knowledge and Understanding dimension was analyzed to evaluate respondents' understanding of the functions and accessibility of Electronic Medical Records (EMRs). The distribution of responses to each questionnaire item is presented in terms of frequency and percentage, as shown in Table 5.

Table 5. Results of Item Analysis for the Knowledge and Understanding Dimension

Items	STS		TS		N		S		SS	
	n	%	n	%	n	%	n	%	n	%
Medical records store my health data.	0	0	6	6,3	25	26,0	41	42,7	24	25,0
I know who is allowed to access medical records.	0	0	15	15,6	20	20,8	34	35,4	27	28,1
The confidentiality of medical records must be maintained.	0	0	5	5,2	24	25,0	34	35,4	33	34,4
I am aware of the right to medical record confidentiality.	0	0	11	11,5	29	30,2	37	38,5	19	18,8

The Knowledge and Understanding dimension evaluated respondents' awareness of Electronic Medical Records (EMRs), including their understanding of health data storage, authorized access, medical record confidentiality, and patients' rights regarding confidentiality. The distribution of responses is presented in Table 5. Most respondents agreed or strongly agreed that medical records store their health information (67 respondents; 69.8%). Similarly, 61 respondents (63.5%) reported that they knew who was authorized to access medical records. Regarding the importance of maintaining medical record confidentiality, 67 respondents (69.8%) agreed or strongly agreed with the statement. Furthermore, 56 respondents (58.3%) indicated that they were aware of their right to medical record confidentiality.

Item Analysis of the Service Experience Dimension

The Service Experience dimension was analyzed to assess respondents' perceptions of the ease of use, security, and convenience of using Electronic Medical Records (EMRs). The distribution of respondents' responses to each statement item is presented in terms of frequency and percentage, as shown in Table 6.

Table 6. Item Analysis Results for the Service Experience Dimension

Items	STS		TS		N		S		SS	
	n	%	n	%	n	%	n	%	n	%
The Electronic Medical Record (EMR) service is easy and fast.	0	0	3	3,1	9	9,4	47	49,0	37	38,5
EMR gives me confidence that data is protected.	0	0	5	5,2	24	25,0	37	38,5	30	31,3
I feel safe providing personal data.	0	0	3	3,1	22	22,9	40	41,7	31	32,3

The Service Experience dimension assessed respondents' perceptions of the usability, convenience, and security of Electronic Medical Record services. The results are presented in Table 6. Most respondents perceived that EMR services were easy and fast to use, with 84 respondents (87.5%) expressing agreement or strong agreement. Regarding confidence in the security of personal health information, 67 respondents (69.8%) agreed or strongly agreed that EMRs adequately protected their data. Likewise, 71 respondents (74.0%) reported feeling safe when providing their personal information through the EMR system.

Item Analysis Results for the Trust in Healthcare Professionals Dimension

The Trust in Healthcare Professionals dimension was analyzed to assess respondents' level of trust in the competence and responsibility of healthcare professionals in managing electronic medical record (EMR) data.

The distribution of respondents' responses to each statement item is presented in terms of frequency and percentage, as shown in Table 7.

Table 7. Item Analysis Results for the Trust in Healthcare Professionals Dimension

Items	STS		TS		N		S		SS	
	n	%	n	%	n	%	n	%	n	%
I trust the staff to safeguard patient data.	0	0	0	0	12	12,5	50	52,1	34	35,4
The officer did not disclose health data.	0	0	3	3,1	17	17,7	43	44,8	33	34,4
The officer clearly explained the use of the data.	0	0	9	9,4	25	26,0	32	33,3	30	31,3
Competent personnel maintain confidentiality.	0	0	0	0	7	7,3	42	43,8	47	49,0

The Trust in Healthcare Professionals dimension assessed respondents' trust in healthcare personnel responsible for managing Electronic Medical Records. The response distribution is shown in Table 7. Most respondents expressed trust that healthcare professionals would safeguard patient information, with 84 respondents (87.5%) agreeing or strongly agreeing with the statement. A total of 76 respondents (79.2%) believed that healthcare professionals did not disclose patients' health information to unauthorized individuals. Regarding communication, 62 respondents (64.6%) agreed or strongly agreed that healthcare professionals clearly explained the use of patient data. Furthermore, 89 respondents (92.8%) agreed or strongly agreed that competent healthcare personnel maintained the confidentiality of medical records.

Item Analysis of Privacy Policy and Education Dimensions

The Privacy Policies and Education dimension was analyzed to assess respondents' perceptions of data protection policies and privacy education related to Electronic Medical Records (EMRs). The distribution of respondents' responses to each statement item is presented in terms of frequency and percentage, as shown in Table 8.

Table 8. Item Analysis Results for the Privacy Policy and Education Dimension

Items	STS		TS		N		S		SS	
	n	%	n	%	n	%	n	%	n	%
There is a data protection policy at the community health center.	0	0	11	11,5	30	31,3	47	49,0	8	8,3
The data is used only by authorized personnel.	0	0	5	5,2	24	25,0	50	52,1	17	17,7
There is education regarding patient confidentiality rights.	0	0	24	25,0	38	39,6	25	26,0	9	9,4
There is security oversight for Electronic Medical Records (EMR).	0	0	7	7,3	30	31,3	37	38,5	22	22,9

The Privacy Policy and Education dimension examined respondents' perceptions regarding institutional privacy policies, patient education, authorized access, and security monitoring related to Electronic Medical Records. The results are summarized in Table 8. Regarding the existence of a data protection policy at the Community Health Center, 55 respondents (57.3%) agreed or strongly agreed with the statement. A total of 67 respondents (69.8%) agreed or strongly agreed that patient data were accessible only to authorized personnel. Concerning education about patients' confidentiality rights, 34 respondents (35.4%) expressed agreement or strong agreement, while 38 respondents (39.6%) provided neutral responses. In addition, 59 respondents (61.4%) agreed or strongly agreed that security monitoring of Electronic Medical Records was implemented at the Community Health Center.

Item Analysis of the Data Confidentiality Dimension

The Data Confidentiality dimension was assessed to evaluate respondents' perceptions regarding the security and confidentiality of health information within the Electronic Medical Record (EMR) system. The distribution of respondents' responses is presented in terms of frequency and percentage, as shown in Table 9.

Table 9. Item Analysis Results for the Data Confidentiality Dimension

Items	STS		TS		N		S		SS	
	n	%	n	%	n	%	n	%	n	%
The confidentiality of the Electronic Medical Record (EMR) provides a sense of security.	0	0	4	4,2	18	18,8	43	44,8	31	32,3
Health data is not misused.	0	0	6	6,3	23	24,0	34	35,4	33	34,4
The confidentiality of the Electronic Medical Record (EMR) boosts trust.	2	2,1	5	5,2	17	17,7	32	33,3	40	41,7

The Data Confidentiality dimension assessed respondents' perceptions regarding the security of health information and the influence of confidentiality on trust in Electronic Medical Records. The results are presented in Table 9.

Most respondents perceived that the confidentiality of Electronic Medical Records provided a sense of security, with 74 respondents (77.1%) agreeing or strongly agreeing. Similarly, 67 respondents (69.8%) agreed or strongly agreed that their health information would not be misused. In addition, 72 respondents (75.0%) agreed or strongly agreed that maintaining the confidentiality of Electronic Medical Records increased their trust in digital healthcare services.

DISCUSSION

The findings indicate that respondents generally demonstrated a positive level of knowledge and understanding regarding the confidentiality of Electronic Medical Records (EMRs). Most participants recognized that medical records contain sensitive personal health information and acknowledged the importance of maintaining their confidentiality. This finding suggests that patients have developed a basic awareness of the role of EMRs in protecting personal health information, which is an essential prerequisite for the successful implementation of digital health systems. Adequate patient knowledge has been shown to increase confidence in healthcare services and encourage greater acceptance of health information technologies [2,5,10].

Despite these encouraging findings, a considerable proportion of respondents still expressed neutral responses regarding who is authorized to access medical records and regarding patients' rights to medical record confidentiality. These responses indicate that although patients understand the importance of confidentiality, many remain unfamiliar with the legal and operational mechanisms governing access to electronic medical records. Limited understanding of data governance may reduce patients' ability to exercise their rights concerning health information and weaken their confidence in digital healthcare systems [2,9,15].

The results are consistent with the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, which stipulates that healthcare facilities are responsible for ensuring the confidentiality, integrity, and availability of medical record information while also providing patients with adequate information regarding the use and protection of their personal health data [2]. Therefore, healthcare providers should not only implement appropriate technical safeguards but also improve patient education regarding confidentiality policies, access rights, and data protection procedures.

These findings are comparable to those reported by Wulandari et al., who found that hospital patients generally demonstrated positive perceptions of EMR confidentiality but still had limited understanding of data access mechanisms and privacy regulations [35]. Similar findings have also been reported internationally, where patient knowledge regarding electronic health information remains an important determinant of trust in digital healthcare services. Studies have shown that patients who understand how their personal information is collected, stored, and accessed are more likely to trust healthcare providers and to disclose complete and accurate health information during clinical encounters [11,20,26,30]. From a theoretical perspective, patient knowledge represents one of the fundamental components shaping health-related perceptions and behaviors. According to health information privacy theories, individuals who possess adequate knowledge regarding information security are more likely to perceive electronic health systems as trustworthy and beneficial. Conversely, insufficient knowledge may increase uncertainty, perceived privacy risks, and reluctance to engage fully with digital health services [27,29,33].

These findings have important practical implications for primary healthcare facilities. Community Health Centers (*Puskesmas*) should strengthen patient education through brochures, digital media, waiting-room information displays, and direct communication from healthcare professionals regarding patients' rights, confidentiality policies, and the security measures implemented within the EMR system. Improving patients'

digital health literacy will not only enhance trust in electronic medical record systems but also contribute to more effective implementation of EMRs and improved quality of healthcare services [3,10,19].

Item Analysis of the Service Experience Dimension

The findings of this study demonstrate that respondents generally reported positive perceptions regarding the confidentiality of Electronic Medical Records (EMRs). Most participants perceived that EMR confidentiality provided a sense of security, protected personal health information from unauthorized use, and strengthened their trust in healthcare services. These findings indicate that patients perceived confidentiality as an important aspect of electronic health information management. However, because this study assessed patients' perceptions rather than conducting an objective audit of technical or organizational security controls, the findings should not be interpreted as evidence that the EMR system has objectively achieved a specific level of security performance. [4–8]. Another limitation concerns the possibility of social desirability bias. Because respondents evaluated the healthcare facility and healthcare personnel providing their services, some participants may have been inclined to provide more favorable responses than their actual experiences. Therefore, the findings should be interpreted as patients' self-reported perceptions rather than objective assessments of EMR security performance.

Patients also expressed a favorable perception of the security of their personal health information during their interactions with the EMR system. Positive service experiences are closely associated with increased confidence in healthcare information systems because patients tend to evaluate information security based on their direct interactions with healthcare providers rather than solely on technical security measures. Nevertheless, the presence of neutral responses indicates that some patients remain uncertain about how their personal health information is stored, processed, and protected. This finding suggests that technical security alone is insufficient to establish public trust; effective communication regarding privacy protection mechanisms is equally important [9,11,15,27]. Another important finding is that respondents generally felt comfortable providing personal health information during healthcare services. A sense of security when sharing sensitive information is a critical determinant of patient engagement because patients who trust that their information will remain confidential are more likely to disclose complete and accurate health information, thereby supporting more appropriate clinical decision-making. Similar findings have been reported in previous studies, which demonstrated that positive service experiences significantly influence patients' confidence in electronic health information systems and strengthen their willingness to participate actively in healthcare services [20,22,30].

These findings are consistent with previous studies showing that patient perceptions of information security are strongly influenced by their experiences with the usability, reliability, and transparency of electronic health information systems [9,10,11]. Studies have also demonstrated that healthcare organizations implementing user-friendly EMR systems with clear privacy protection policies tend to achieve higher levels of patient satisfaction and trust [5,8,19]. Therefore, patient experience should be considered an essential indicator when evaluating the effectiveness of EMR implementation in primary healthcare settings. From a regulatory perspective, these findings support the implementation of the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, which requires healthcare facilities to maintain the confidentiality, integrity, and availability of electronic medical record data while ensuring that patients receive adequate information regarding the management of their personal health information [2]. Accordingly, Community Health Centers (*Puskesmas*) should complement technical information security measures with effective communication strategies, including patient education, transparent explanations of data access procedures, and regular dissemination of privacy policies. Such initiatives are expected to strengthen patient trust, improve satisfaction with healthcare services, and promote the sustainable implementation of Electronic Medical Records in primary healthcare facilities [3,19,28].

Item Analysis Results for the Trust in Healthcare Professionals Dimension

The findings indicate that respondents generally demonstrated a high level of trust in healthcare professionals regarding the management and confidentiality of Electronic Medical Record (EMR) data. Patients perceived that healthcare professionals were competent, responsible, and committed to protecting the privacy of their personal health information. This finding suggests that professional integrity and ethical conduct among healthcare personnel play a crucial role in fostering patient confidence in digital healthcare services. Trust in healthcare professionals is widely recognized as one of the key determinants of successful EMR implementation because patients are more willing to disclose accurate and complete health information when they believe that healthcare providers will maintain confidentiality and use their information appropriately [10,20,22].

The findings also demonstrate that respondents perceived healthcare professionals as possessing adequate competence to manage electronic medical records while maintaining data confidentiality. Professional competence extends beyond technical skills in operating EMR systems and includes adherence to ethical principles, legal responsibilities, and information security standards. Previous studies have shown that patients'

perceptions of healthcare professionals' competence significantly influence their confidence in electronic health information systems and contribute to higher acceptance of digital healthcare technologies [5,7,9,30].

Although respondents generally trusted healthcare professionals not to misuse or disclose their personal health information, a proportion of respondents expressed neutral perceptions regarding the transparency of communication about how medical data are collected, accessed, and utilized. This finding indicates that patient trust is influenced not only by professional competence but also by effective communication between healthcare providers and patients. Transparent explanations regarding data management, confidentiality policies, and patients' rights can reduce uncertainty and strengthen patients' confidence in the healthcare system [11,13,26].

These findings are consistent with previous research demonstrating that trust in healthcare professionals is closely associated with perceptions of professionalism, ethical responsibility, and effective communication. Muralidharan and Jeyachidra reported that patients who perceived healthcare personnel as competent and trustworthy were more likely to accept EMR implementation and express confidence in electronic health information systems [10]. Similarly, studies on patient trust have emphasized that healthcare providers' ethical behavior and transparency in handling personal health information are fundamental factors influencing patients' willingness to participate in digital healthcare services [22,29,32]. From a regulatory perspective, the findings support the implementation of the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, which requires healthcare facilities to ensure the confidentiality, integrity, and security of patients' medical records while guaranteeing that access is restricted to authorized personnel [2]. Compliance with these regulations should be accompanied by continuous training for healthcare professionals on information security, patient privacy, and professional ethics. In addition, healthcare facilities should encourage healthcare professionals to communicate more openly about data management procedures and patients' privacy rights. Such measures are expected to strengthen patient trust, improve transparency, and support the sustainable implementation of Electronic Medical Records in primary healthcare settings [3,19,27].

Item Analysis of Privacy Policy and Education Dimensions

The findings indicate that respondents demonstrated relatively positive perceptions regarding the existence of privacy policies and data protection measures at Baki Community Health Center. Most participants believed that their personal health information was accessible only to authorized personnel and that appropriate security measures had been implemented to protect Electronic Medical Record (EMR) data. These findings suggest that the health center has established a reasonable level of patient confidence in the technical aspects of information security. Previous studies have similarly reported that the implementation of organizational privacy policies and access control mechanisms contributes substantially to strengthening patients' trust in electronic health information systems [9,15,27].

Despite these positive perceptions, respondents exhibited limited understanding of privacy policies and their rights concerning the confidentiality of personal health information. A considerable proportion of respondents remained uncertain about whether they had received adequate information regarding confidentiality policies and data protection procedures. This finding indicates that the communication of privacy policies has not yet been fully effective. While healthcare facilities may have implemented appropriate technical and administrative safeguards, these measures do not necessarily translate into patient awareness unless they are accompanied by structured education and clear communication [10,11,25].

The findings also suggest that patients' confidence in the security of EMR systems is influenced not only by the existence of technical protection mechanisms but also by their understanding of how these mechanisms operate. Patients who are informed about data access procedures, confidentiality regulations, and their rights regarding personal health information are more likely to trust healthcare providers and actively participate in healthcare services. Conversely, inadequate communication regarding privacy policies may increase uncertainty and reduce patients' confidence in digital health systems [20,26,29].

These findings are consistent with previous studies demonstrating that patient education remains one of the major challenges in the implementation of Electronic Medical Records. Muralidharan and Jeyachidra reported that inadequate patient education regarding privacy policies may limit public acceptance of EMR systems despite the availability of appropriate technical safeguards [10]. Similarly, studies on health information privacy have emphasized that transparency regarding data management practices, patients' rights, and institutional privacy policies is essential for strengthening trust and promoting patient engagement in digital healthcare services [11,12,27,33].

About a regulatory perspective, the findings support the implementation of the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, which requires healthcare facilities to ensure not only the confidentiality and security of medical records but also to provide patients with clear, comprehensive, and understandable information regarding the management, utilization, and protection of their personal health information [2]. Therefore, Community Health Centers (*Puskesmas*) should complement technical security

measures with continuous patient education through brochures, digital information displays, counseling sessions, and direct communication from healthcare professionals. Strengthening privacy education is expected to improve patients' understanding of their rights, enhance transparency, increase public trust, and ultimately support the sustainable implementation of Electronic Medical Records in primary healthcare settings [3,19,28].

Item Analysis of the Data Confidentiality Dimension

The findings of this study demonstrate that respondents generally exhibited positive perceptions regarding the confidentiality of Electronic Medical Records (EMRs). Most participants believed that the confidentiality of EMRs provides a sense of security, protects personal health information from unauthorized use, and strengthens their trust in healthcare services. These findings indicate that patients recognize confidentiality as a fundamental principle of electronic health information management and regard it as an essential prerequisite for accepting digital healthcare systems. The results also suggest that the implementation of EMRs at Baki Community Health Center has successfully established a positive perception of information security among service users.

Data confidentiality is one of the fundamental pillars of Electronic Medical Record implementation because patients routinely disclose highly sensitive personal information, including demographic characteristics, medical history, diagnoses, laboratory results, treatment plans, and other confidential health records. Patients are generally willing to provide complete and accurate information only when they believe that healthcare providers will protect their privacy and use their information solely for legitimate clinical purposes. Consequently, maintaining the confidentiality of medical information is not only an ethical and legal obligation but also a critical factor influencing patient participation, continuity of care, and the overall quality of healthcare services [2,6,16].

Although respondents generally expressed confidence in the confidentiality of their health information, a small proportion remained uncertain or disagreed that EMR confidentiality could fully enhance their trust in healthcare services. This finding suggests that concerns regarding potential data breaches, unauthorized access, or misuse of electronic health information continue to exist among some patients. Such concerns are understandable considering the increasing number of cybersecurity incidents and personal data breaches reported globally, which have heightened public awareness regarding digital privacy. Therefore, healthcare facilities should continuously strengthen both technical and organizational safeguards to ensure that patients' personal health information remains secure throughout the entire data management process [21,23,28,33].

The positive perceptions observed in this study are consistent with previous research demonstrating that confidence in data confidentiality is strongly associated with patients' willingness to utilize electronic health services and disclose accurate health information. Puteri reported that patients who perceived electronic medical records as secure were more likely to trust healthcare providers and actively participate in healthcare services [34]. Similarly, Saleem et al. concluded that effective privacy protection and robust information security mechanisms significantly improve patients' confidence in Electronic Health Record systems and reduce concerns regarding unauthorized access to personal health information [9]. Comparable findings have also been reported by Small et al., who emphasized that transparency in health information management and effective communication regarding privacy protection are essential determinants of patients' trust in digital healthcare environments [11].

These findings are further supported by studies conducted by Keshta and Odeh, who argued that information security in Electronic Health Records should integrate technical safeguards, administrative controls, and user awareness to effectively protect patient privacy [28]. Likewise, Kruse et al. emphasized that healthcare organizations should continuously evaluate cybersecurity risks, implement access control mechanisms, authentication procedures, encryption technologies, and routine security monitoring to minimize the risk of unauthorized disclosure of health information [18]. Therefore, data confidentiality should not be viewed solely as an information technology issue but also as an integral component of healthcare governance and patient-centered service delivery, from a regulatory perspective, these findings support the implementation of the Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022, which requires every healthcare facility implementing Electronic Medical Records to ensure the confidentiality, integrity, availability, and security of patients' medical information throughout the data lifecycle [2]. Compliance with these regulations requires not only adequate technological infrastructure but also the commitment of healthcare professionals to uphold ethical standards in handling patient information.

Overall, the findings indicate that confidentiality remains one of the strongest determinants of patient trust in Electronic Medical Record implementation. Therefore, healthcare facilities should continue strengthening information security through regular staff training, strict access control policies, periodic security audits, continuous patient education regarding privacy rights, and transparent communication about how personal health information is collected, stored, accessed, and protected. These efforts are expected to further enhance patients' confidence in Electronic Medical Records and support the sustainable implementation of digital health services within primary healthcare settings.

CONCLUSION

Patients at Baki Community Health Center generally reported positive perceptions regarding the confidentiality of Electronic Medical Records across the dimensions of knowledge and understanding, service experience, trust in healthcare professionals, and data confidentiality. However, perceptions regarding privacy policies and patient education were comparatively weaker, particularly concerning patients' awareness of their confidentiality rights. These findings indicate the need to strengthen patient education and communication regarding privacy policies, data access, and confidentiality rights. Because this study assessed self-reported perceptions in a single primary healthcare facility using quota sampling, the findings should not be interpreted as an objective assessment of EMR security performance or generalized to other healthcare settings.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to the management and healthcare staff of Baki Community Health Center for granting permission and providing valuable assistance throughout the research process. The authors also extend their appreciation to all patients who voluntarily participated in this study and generously shared their time and responses. Special thanks are addressed to **FKMIK, Universitas Veteran Bangun Nusantara**, for its academic support and encouragement during the completion of this research. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

1. World Health Organization. Global strategy on digital health 2020–2025. Geneva: World Health Organization; 2021.
2. Kementerian Kesehatan Republik Indonesia. Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kementerian Kesehatan RI; 2022.
3. Kementerian Kesehatan Republik Indonesia. Transformasi Kesehatan Indonesia. Jakarta: Kementerian Kesehatan RI; 2023.
4. Maryati W, Yuliani N, Susanto A, Wannay AO, Justika AI. Reduced hospital revenue due to error code diagnosis in the implementation of INA-CBGs. Int J Public Health Sci. 2021;10(2):354–360.
5. Kutney-Lee A, Carthon JMB, Sloane DM, Bowles KH, McHugh MD, Aiken LH. Electronic Health Record usability: associations with nurse and patient outcomes in hospitals. Med Care. 2021;59(7):625–631.
6. James N, Marwaha S, Brough S, John TT. Impact of single sign-on adoption in an assessment triage unit: a hospital's journey to higher efficiency. J Nurs Adm. 2020;50(3):159–164.
7. Arabi YM, Al Ghamdi AA, Al-Moamary M, Al Mutrafy A, AlHazme RH, Al Knawy BA. Electronic medical record implementation in a large healthcare system from a leadership perspective. BMC Med Inform Decis Mak. 2022;22:1–10.
8. Mullins A, O'Donnell R, Mousa M, Rankin D, Ben-Meir M, Boyd-Skinner C, et al. Health outcomes and healthcare efficiencies associated with the use of electronic health records in hospital emergency departments: a systematic review. J Med Syst. 2020;44:205.
9. Saleem JJ, Herout J, Wilck N, et al. Human factors in electronic health record usability and patient safety: a systematic review. Appl Clin Inform. 2022.
10. Muralidharan S, Jeyachidra J. Patient perception toward electronic medical records and information security in healthcare settings. Int J Health Sci. 2022.
11. Small SS, Hohl CM, Balka E. Patient perspectives on health data privacy and implications for adverse drug event documentation and communication: qualitative study. J Med Internet Res. 2021;23:e21452.
12. de Man J, et al. Behind open doors: patient privacy and the impact of design in primary health care, a qualitative study in Indonesia. Front Med. 2022;9:915237.
13. Perera G, Holbrook A, Thabane L, Foster G, Willison DJ. Views on health information sharing and privacy from primary care practices using electronic medical records. Int J Med Inform. 2011;80(2):94–101.
14. Currie LM, Rush KL, Burton L, et al. Perceptions of personal health records in rural primary health clinics in Canada. Stud Health Technol Inform. 2022;289:122–126.
15. Saito K, Shofer FS, Saberi P, Green-McKenzie J. Health care personnel perception of the privacy of electronic health records. J Healthc Risk Manag. 2017;36(3):5–14.
16. Liu J, Li X, Ye L, Zhang H, Du X, Guizani M. Blockchain-based privacy-preserving data sharing for electronic medical records. IEEE Access. 2019;7:151963–151972.
17. Shah SM, Khan RA. Secondary use of electronic health records: opportunities and challenges. Health Inf Sci Syst. 2020.
18. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security techniques for the electronic health records. J Med Syst. 2017;41:127.

19. Kruse CS, Stein A, Thomas H, Kaur H. The use of electronic health records to support population health. Risk Manag Healthc Policy. 2018;11:45–50.
20. Adler-Milstein J, Holmgren AJ. Health information exchange and patient outcomes. Health Aff. 2021;40(7):1127–1134.
21. Blease C, Walker J, Torous J. Patients, clinicians and open notes: information transparency in healthcare. Lancet Digit Health. 2021;3:e507–e512.
22. Cresswell KM, Sheikh A. Organizational issues in the implementation of electronic health records. Health Policy Technol. 2017;6(4):352–358.
23. McAlearney AS, et al. Patient trust and electronic health records. BMJ Health Care Inform. 2020.
24. Vest JR, Kash BA. Health information exchange: persistent challenges and future directions. J Am Med Inform Assoc. 2021.
25. Ratwani RM, et al. Electronic health record usability: analysis and implications. JAMA. 2018.
26. Aguirre RR, et al. Patient perspectives regarding confidentiality in electronic health records. BMC Health Serv Res. 2022.
27. Grando MA, et al. Consumer perspectives on health information privacy. J Am Med Inform Assoc. 2020.
28. Keshta I, Odeh A. Security and privacy of electronic health records: concerns and challenges. Egypt Inform J. 2021.
29. Javaid M, Haleem A, Singh RP. Digital technologies for healthcare information systems. Int J Health Sci. 2023.
30. Esmaeilzadeh P. Patients' concerns regarding privacy of electronic medical records. Inform Health Soc Care. 2019.
31. Agaku IT, et al. Patients' trust in electronic health information systems. BMC Med Inform Decis Mak. 2022.
32. Anggraini D. Statistical approaches for validity and reliability testing in health research instruments. Indones J Health Res. 2022.
33. Asminoto. Protection of patient confidentiality in electronic medical records. J Rekam Medis Indones. 2024.
34. Puteri R. Patient perception of electronic medical record confidentiality in healthcare services. J Health Inform Indones. 2024.
35. Wulandari D, et al. Patients' perceptions of electronic medical record confidentiality at Hidayah Boyolali Hospital. J Rekam Medis Indones. 2025.