EVALUATION OF ELECTRONIC MEDICAL RECORD DATA SECURITY BASED ON BASIC ASPECTS OF INFORMATION SECURITY

Dian Felinda [1], Ahmad Amiruddin [2], Niska Salsiani Sinta[3]*
[1,2,3] Politeknik Baubau, Baubau Indonesia

ARTICLE INFORMATION

Received: 20 Januari 2025
Revised : 28 Januari 2025
Accepted: 27 Februari 2025
DOI :

KEYWORDS

Keywords: Basic Information Security, SIMRS, Medical Records

CORRESPONDING AUTHOR

Name : Ahmad Amiruddin
Address: Topaz 2, Kec. Betoambari, Kota BauBau
E-mail : ahmadamiruddinpoltekbaubau@gmail.com

A B S T R A C T

Within the angle of overseeing electronic wellbeing information data security, it could be a combination of mechanical and organizational viewpoints. The strategy chosen for this will moreover have an affect on the taken a toll, complexity and level of security delivered. The innovative perspective can be utilized to control confirmation, authorization, keenness, review trails, post-disaster recuperation, secure information capacity and transmission.. This research aims to find out how to evaluate the security of electronic medical record data in dealing with cybersecurity threats at BLUD RSUD Baubau City in 2024. This research was conducted at BLUD RSUD Baubau City Year 2024. The method used is using a descriptive type of approach with a qualitative approach and the method of data collection techniques using interview methods, and observation. Data collection tools using interview guidelines, observation sheets. In the aspect of Authentification, each health worker account in using the SIMRS application has a different user and password. In the authorization aspect, each health worker can only use the menu features in the SIMRS application according to their respective domains, this is made so that data can be protected from irresponsible people. In the privacy aspect, full access to the SIMRS application can only be done by IT officers and data processing officers, besides that the data security system owned in SIMRS is only a standard system, this can still be done by hacking data by irresponsible parties. The conclusion needs to be re-evaluated regarding the security system used in SIMRS in order to keep electronic medical record data safer from irresponsible parties.

INTRODUCTION

A restorative record is a record that contains information on the person's understanding, examination, treatment, strategies and other administration of that understanding. Electronic Restorative Records are Restorative Records created utilizing an electronic planning framework for the administration of Restorative Records (Wellbeing, 2022).

A wellbeing data framework can be an instrument for gathering, preparing, analyzing, and sending the data required to organize and run wellbeing administrations and to investigate and prepare. A management data framework (often known by its acronym MIS) is the application of a data framework in an organization to support the data needed by all levels of management. In theory, computers do not have to be used in a MIS, but in reality it is incomprehensible that a complex MIS could operate without including a computer component. MIS is continually concerned with computer-based data handling (Anita, 2019).

The rapid advancement of data technology in various fields has become a common wonder in this day and age. The health sector is no exception, one of the forms of using data systems in health services. It is no secret that the use of data systems in health services can provide various benefits that benefit service providers, in this case treatment centers, clinics, and so on. Some examples of benefits that can be obtained are improving the quality of benefits, reducing recovery errors, expanding research on facility accessibility and data availability (Tiorentap and Hosizah, 2020).

In the perspective of information security supervision of electronic welfare data, it may be a combination of innovative and organizational perspectives. The strategy chosen for this will also have an impact on the impact, complexity and level of security. Mechanical viewpoints can be used to control confirmation, authorization, acuity, review paths, post-disaster recovery, securing capacity and information transmission. The organizational perspective plays a very important role in determining the formal approach, determining the structure for creating and implementing approaches and strategies, as well as determining methods for filtering and allowing security breaches and information security arrangements (Nanda, Sudra and Rohmadi, 2009).

Based on preliminary studies conducted at BLUD RSUD Baubau City, the use of Electronic Medical Records has been running and will enter two years of use but SIMRS BLUD RSUD Baubau City does not yet have data security features. As a result, the hospital only limits user access rights to avoid leakage of electronic medical record data, but this has not been done optimally. Therefore, it is necessary to conduct research on the Evaluation of Electronic Medical Record Data Security Based on Basic Aspects of Information Security at BLUD RSUD Kota Baubau in 2024, in order to maintain Electronic Medical Record data and avoid the threat of data leakage.

METHODOLOGY

The method in the study used a qualitative method using a descriptive approach. The implementation of this research will start from March - June 2024. this research was conducted at BLUD RSUD Baubau City which is located in Baadia Village, Murhum District, Baubau City, Southeast Sulawesi Province. The subjects involved in this study were the Head of IT, Head of Medical Records, Record Officers, Registration Officers... The object involved in planning the implementation of electronic medical records is Electronic Medical Record Data Security (SIMRS) on the part of the hospital to be based on basic aspects of information security. The method of data collection techniques uses interview methods, and observation. Data collection tools using interview guidelines, observation sheets

RESULTS & DISCUSSION

Evaluation of Medical Record Data Security of Electronic Medical Record Data Based on Information Security Basis on the Aspect of Authentification

Account creation is made by IT officers. In addition, before the account is created, health workers will be given a link. In creating an account for Username and Password each health worker will be different, if the health worker forgets his username or password, he must contact the IT Staff to update the username or password for the health worker's account.

Table 1. Observation results on the Authentification Aspect

No	Objects Observed	Description
1	*User*name dan password	Accounts on health workers users and passwords are not the same, which have differences for each health worker.
2	Steps to create a new account	In creating a new account, the officer must first contact the head of the room or the person in charge if the person in charge agrees, then the person in charge will contact the IT officer to create a new account for the health worker.
3	Account repair steps	If there are health workers who forget their account such as forgetting the user and password or filling in the wrong user and password, they can contact IT to follow up on repairing the account.

Source: Primary Data, 2024

Based on the results of the observation table above, it is known that each user and password for health workers is different, besides that in the process of creating a new account for health workers who have just entered the officer must first be confirmed by the person in charge, if the person in charge agrees, the person in charge will contact the IT Staff to create a new account for the incoming registration officer. If there are problems such as forgetting the user or password, the health worker will contact the IT Staff to overcome these problems.

Agree with (Hanafi, 2022). Confirmation is essential to any security framework, as it is the key to confirming the source of a message or that a person is who he claims to be. NIAG characterizes confirmation as a security level designed to establish the legitimacy of a transmission, message, or originator, or the implications of verifying an individual's authorization to obtain certain categories of data. In ordinary applications, many verification models have been illustrated, such as the most common, when we open an email we will be asked to enter a motto, when we need to make a budget exchange

through mobile banking or a payment gateway, we need two layers, specifically a secret word and a wand, when we enter a room. All that matters is to enter a finger print or ID card, and there are many more illustrations in ordinary applications.

In line with previous research conducted by Waisantoro, Rohmadi, and Mulyono (2014), it appears that the Surakarta Regional Clinic uses SIMRS with an inadequate confirmation security system, because the security verification of SIMRS cannot recognize clients on the system. . Security verification ostensibly exists as a pathway through which clients can enter the framework. As for information security in SIMRS, confirmation should be a part that also plays an important role. Indeed, although basically every officer has his or her own confidential statement, it does not guarantee that the security framework is running properly. Therefore, confirmation is needed to identify and authorize clients so that parties who have no interest in the security of the computer system can be identified as early as possible. If the verification (client validation) in SIMRS is appropriate, the health center will maintain information security legally.

Evaluation of Electronic Medical Record Data Security Electronic Medical Record Data Based on the Basis of Information Security on the Aspect of Authorization

Based on the authorization aspect of SIMRS BLUD RSUD Baubau City, that currently BLUD RSUD Baubau City does not have procedures governing the creation of accounts and their users. In addition, health workers cannot create their own accounts but only IT officers have access rights for this.

Table 2. Observation Results On The Authority Aspect

No	Objects observed	Description
1	SIMRS account creation SOP	At this time there are no procedures governing the creation of user accounts and restrictions on access rights, officers only make them according to reports received for account creation.
2	Account creation rights	The only officer entitled to create this account is the IT officer, who is responsible for creating the SIMRS account.
3	Electronic Medical Record Protection	Protection of electronic medical records is carried out by limiting the domain that can only be entered according to the domain and duties of the health employee.
4	Electronic medical record protection information	Information on the protection of electronic medical records is not officially carried out, because IT officers only convey that the use of SIMRS is limited according to the realm of each health worker in order to protect electronic medical records from data theft or data hacking. In addition, the understanding of the importance of medical records has also been understood by health workers that medical records are confidential and can only be accessed by responsible parties.

Source: Primary Data, 2024

Based on the results of the observation table above, it is known that there is no procedure related to making a SIMRS account, other than that making a SIMRS account will be made by IT staff. Each access right to use SIMRS is limited according to the domain owned by each health worker, electronic medical record protection information is carried out by means of notification that each SIMRS user is carried out according to the domain of each health worker not given full access to maintain the security of electronic medical record data from irresponsible parties.

In agreement with (Dhika and Hanipah, 2020), Get to Authorization is setting up security by using a secret word or key, when connecting devices to settings. This is often done so that the director can limit access to only selected clients who can interact with the agreement.

Usually in line with previous research conducted by (Vinta Aryanti Bintoro, Setya Wardhana and Dwi Agustin, 2022) that the control/authorization point of view is emphasized on the organizing officer to use various combinations of Client ID and Secret Word for each person or with other components to get to the client to exchange data related to confirmation and protection issues15. Considering article 12 paragraph (4) of the National Welfare Law of the Republic of Indonesia Number 269 of 2008, it states that in general, medical records belong to the patient. In this consideration, it

appears that Healing Center A and Healing Center B should be stored in an electronic therapy record system and logged in using the Client ID and Secret Word.

Evaluation of Electronic Medical Record Data Security of Electronic Medical Record Data Based on the Basis of Information Security on the Aspect of Confidentiality

At BLUD RSUD Baubau City in the Confidentiality/privacy aspect, the features of SIMRS cannot be fully accessed by health workers and can only be fully accessed by IT officers themselves, because full access rights can only be entered by health workers who have jobs such as IT, such as data processing officers.

Table 3. Observation Results On The Privacy Aspect

No	Objects observed	Description
1	Account usage access	On usage access, full access is only given by IT officers and some data processing officers in accordance with their domain.
2	Account usage	Health workers use their own accounts, so there has been no use of other officers' accounts because each account must have a different user and password.
3	System error in SIMRS	If there is a system error in SIMRS, there will be information by the IT officer along with the estimated time for repairing the system.
4	Data security system	The data security system is already available but the data security system is still a standard system and it can still be penetrated.

Source: Primary Data, 2024

Based on the results of the observation table, it is known that in privacy access, namely SIMRS owned by BLUD RSUD Baubau City, full access can only be done by IT officers and several other officers such as data processing officers, besides that officers also do not enter other officers' accounts because each officer has a different account according to the officer's domain, if an error occurs in SIMRS, it will be notified that it will be in the repair period and the estimate will be determined according to the repair period but the security system owned is a security system with a standard security level, this can make the system hacked.

Agreeing with (Stallings and Bauer, 2012), Protection ensures that people control or influence what data related to them can be collected and stored and by whom and to whom it can be disclosed. In addition, Information Privacy ensures that individual or confidential data cannot be accessed or disclosed by unauthorized persons.

In agreement with previous analysts (Vinta Aryanti Bintoro, Setya Wardhana and Dwi Agustin, 2022), the perspective of protection or confidentiality is the ownership of individual patient information and this security framework needs to be done because it is related to patient rights. Specialist doctors, dental practitioners, nurses and workers at Clinic A and Clinic B have Client ID and Watchword to guarantee security and get electronic medical record information by using cryptographic innovation and each healing center is equipped with firewalls and report documents as a guarantee to anticipate information leakage.

CONCLUSION

In the aspect of Authentification, each health worker account in using the SIMRS application has a different user and password. In the authorization aspect, each health worker can only use the menu features in the SIMRS application according to their respective domains, this is made so that data can be protected from irresponsible people. In the privacy aspect, full access to the SIMRS application can only be done by IT officers and data processing officers, besides that the data security system owned in SIMRS is only a standard system, this can still be hacked by irresponsible parties. We recommend that in the authentication, a face scanner be added for security so that the user account is not used by others.

It is better to do more official socialization about data security systems based on aspects of Authentication, authorization and privacy.

ACKNOWLEDGMENT

On this occasion, the author would like to thank Mr. Ahmad Amiruddin as the first supervisor who has helped and guided in writing scientific papers, Mrs. Niska Salsiani Sinta, S.KM., M.Kes as the second supervisor who has helped and guided in writing scientific papers, as well as family and friends who always support in any circumstances.

REFERENCES

A Nita, S. (2019) 'Sistem Informasi Kesehatan', Jurnal Informasi dan Pemodelan Kimia, 53(9), hlm. 1689-1699.

Anjani, D. dkk. 'Identifikasi, Penilaian, Dan Mitigasi Risiko Keamanan Informasi Dalam Sistem Rekam Medis Elektronik (Studi Kasus: Aplikasi ...', Academia.Edu [Preprint]. Tersedia di: Https://Www.Academia.Edu/Download/40964553/5211100190-Paper.Pdf.

Arief, MR (2010) 'Otentikasi, Kontrol Akses, Audit Sistem', Jurnal Dasi, 11(3), hlm. 73-76. Tersedia di: Https://Media.Neliti.Com/Media/Publications/91200-Id-Autentikasi-Kendali-Akses-Audit-Sistem-K.Pdf.

Dr. Umar Sidiq, M.Ag Dr. Moh. Miftachul Choiri, M. (2019) Metode Penelitian Kualitatif Dalam Pendidikan, Jurnal Informasi dan Pemodelan Kimia. Tersedia di: Http://Repository.Iainponorogo.Ac.Id/484/1/Metode Penelitian Kualitatif Dalam Pendidikan.Pdf.

Eka Siti Hastuti, Sri Sugiarsi Dan Sri Mulyono (2023) 'Analisis Tingkat Kesiapan Penerapan Rekam Medis Elektronik Di Puskesmas Kabupaten Boyolali', Jurnal Manajemen Informasi Kesehatan Indonesia (Jmiki), 11(2). Tersedia di: Https://Doi.Org/10.33560/Jmiki.V11i2.570.Fitri Apsari, A. *dkk.* (2022) 'Perlindungan Data pribadi pasien terhadap serangan cyber crime', *Sanskara Hukum dan Ham*, 01(02), hlm. 47–53.

Hanafi (2022) 'Dasar Cyber Security Dan Forensic', hlm. 236. Tersedia di: Https://Eprints.Amikom.Ac.Id/Id/Eprint/10688/.

Hanipah, R & Dhika, H. (2020), "Analisa Pencegahan Aktivitas Ilegal Didalamjaringan Dengan Wireshark," Journal Of Computer And Information Technology. Vol. 4, No.1, Hal. 11-23

Herlambang, P.M. *dkk.* (2020) 'Model Perilaku Keamanan Siber Pada Pengguna Sistem Informasi Kesehatan Selama Pandemi Covid-19', *Keamanan Siber Dan Forensik Digital*, 3(2), hlm. 27–33. Tersedia di: Https://Doi.Org/10.14421/Csecurity.2020.3.2.2152.

Irlaili, LD Dan Rohmadi, R.M.D. (2017) 'Tinjauan Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan Aspek Privasi, Integritas Dan Otentikasi Di Rsud Dr...', Rekam Medis [Preprint]. Tersedia di: Https://Www.Ejurnal.Stikesmhk.Ac.Id/Index.Php/Rm/Article/View/652.

Kesehatan, M. (2022) Peraturan Menteri Kesehatan Republik Indonesia Tentang Rekam Medis Elektronik Tahun 2022. Jakarta: Nanda, S. Roma Hasiani Oktavia, Sudra, R.I. dan Rohmadi (2009) 'Evaluasi Fitur Keamanan Data Dalam Sistem Registrasi Rawat Jalan Berbasis

Komputer Di Rumah Sakit Dr. Moewardi', Jurnal Kesehatan, 3(2), hlm. 22-41.

Mayang, S., Amirudin, A. dan Lestari, S.L. (2024) 'Desain Sistem Informasi Retensi dan Penyusutan File Rekam Medis di Rumah Sakit', Jurnal Retensi dan Penyusutan Rekam Medis di Rumah Sakit Sistem Informasi untuk Retensi dan Penyusutan File Rekam Medis di Rumah Sakit', Jurnal Sains dan Kesehatan, 3(1), hlm. 35-43. Sains dan Kesehatan, 3(1), hlm. 35-43. Tersedia di: https://doi.org/10.57151/jsika.v3i1.370.

Ningtyas, AM dan Lubis, IK (2018) 'Tinjauan Literatur Masalah Privasi Dalam Rekam Medis Elektronik', Pseudocode, 5(2), hlm. 12-17. Tersedia di: Https://Doi.Org/10.33369/Pseudocode.5.2.12-17

Nugroho, F. dan Ali, H. (2022) 'Penentu Simrs: Perangkat Keras, Perangkat Lunak, Dan Brainware (Tinjauan Literatur Sistem Pendukung Eksekutif (Ess) Untuk Bisnis)', Jurnal Manajemen Pendidikan Dan Ilmu Sosial, 3(1), hlm. 254-265. Tersedia di: Https://Doi.Org/10.38035/Jmpis.V3i1.871.

Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis', Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 Tentang Rekam Medis, 151(2), hlm. 10-17.

Sa, U. et al. (2024) 'Seminar Dan Lokakarya Internasional Aspek Keamanan Data Rekam Medis Elektronik Di Masyarakat 5. 0 Era Di Indonesia: Tinjauan Literatur Sistematis', hlm. 120setyawan, D.A. (2017) 'Mk Handout. Sistem Informasi Kesehatan Rekam Medis Elektronik (RME)', Program Studi Diploma IV Kebidanan, Departemen Kebidanan, Poltekkes Surakarta, hlm. 5–6.

Salsiani Sinta, N. dan Sulistiawan, W. (2022) 'Faktor-faktor yang menghambat pelayanan rawat jalan di Rumah Sakit Umum Daerah Kabupaten Buton', Jurnal Sains dan Kesehatan, 1(2), hlm. 30-42. Tersedia di: https://doi.org/10.57151/jsika.v1i2.46.

Silalahi, FD (2022) 'Keamanan Cyber', Penerbit Yayasan Prima Agus Teknik, hlm. 1–285. Tersedia di: Http://Penerbit.Stekom.Ac.Id/Index.Php/Yayasanpat/Article/View/367.

Sofia, S. dkk. (2022) 'Analisis Aspek Keamanan Informasi Data Pasien Dalam Penerapan RME Di Fasilitas Kesehatan', Jurnal Rekam Medis & Manajemen Informasi Kesehatan, 1(2), hlm. 94–103. Tersedia di: Https://Doi.Org/10.47134/Rmik.V1i2.29.Stallings, W. dan Bauer, M. (2012) Prinsip Dan Praktek Keamanan Komputer (Edisi Kedua). New York: Pearson. Doi: 10.1016/0142-0496(87)90093-2.

Tiorentap, DRA dan Hosizah, H. (2020) 'Aspek Keamanan Informasi Dalam Penerapan Rekam Medis Elektronik Di Klinik Pemeriksaan Kesehatan Mp', Prosiding ke-4 Perspektif Implementasi Fhir. ISBN: 978-623-6566-34-3, 4(0), hlm. 79–84. Tersedia di: Https://Prosiding.Esaunggul.Ac.Id/Index.Php/Fhir/Article/View/71.

Ulfa, N. Dan Yuspin, W. (2023) 'Legalitas Rekam Medis Elektronik (RME) Dalam Kesiapan Sistem Informasi Manajemen Rumah Sakit Berdasarkan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 Tentang Rekam Medis', Soepra, 9(1), hlm. 72–78. Tersedia di: Https://Doi.Org/10.24167/Sjhk.V9i1.6122.

Vinta Aryanti Bintoro, A., Setya Wardhana, E. dan Dwi Agustin, E. (2022) 'Evaluasi Format Rekam

Medis Elektronik Dan Sistem Keamanan Di Klinik Gigi Rumah Sakit Umum Kota Batam', Jurnal Medali, 4(1) , hlm. 1–10.

Wulandari, S. dkk. (2020) 'Penambahan Algoritma Kriptografi Untuk Keamanan Gambar Bitmap Sistem Informasi Rekam Medis Elektronik (Rme)', Jufdikes: Sisthana Jurnal Fisioterapi Dan Ilmu Kesehatan, 2(1), hlm. 52–65.