JPPIPA 11(6) (2025)

Jurnal Penelitian Pendidikan IPA

http://jppipa.unram.ac.id/index.php/jppipa/index

Analysis of Electronic Medical Records Data Security: Case Study in Citra Husada Sigli Hospital

Juliana[1], Alamsyah[2], Susanna Halim[3*]

[1] Department of Hospital Management, Citra Husada General Hospital, Sigli, Indonesia
[2] Department of Business Management, HealthCare and Hospital Management, Portman College , Malaysia
[3] Faculty of Medicine, Dentistry and Helath Science, University of Prima, Indonesia

Received: April 15, 2025
Revised: June 10, 2025
Accepted: June 25, 2025
Published: June 30, 2025

Corresponding Author:
Susanna Halim
susannahalim@unprimdn.ac.id

DOI: 10.29303/jppipa.v11i6.11081

Abstract: In health services, electronic medical record (E-MR) stands as tool to accelerate the provision of services to patients. However, patient's medical record data must be kept secure, especially because it is easily hacked by unauthorized parties. This study aims to analyze the security of E-MR data at Citra Husada Hospital and identify risks that can occur. This study uses a qualitative survey with a case study design with 10 respondents that were selected by purposive sampling. The aspects of patient's E-MR data security studied were confidentiality, integrity, authentication, availability, access control and non-repudiation. The security of E-RM data is generally good in confidentiality, authentication, availability, access control, and non-repudiation. However, some areas need improvement. While login requires a username and password, the password complexity is weak. Integrity is inadequate due to the lack of an SOP for data changes. Authentication includes digital signature related to encrypted username and password but lacks a certified electronic signature. The system is accessible only within the hospital's intranet, ensuring availability. Access rights are well-structured. A track record ensures non-repudiation. The highest risk is unauthorized changes to patient data, highlighting the need for stronger risk management measures.

Keywords: Data Security Aspects; Electronic Medical Records; Hospital

Introduction

One of the uses of information technology (IT) in the health sector that is trending in global health services is electronic medical records. In Indonesia, this is known as Electronic Medical Records (EMR). Medical records are documents containing patient identity data, examinations, treatments, actions and other services that have been provided to patients. Electronic medical records are medical records created using an electronic system that is intended for. This system is a warehouse for storing electronic information containing the health status and health services obtained by patients throughout their lives (Menteri Kesehatan, 2022)

This digital system will certainly help staff, doctors and health workers to manage patient data more easily. In addition, patients can also access their health data, so that when needed, patients do not need to be confused about requesting physical data or providing a medical history again. With the use of information systems in health services, gives benefits such as improving the quality of service, reducing medical errors, increasing the reading of facility availability and accessibility of information (Menteri Kesehatan, 2022)

Patient medical records have begun to switch to being electronic with the issuance of the Minister of Health Regulation (PMK) number 24 of 2022 concerning Medical Records. Through this policy, health service facilities are required to implement an electronic patient medical history recording system. The transition process will be carried out until December 31, 2023 at the latest (Menteri Kesehatan, 2022)

Reported from persi.or.id, a survey conducted by the Indonesian Hospital Association (PERSI) in March

How to Cite:
Juliana, J., Alamsyah, A., & Halim, S. (2025). Analysis of Electronic Medical Records Data Security: Case Study in Citra Husada Sigli Hospital. *Jurnal Penelitian Pendidikan IPA*, *11*(6), 773–782. https://doi.org/10.29303/jppipa.v11i6.11081

2022 found that of the 3,000 hospitals in Indonesia, only 50% had implemented an electronic medical record system. Of that percentage, only 16% have properly organized electronic medical records. This fact shows that there are still many hospitals that must switch to electronic systems, as well as optimize the electronic systems that have been implemented (Sofia et al., 2022).

Every change certainly has its own challenges, including the implementation of electronic medical records. There are various preparations and challenges that must be faced in order to successfully transform from manual to digital systems, as well as their operations in providing hospital health services. One of the biggest challenges is data security. Patient medical record data contains very sensitive information, including personal information, medical history, to emergency contact data that if leaked or misused can have serious impacts on patient privacy and safety (Ardianto & Nurjanah, 2024; Sofia et al., 2022). On the other hand, vulnerability to cybersecurity threats such as hacking, malware and phishing is also increasing. Attacks on health information systems can pose broad risks, such as data theft, manipulation of medical information, and even termination of health services (Ardianto & Nurjanah, 2024).

Regarding the rapid use of information technology today, information governance is needed to maintain the security of information and data. The increasing trend of data theft is a serious problem. Health data theft is nothing new in Indonesia. In 2020, 230 Covid-19 patient data were known to have had their health data stolen, in addition, in January 2022, it was suspected that there had been a data breach of patient records in several hospitals in Indonesia amounting to 720 GB which was sold on online forums, Ransomeware Wanna Cry is the largest data leak case in the world where in this case 150 countries became victims and resulted in system paralysis, one of which was the information system at Dharmais Cancer Hospital which experienced system paralysis due to this and caused a backlog of patients (Ardianto & Nurjanah, 2024).

Citra Husada Hospital is a Private Hospital with a legal entity of a Limited Liability Company, under PT Citra Husada Bhakti. RSU Citra Husada is a type D hospital domiciled in Pidie Regency, Aceh Province. RSU Citra Husada has been operating since 2012, with 233 employees and 85 beds. It currently has 14 specialist services in outpatient and inpatient care. It has three medical record staff and 2 IT staff. RSU Citra Husada has had a Hospital Management Information System (SIMRS) since 2015, in collaboration with the SIMRS developer vendor, PT Total Solution, but its implementation is limited to patient personal data, patient entry and exit times, use of drugs and other consumables, use of supporting examinations, and patient billing, has not implemented medical records containing patient medical information. This is because the medical record format in the Hospital SIMRS does not comply with the provisions in the Hospital accreditation standards and there is no legislation that requires the use of electronic medical records.

RSU Citra Husada has implemented Electronic Medical Records in early of year 2024, but its implementation is only in outpatient polyclinics, while for inpatients it has not been implemented due to limited facilities, infrastructure and incomplete inpatient medical record formats in SIMRS.

Previous studies have shown that health information systems, including electronic medical record applications, often have vulnerabilities that have not been identified or are not handled properly. The principles of information security, especially in the health sector, include six aspects, namely privacy, integrity, authentication, availability, access control and non-repudiation (Sofia et al., 2022). Some of the causes include lack of security assessment, limited understanding and resources to maintain data security and the suboptimal implementation of cybersecurity policies in many health facilities. This study aims to analyze the security of E-MR data at Citra Husada Hospital and identify risks that can occur

Method

Time and place of research.

The research was conducted on January 2025 at RS Citra Husada, Prof. A. Majid Street, Pidie Regency, Aceh province, Indonesia

Research methods

The type of research used is qualitative research with a case study design. The method of selecting informants was using the purposive sampling technique. The selection of informants was based on certain criteria. Criteria for selecting informants. The Director of Citra Husada Hospital is an official who is responsible for leading, controlling, supervising and coordinating the hospital organizers. The Head of Medical Records unit is the person in charge of medical record activities and has knowledge about medical records. The criteria for IT personnel are those responsible for programming software and hardware related to EMR. The criteria for general practitioners and nurses are officers who use electronic medical record applications on a daily basis.

Research tools

Questionnaires and interviews are essential research tools used to collect data. Questionnaires are structured sets of questions that allow researchers to

gather standardized information from many respondents efficiently, making them suitable for quantitative studies. They are cost-effective but may lack depth. In contrast, interviews involve direct interaction and are used in qualitative research to explore participants' experiences and perceptions in detail. Although interviews provide richer data, they are more time-consuming and require skilled interviewers. Both tools can complement each other—questionnaires offer breadth, while interviews provide depth

Research subjects.

The research subjects were 10 respondents, namely the Director, 2 Information Technology (IT) personnel, Head of Medical Records, 2 general practitioners, 2 outpatient nurses, 2 inpatient nurses. The study was conducted by interviewing the subjects in depth and asking them to fill out a questionnaire.

Data Analysis

Primary data collection is carried out through interviews, questionnaires, observations and documentation. Data analysis in this study was carried out by data reduction, data presentation and drawing conclusions. Data validity testing is carried out using source triangulation and technique triangulation.

Result and Discussion

Result

Electronic Medical Record Data Security Analysis Based on Confidentiality Aspects

The confidentiality aspect is a guarantee of data and information security from internal or external interference from parties who do not have the right to access data and information contained in electronic medical records, protected use and distribution.(Ardianto & Nurjanah, 2024; Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019).

Regarding the results of research conducted related to the security of electronic medical record information, the following interview results were obtained with respondents: All respondents said that to log in to the e-RM system, they must use a username and password. Each user has received a personal username and password from IT. From the results of the researcher's observations, the same thing was also obtained. Here is a photo of the display when logging in:

Figure 1. SIMRS login display

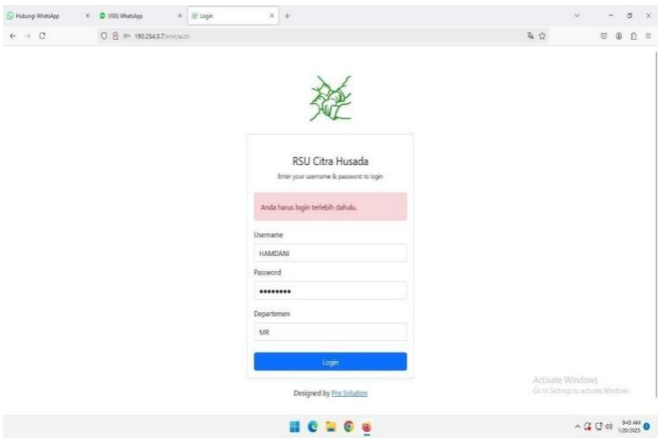

Figure 2. E-RM system login display

This is in accordance with research conducted by Efri Tri Ardianto et al. at Hospital X, which also explains the use of usernames and passwords in E-RM to prove that users have the authority to enter the system and prevent access by users who do not have authority(Ardianto & Nurjanah, 2024). Inline with the research conducted by Waisantoro et al at RSUD Surakarta, the use of passwords and user IDs were also enforced on the computer system to maintain the security of existing data.(Waisantoro et al., 2014)

Based on the interview results, 9 out of 10 respondents said the passwords used were still not strong because they only contained numbers and letters, no special characters. Only 1 respondent, namely IT from the vendor, stated that the password system used was strong enough even though it did not require the use of special characters. The following is an excerpt from an interview with a respondent:

> *"There is already a password with a combination of letters and numbers, it is quite optimal because the password already uses Message-Digest Algorithm 5 (MD5). MD5 is a cryptographic hash algorithm used to verify content, digital signatures and authenticate messages" (Respondent 2, IT Vendor E-RM system)*

"*There is already a username and password setting for each user, so far there has never been a case of misuse by unauthorized users.*" *(Respondents 9 and 10, Head of Medical Records and Hospital IT Officer)*

Users should change their passwords periodically, to avoid usernames and passwords being known and used by unauthorized parties. Based on the interviews conducted, the following are the results obtained: only 1 out of 10 respondents changes passwords periodically. The reason is because there is no time limit for changing passwords (interview with Respondent 9 and 10).

To maintain security, it is expected that there will be an automatic logout feature after no activity for a certain period of time, so that the system is not used by unauthorized parties when users forget to log out. Based on the interview, the following results were obtained:

"*Automatic logout occurs when the day changes, at 00.00 WIB, every day, the system will automatically close completely because data is backed up at that time. So if there is a user who forgets to log out, then at 00.00 there will be an automatic log out.*" *(Respondent 2)*

To ensure that all users of the E-RM system comply with data security protection procedures, Hospital Management should create a Standard Operating Procedure related to E-RM data security. The following results were obtained from the interview:

"*There is already an SOP related to E-RM data security protection and the implementation of E-RM in the Hospital.*" *(Respondent 1).*

Analysis of Electronic Medical Record Data Security Based on Integrity Aspects

Data integrity refers to the accuracy, completeness and consistency of data throughout its life cycle. In electronic medical records (E-RM), data integrity means that patient information must not be damaged, changed without authorization or lost. Integrity is a guarantee of the accuracy of data and information contained in electronic medical records and changes to data may only be made by people who are given access rights to change.(Ardianto & Nurjanah, 2024; Menteri Kesehatan, 2022) In this study, integrity can be seen from the edit and delete features that can be used to change patient data in the electronic medical record system. The edit and delete features should be limited to use only by authorized users. It is known from the results of the interview that the E-RM system at Citra Husada Hospital only has an edit (change) facility. This is in line with research conducted by Efri Tri Ardianto et al., which explains that the E-RM system at Hospital X does not have a deletion process.(Ardianto & Nurjanah, 2024) According to the laws and regulations regarding medical records, data deletion is not permitted, if there is a writing error, then what is done is to cross out the wrong one and write the correct one.(Menteri Kesehatan, 2022) However, deletion in electronic medical records cannot be done so that tighter security is needed so that data is not simply deleted or edited. This result is inline with the research conducted by Nugraheni, S.W et al in RSUD Dr. Moewardi. The legal aspect of electronic medical records at Dr. Moewardi Hospital based on the integrity aspect has not facilitated changes to information. Erasure/deletion cannot be done in electronic medical records.(Nugraheni, 2018)

The editing process in Electronic Medical Record at Citra Husada hospital can only be done by the officer who inputs the data. Other officers, even though they work in the same field and have access to the E-RM system, cannot make changes to data inputted by others. However, the data change process can be done without the approval of other authorized parties such as the head of the medical record unit. At Citra Husada Hospital, there is no time limit for making data changes. The following is an excerpt from an interview with a respondent.

"The edit and delete features are available in both E-RM systems, both web-based and desktop. Data that has been updated and recalled for editing can only be done by users with the same username as the first person to write it. So if another user reopens the data, it cannot be edited. The feature can also be used by medical record users for all medical record data. However, the deletion process can only be done by the IT Vendor" (Respondent 2)

This is not in line with the research conducted by Efri Tri Ardianto at Hospital X(Ardianto & Nurjanah, 2024) and E.N. Hidayah at Dr. Cipto Mangunkusumo National General Hospital, Jakarta, which explained that if a doctor wants to make changes to the contents of an electronic medical record, they need approval from the medical record section, namely the head of the medical record subsection, the person in charge of medical record services, and the head of the medical record and admissions agency.(Hidayah, 2023). To ensure the integrity of patient data in E-RM, it is important to determine the time limit for editing or deleting data. From the interview results, it was found that:

"*There is no time limit for making data changes.*" *(All respondents)*

In order for all authorized officers to know about the procedures for making data changes in the E-RM system, hospital management should create a policy in the form of a special SOP regarding data change (edit) procedures.(Hidayah, 2023) Based on the interview results, there is no special SOP for data editing procedures at Citra Husada Hospital.

Analysis of Electronic Medical Record Data Security Based on Authentication Aspect

Authentication is an aspect of patient data security related to information access or how the system states

the validity for users to access data in the system (Menteri Kesehatan, 2022; Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019) The methods used can be the use of passwords, personal identification numbers (PINs), biometrics and so on. Another way that can be used to maintain the security of patient data from the authentication aspect is by implementing electronic signatures. The implementation of electronic medical records in health care facilities can be equipped with electronic signatures.

An electronic signature is a signature that is placed in association or related to other electronic information that is used as a means of verification and authentication.(Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019) Electronic signatures are used as a means of verification and authentication of electronic medical records and the identity of the signatory. An electronic signature that has legal force is a signature made using the services of an electronic certificate provider (Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019). The signatory is a legal subject that is associated or related to the electronic signature (Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019)

From the results of the study at Citra Husada Hospital, it is known that electronic signatures have not been implemented in the E-RM system, which already has a digital signature, which is scanned from the user's original signature. Digital signatures at Citra Husada Hospital already have a secure encryption system, can avoid the risk of forgery of signatures or misuse by irresponsible parties, are efficient and protected by the guarantor. The digital signatures also connected with user ids and passwords. This condition is inline with the research conducted by Adam Reza Pahlevi et al at RSIGM Sultan Agung Semarang, where electronic signatures are replaced with user ID and passwords (Pahlevi et al., 2021). Different results were obtained from the research conducted by Waisantoro D.U et al at RSUD Surakarta, where the Hospital Information System could not identify users so that each user can open all modules in the system. Each user who entered a username and password had no restictions in accessing the system so that confidentiality of datas was not maintained properly (Waisantoro et al., 2014).

This is not the same as the research conducted by Efri Tri Ardianto at Hospital X, which has implemented electronic signatures for caregivers but has not implemented electronic signatures for patients (Ardianto & Nurjanah, 2024)

Quoted from the results of an interview with an IT Vendor:

> "*There is no electronic signature authorized by an institution that has the right to issue certification related to electronic signatures. What is already there is a digital signature that is scanned and related to the user's username and password. So when logging in, the doctor or nurse only needs to input their respective username and password, then the user's digital signature will be listed in the place that requires a signature.*" *(Respondent 2)*

E-RM system uses a username and password to ensure authentication. Each doctor can only open the E-RM of patients registered in the registration for consultation with the doctor. The digital signature has been associated with the username and password of each user. For medical record users, they can open all E-RM data, but cannot make changes or delete data.

Analysis of Electronic Medical Record Data Security Based on Availability Aspects

Electronic medical record storage must guarantee the security, integrity, confidentiality and availability of electronic medical record data.(Menteri Kesehatan, 2022) Availability is an aspect that ensures data will be available when needed anytime and anywhere for users who have access rights.(Ardianto & Nurjanah, 2024; Menteri Kesehatan, 2022) Medical records must be available quickly and can display the history of previously stored data (Ardianto & Nurjanah, 2024).

Regarding the results of research at Citra Husada Hospital, it is known that E-RM data storage is quite safe. Data is stored on a server with a capacity of 1 Terabyte. The server is placed in a special server room with fire protection. In addition, for data backup, the hospital provides two devices, one backup server with a capacity of 2 Terabytes, which runs data backup in real time. One external hard disk with a capacity of 2 TeraByte for routine data backup and periodic data backup in the cloud.

The following are the interview results obtained from IT vendors:

> "*E-RM data is stored on a server stored in a special server room, data is backed up in real time on the backup server and routinely on an external hard disk. Data is also backed up in the cloud, namely Google Drive, routinely.*" *(Respondent 2)*

Regarding the results of research at Citra Husada Hospital, it is known that E-RM can only be accessed in the hospital environment and network. This is evident from the results of interviews with respondents as follows:

> "*E-RM in outpatient care is indeed a web-based system, but access is not opened outside the hospital, because its Public IP is not opened for public access. While E-RM in*

the ER and inpatient care uses a desktop system, so it cannot be accessed from outside the hospital." (Respondent 2, IT Vendor)

"E-RM can only be accessed in the hospital environment using a computer connected to a LAN cable, cannot use other devices that are not connected to a LAN cable." (Respondents 3,4,5,6,7,8 E-RM system users)

This is in accordance with research conducted by Efri Tri Ardianto, et al. at Hospital X(Ardianto & Nurjanah, 2024) and research by A.T. Ramadhanti at PHC Hospital Surabaya, where the electronic medical record system can only be accessed via the Hospital's internet network, cannot be accessed with other internet networks(Ramadhanti, 2022)

It is explained in the Republic of Indonesia Law Number 11 of 2008 concerning Information and Electronic Transactions, that every electronic system organizer must operate an electronic system that meets minimum requirements, one of which is being able to display electronic information and/or being able to protect the availability, integrity, authenticity, confidentiality and accessibility of electronic information in the implementation of the electronic system.(Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 2008) From the results of the study referring to interviews, it is known that all officers who have access rights to the E-RM system can access E-RM easily. The E-RM system can be accessed without any time limits for officers who have been given access rights.

Here is a quote from the interview results:

"*Doctors and nurses who already have a username and password can access E-RM at any time. They can review data that has been saved several days or several months ago." (Respondents 3,4,5,6 and 7)*

"*Officers who have access rights can open and view E-RM data at any time and the data that can be accessed is patient data since it was first entered into the E-RM system. However, doctors can only open patient data who consult with the doctor, they cannot open data that is not their patient. As for medical record users, they can open all patient data." (Resondents 2, 9 and 10).*

Analysis of Electronic Medical Record Data Security Based on Acess Control Aspects

Access control is the regulation of user access to the information system. This is done to ensure that only officers who have access rights can use the E-RM system.(Sofia et al., 2022) With access control, user access rights can be limited. So each user group can only access certain features in the health information system, not all features can be accessed. Access rights for the Doctor user group are different from access rights for the nurse user group. Each user does have their own username and password, access rights are regulated through department selection. Access rights are regulated through Hospital policies and set by IT.

Here are the answers from IT respondents:

*"Access rights are limited by username, password and department*0t. Users are grouped into several departments. Each department can only access certain features in the E-RM system according to their duties, authority and responsibilities. For example, users of the Doctor department can only open the E-RM form that is the Doctor's job, they cannot open the form for nurses. Likewise, users of the Nurse department cannot open the form that is the Doctor's job. The Medical Record user group cannot open the edit feature, they can only view the filled-in Medical Records. The Pharmacy department user group cannot open medical records, they can only open features for pharmacy services. So every time a user wants to log in, there is a request to fill in a username and password and select a department. Certain users have been set up related to certain departments as well, so if the department selection is wrong, the user cannot log in. " (Respondents 2 and 10).*

This is in line with research conducted by Efri Tri Ardianto et al. at Hospital X(Ardianto & Nurjanah, 2024) and A.T. Ramadhanti at PHC Hospital Surabaya which explained that the setting of HIS user access rights is in accordance with their respective duties and authorities. (Ramadhanti, 2022)

Based on the interview results, it was found that the E-RM display is the same for all departments, only features with limited access rights cannot be used. The following is an excerpt from an interview with respondents who use the E-RM system:

"The menu display in E-RM is the same for each user, but there are several features that cannot be accessed by doctors/nurses" (Respondents 3,4,5,6,7 and 8)

"The display of all menus can be seen by all users. For the medical records department, they cannot access the features for filling in and editing medical records, they cannot access features related to pharmacy. They can only open the feature to view medical record history. " (Respondent 9)

Analysis of Electronic Medical Record Data Security Based on the Non-Repudiation Aspect

Non-repudiation is a concept in information security that ensures that actions taken by a person cannot be denied later by that party. Non-repudiation is how the system can record traces of data changes made by the user.(Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019; Sofia et al., 2022) According to government regulation number 71 of 2019 concerning the implementation of electronic systems and transactions, it is explained that it is mandatory to provide an audit trail of all electronic system

implementation activities used for the purposes of supervision, law enforcement, dispute resolution, verification, testing and other examination.(Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019)

From the results of the study, based on the results of interviews with IT Vendors of the E-RM system, it was found that there was already a history for users who accessed the E-RM system. The following are the results of interviews with IT respondents:

> "*There is already a track record in the data log, you can see the track record of each user logging in or out. There is also a track record of what the user did, when to fill in, when to edit and when to send data to another unit. So that it can be traced back who edited the data or if there is data loss, it can be traced which user deleted it*" *(Respondent 2).*

This is in line with research conducted by Efri Tri Ardianto, et al. at Hospital X, explaining that changes to patient medical record history data must be clearly known, if there is a change in data, the data history is stored and cannot be removed in writing electronic medical records(Ardianto & Nurjanah, 2024). One way to find out who is accessing information and what changes have been made to patient data is to conduct a data security audit. From the interview results, it is known that an E-RM system audit has never been carried out. The following is an excerpt from an interview with an IT respondent:

> *"E-RM system has never been audited." (Respondents 2 and 10).*
>
> *"Never been audited." (Respondent 1).*

Discussion

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on Confidentiality Aspects

From the aspect of confidentiality, the level of patient data security is quite good. To log in to the system, it is mandatory to use a username and password that have been registered for each user according to the duties, authorities and responsibilities of each user. Citra Husada Hospital Management has also prepared an SOP for E-RM data security. However, there are still several shortcomings, including:

a. There are no provisions for creating passwords, so there are some users who create passwords that are too easy, so it is feared that they are easily guessed by unauthorized users.
b. There are no provisions for the password change interval, so there are users who routinely change their passwords but there are some users who never change their passwords.
c. The automatic logout system has too long a time, namely when the day changes, so it is feared that if the user forgets to log out after use, the E-RM system can be accessed by unauthorized users.
d. The SOP on E-RM data security protection already exists, but not all users know and understand the contents of the SOP.

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on Integrity Aspect

Based on the results of interviews and observations, data security from the Integrity Aspect still needs improvement. There is already a data edit feature in E-RM, but users cannot delete data. Data deletion can only be done by the IT Vendor. IT has made restrictions on users of the edit feature, namely users who input data who can edit data. So if there is incorrect data that needs to be edited, you must log in using the username that input the data, you cannot use another username.

However, there is no authority system in using the edit feature. There are no provisions for time limits for changing data. The authority to delete data lies with the IT Vendor, without any provisions for obtaining approval from the Hospital Management. Hospital Management has also not prepared a special SOP related to improving E-RM data.

Hospital Management should immediately create provisions in the form of SOPs related to improving E-RM data, especially the regulation of the authority granting permission to make data changes and the time limit for making data changes.

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on Authentication Aspects

From the results of interviews and observations, it was found that the level of patient data security based on authentication aspects was quite good. Where it was found that each user has their own username and password to log in. The username and password are also related to each user's digital signature. After the user (doctor or nurse) logs in with their respective username and password, then in certain parts of the medical record that require a signature, the digital signature of the user who logged in will be displayed. Digital signatures at Citra Husada Hospital already have a secure encryption system, which can avoid the risk of forgery of signatures or irresponsible misuse. In addition, users (doctors or nurses) cannot open patient data who have not registered for consultation with the doctor, so it cannot be misused by other unauthorized users. However, because the automatic logout occurs at the end of the day, it is still possible for other users to log in when the previous user forgot to log out. This can be a deficiency in the authentication aspect.

Researchers suggest that hospital management also start implementing electronic signatures issued by electronic certification institutions. Electronic signatures provide greater authentication because each time a signature is signed, a One Time Password (OTP) is required, sent by the institution to the user via email or message to the user's phone number registered with the institution (Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 2019)

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on Availability Aspect

From the results of interviews and observations, it was found that the storage of electronic medical record data at Citra Husada Hospital has guaranteed the security, integrity, confidentiality and availability of electronic medical record data. Electronic medical record data is stored on a server located in a special server room. The room is locked and only authorized officers are given the right to access the room. The server room is also equipped with air conditioning to prevent damage to the server due to high temperatures.

To prevent data loss due to server damage, real-time data backup is carried out on the backup server and on an external hard disk located in the same room as the main server. To prevent data loss due to disasters that hit the Hospital, such as fires, earthquakes, floods, and others, electronic medical record data is also stored in the cloud in the form of Google Drive, which is done routinely. Data on Google Drive can only be accessed by IT Vendors. According to researchers, data storage has guaranteed security, integrity and confidentiality.

The availability of medical record data is good. Every user can access E-RM data at any time in the Hospital environment. There is no time limit for E-RM data that can be accessed. Users can access data from the first time it is input.

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on Access Control Aspects

From the results of interviews and observations, it was found that not all features in E-RM can be accessed by all users. There are several groups of departments in the E-RM system. Each department gets access to certain features according to the details of its duties and authorities and is limited to certain features that are not the authority and responsibility of the department. All users are grouped into departments according to their respective duties and authorities.

These access rights are regulated by Hospital Management and set by IT. Every time they log in to the system, users must write a username, password and select a department. The username has also been linked to the department, so if the user chooses the wrong department, they cannot log in. After logging in, the E-RM menu display is the same for all departments, but there are some features that cannot be clicked or accessed. For example, an administrative officer logs in to the system, then they will see the same display as a doctor or nurse user, but the administrative officer cannot open the medical record menu, while the doctor or nurse cannot open the registration menu. One user can be given access rights for two departments according to their duties and responsibilities.

In addition to feature restrictions, the access rights of doctors or nurses to the E-RM system are also linked to the registration system. So when a patient registers, they will get a doctor's code in the system. When a doctor opens E-RM, only patient data registered with that doctor can be accessed, they cannot access other doctors' patient data.

According to researchers, the security of patient data in the E-RM system from the aspect of access control is quite good. However, because automatic log out is still not optimal, there is still a gap for misuse if users forget to log out.

Patient Data Security in Electronic Medical Records at Citra Husada Hospital Based on the Non-Repudiation Aspect

The results of the study through interviews with IT Vendors, in the E-RM system at Citra Husada Hospital there is already a track record of all activities carried out and stored in the data log. IT can see the history of E-RM usage, related to who the user is who accesses, what is done, filling in new data or editing data and when the activity was carried out. So that if there is a change in data in the patient's medical record, it can be clearly identified. Data changes are stored in the data history and cannot be removed in writing electronic medical records.

From the results of the study, it can be concluded that the aspect of patient data security for the non-repudiation variable is good. However, an audit of the E-RM system has never been carried out.

Risk Management of Data Security in the E-RM System at Citra Husada Hospital

After obtaining the results of the study on patient data security in E-RM, the researcher compiled a risk register and compiled a priority scale for suggestions for improving E-RM at Citra Husada Hospital. When sorted according to priority scale, the order of the main risks that must be fixed by the hospital is:

1. Risk of patient data being changed by unauthorized persons.
2 Risk of patient data being inauthentic.
3. Risk of losing patient data due to data storage corruption

4. Risk of patient data being edited and deleted by unauthorized parties
5. Risk of unauthorized users entering the E-RM system
6. Risk of patient data being changed by unauthorized users.

Conclusion

Based on the analysis, the security of the Electronic Medical Record (E-RM) system at Citra Husada Hospital is generally considered good in terms of confidentiality, authentication, availability, access control, and non-repudiation. The system uses encryption through the Message-Digest Algorithm 5 (MD5) and applies access restrictions based on each user's department and responsibilities. However, several areas still require improvement. The password complexity is weak, and the automatic logout system is not optimal, posing a risk of unauthorized access if users forget to log out.

In terms of data integrity, while data editing features are restricted to authorized personnel, there is no clear time limit for changes (e.g., limited to within 2 x 24 hours), and there is no specific Standard Operating Procedure (SOP) for data modification or deletion. Currently, data deletion can only be performed by the vendor's IT team without the necessary approval from the Hospital Director, which raises concerns regarding authority and control.

From the authentication aspect, the system uses encrypted digital signatures and restricts access so that doctors and nurses can only view the records of their own patients. However, certified electronic signatures—which provide stronger authentication and legal validity—have not yet been implemented. In terms of availability, the E-RM system can only be accessed within the hospital network, ensuring data security while still allowing fast and continuous access to patient records without time limitations.

Access control is well-managed, as hospital IT has configured user access rights based on work units and job descriptions. Even though the interface looks the same across users, the features accessible are restricted according to department. Regarding non-repudiation, the system maintains detailed activity logs that track who accessed what data and when. However, these logs are only accessible to the external IT vendor, and no audit has yet been conducted on the system, limiting the hospital's internal oversight over data security.

In conclusion, while the E-RM system demonstrates a reasonably strong security foundation, improvements are needed in internal regulation, stronger authentication mechanisms, detailed SOPs for data modification and deletion, and better oversight of third-party vendors to ensure comprehensive data security.

Acknowledgments
Thank you for the Director of Citra Husada Hospital and all respondents who had participated in this study.

Author Contributions
J: Collect data, analyze data, and prepare articles for publication.
A&S : review and editing.

Funding
This research received no external funding.

Conflicts of Interest
The authors declare no conflict of interest.

References

Ardianto, E. T., & Nurjanah, L. (2024). Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X. *Jurnal Rekam Medik Dan Manajemen Informasi Kesehatan*, *3*(2), 18–30.

Hidayah, E. N. (2023). *Analisis Aspek Keamanan Data Pada Hospital Information System (His) Dalam Penerapan Rekam Medis Elektronik Di Rsup Nasional Dr. Cipto Mangunkusumo Jakarta*.

Menteri Kesehatan. (2022). Peraturan Menteri Kesehatan RI No 24 tahun 2022 tentang Rekam Medis. *Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022*, *151*(2), 1–19.

Nugraheni, N. (2018). Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi. *Prosiding Seminar Nasional Unimus*, *1*, 92–97.

Pahlevi, A. R., Wardhana, E. S., & Agustin, E. D. (2021). Electronic Medical Record At Rsigm Sultan Agung Semarang Reviewed From the Completeness and the Safety Format System. *Jurnal Medali*, *3*(1), 20. https://doi.org/10.30659/medali.v3i1.16892

Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik, 7 Media Hukum 70 (2019).

Ramadhanti, A. T. (2022). *Analisis Aspek Keamanan Informasi Pasien dalam Penerapan Rekam Medis Elektronik di Rumah Sakit PHC Surabaya*.

Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis Aspek Keamanan Informasi Data Pasien Pada Penerapan RME di Fasilitas Kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, *1*(2), 94–103. https://doi.org/10.47134/rmik.v1i2.29

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, Bi.Go.Id 1 (2008). https://peraturan.bpk.go.id/Home/Details/37589/uu-no-11-tahun-2008

Waisantoro, Rohmadi, & Mulyono, S. (2014). Tinjauan Penerapan Otentifikasi Keamanan Sistem

Informasi Managemen Rumah Sakit Umum Daerah Surakarta. *Rekam Medis*, *VIII*(1), 29–35.