

EVALUATION OF FORMAT AND SECURITY OF DENTAL ELECTRONIC MEDICAL RECORD SYSTEMS IN GENERAL HOSPITAL BASED ON LEGISLATION

Erdianto Setya Wardhana*, Suryono**, Ari Hernawan***, Lukito Edi Nugroho****

* Doctorate Student Faculty of Dentistry Gadjah Mada University Yogyakarta

** Department of Periodontics, Faculty of Dentistry Gadjah Mada University Yogyakarta

*** Faculty of Law Gadjah Mada University Yogyakarta

**** Faculty of Engineering Gadjah Mada University Yogyakarta

Correspondence: erdianto.wardhana@unissula.ac.id

Keywords:

Dental electronic medical record, Complete format, Security system

ABSTRACT

Background: Electronic medical records in dentistry are the latest implementation in the health sector, especially dental health history to the services needed by patients by health care facilities and affect the format of dental, medical records and electronic medical record security systems. This study aimed to review the completeness of the medical record format and the electronic medical record security system of the dental polyclinic of the General Hospital in Batam City.

Method: This study used a descriptive cross-sectional observational design with two samples. Processing data in the form of tables and texts and conclusions as a result of research.

Result: The results showed incomplete dental electronic medical record formats at hospital A, such as patient identity, required medical data, odontogram, intraoral examination, and treatment chart, while Hospital B included patient identity, required medical data, intraoral analysis, treatment chart, and appendix. The two samples did not meet the integrity and non-repudiation aspects of the electronic medical record security system.

Conclusion: According to the Indonesian Dental Medical Record Guidelines, both samples have an incomplete dental electronic medical record format and security system.

INTRODUCTION

The development of technology and information systems in Indonesia is growing rapidly. One of the fields that benefits from technology and information systems is the health sector: they are used to improve the quality of health services in Indonesia. One of new inventions developed in the health sector is electronic medical records. Electronic medical records are stated in the Regulation of the Minister of Health of the Republic of Indonesia Number 269 of 2008 Article 2 paragraph (1). It is stated that medical records must be made completely and clearly in written or electronic forms. Also, in Article 2 paragraph (2) it is

stated that the management of electronic medical records is regulated by separate regulations. These underlie the development of information technology-based medical records in the health sector, especially in dentistry¹.

Hospitals in Indonesia have begun to implement electronic medical records as hospital management information systems in their services, including the field of dentistry. On the one hand, electronic medical records have many benefits, such as easy data access, ease of storage, and being environmentally friendly because they are paperless and effective in health services. On the other hand, electronic medical records also have

several weaknesses, such as data confidentiality, vulnerability against computer virus threats and high expense in application development⁷. Electronic medical records are more efficient for clinical documentation than written ones. However, its usage, especially in the completeness of data entry, has not yet reached 100%, so it may cause legal problems⁸. Several studies in the United States have found several weaknesses of electronic medical records, namely electronic medical record data is not stored properly, biased or missing⁹. Other research on electronic medical records was also conducted in RSUD Dr. Moewardi, Indonesia. In terms of integrity, it was found that there was no feature in the application for striking through a piece of medical data when there was an error in writing. In terms of availability, it was found that there were insufficiencies in the availability of the application. In terms of non-repudiation, it was found that the identification of parties who filled out and changed information was not optimal⁴.

Regarding the issue of privacy of electronic medical records, it was recorded that in May 2017, hundreds of hospital information systems in Europe were hacked by the WannaCry malware. 70% of the people were worried about personal health information leaks. This was proven by the sale of 130,000 medical records at the University of Chicago Hospital and Wilcox Memorial Hospital, Kauai, Hawaii⁶. This has drawn concerns towards the security of electronic medical record systems from many countries, including Indonesia. Therefore, confidentiality and security must be in accordance with the rules by the legislation and the policies of each hospital's management system. The use of electronic medical records, which is still in the stage of technological development, has raised many issues and challenges in ethics and applicable law due to unclear regulations for overcoming these challenges. Therefore, new

regulations must be formed specifically for electronic medical records so that they can be used in Indonesia⁵.

Based on this information, the author is interested in researching further about the completeness of format and security system of electronic medical records for dentistry in several hospitals in Indonesia.

RESEARCH METHOD

This research used a descriptive observational research with a cross sectional design. Samples in this research were Hospital A and Hospital B in Batam city. The names of the hospitals in this research were not stated explicitly as per the hospitals' requests. In this research, we could not add more samples because other hospitals did not yet have electronic medical record systems. This research received the ethical approval from Unissula FKG with Numbers: 280/B.1-KEPK/SA-FKG/VI/2021. The samples were chosen using the purposive sampling technique from the non-probability sampling method based on the inclusion and exclusion criteria. The research evaluated the completeness of format and the security system of the electronic dental medical records using a research instrument in form of checklist sheets. The checklist sheets contained dental medical record formats based on the Guide to Dental Medical Records from the Ministry of Health and the Minister of Health of the Republic of Indonesia Number 269 of 2008¹. In conducting the data analysis, the data results were presented in tables and explained in texts. After that, a comprehensive conclusion was drawn from the analysis.

RESEARCH RESULT

A. Hospital A

Table 1. Patient Identity

Contents of Electronic Medical Record	Completeness		
	Available	Not available	
Patient Identity	Name	√	
	Place and Date of Birth	√	
	ID Numbers	√	
	Gender	√	
	Ethnic group / Race	√	
	Occupation	√	
	Home Address	√	
	Home Phone numbers	√	
	Work Address	√	
	Cellular phone numbers	√	
			√
			√
			√

Table 1. Table 1. shows that work address format is unavailable.

Table 2. contents of Medical Data

Contents of Electronic Medical Record	Completeness	
	Available	Not available
Medical Data that require attention	Blood type	√
	Blood pressure	√
	Heart disease	√
	Diabetes	√
	Haemophilia	√
	Hepatitis	√
	Gastrin	√
	Other diseases	√
	Drug allergy	√
	Food allergy	√

Table 2. shows that there are no formats for heart disease, diabetes, haemophilia, hepatitis and gastrin. The format for blood type is included not in the Medical Data but Patient Identity column.

Table 3. Odontogram and Intra-oral Examination

Contents of Electric Medical Record	Completeness	
	Available	Not available
Odontogram	Map images of odontogram	√
	Writing of odontogram	√

Intra-oral Examination	Completeness	
	Available	Not available
Application/ server for writing odontogram	Occlusion	√
	Torus palatinus	√
	Torus mandibularis	√
	Palatum	√
	Diastema	√
	Dental anomaly	√
	Others	√

Table 3. shows that formats for odontogram and intra-oral examination are not available.

Table 4. Treatment Table

Contents of Electronic Medical Record	Completeness	
	Available	Not available
Treatment Table	Date	√
	Teeth being treated	√
	Symptoms and diagnosis	√
	ICD – 10 Codes	√
	Treatment	√
	Dentist's signature	√
Annotation	√	

Table 4. shows that there is no format for dentist's signature. However, dentist's signature will be replaced with User IDs and Passwords to access Electronic Medical Records. Other formats such as SOAP (Subjective, Objective, Assessment and Plan) will be developed in form of explanation and typed by dentists.

Table 5. Supplementary Attachment

Contents of Electric Medical Record	Completeness	
	Available	Not available
Supplementary Attachment	(informed/refusal consent)	√
	Laboratory and Radiology	√

Table 5. shows that Supplementary Attachment format is available in the Electronic Medical Record.

Table 6. Privacy or Confidentiality

Security System	Security System	
	Available	Not available
The security of accounts of doctors or health workers are guaranteed or not (using cryptography technology)	√	
User IDs or Passwords for doctors are provided to access	√	

Table 6. shows that doctors, dentists and health workers have User IDs and Passwords

Table 7. Integrity

Security System	Security System	
	Available	Not available
Information in electronic medical records cannot be changed without the consent from doctors or health workers who filled them first	√	
There is electronic signature of a doctor when he/she is writing in electronic medical records		√

Table 7. shows that there is no electronic signature format.

Table 8. Authentication

Security System	Security System	
	Available	Not available
The authenticity of information in electronic medical record can be accounted for (the people filling in forms with information are the doctors who treat patients)	√	
There is doctor's electronic signature when writing electronic medical record/ There are doctors' User IDs and Passwords for access	√	

Table 8. shows that patients visit to their desired polyclinics.

Table 9. Availability

Security System	Security System	
	Available	Not available
There is availability of information when needed	√	
There are supplementary systems in electronic medical records	√	

Table 9. shows that access to and usage of application are easy, its connection is fast, and its formats vary according to the guide to medical records from Electronic Medical Records available in each department/policlinic.

Table 10. Access Control

Security System	Security System	
	Available	Not available
User IDs and Passwords are secured	√	
How is the procedure of logging into the electronic medical records? Are User IDs and Password required?	√	

Table 10. shows that the first display of application, before accessing into Electronic Medical Records, consists of a login menu containing User ID and Password forms.

Table 11. Non-repudiation

Security System	Security System	
	Available	Not available
Digital track records can be viewed	√	
When a patient's data in his/her medical record is changed, health workers can ensure that such change does not erase other medical data history (any wrong data must not be deleted but be struck through with one line)		√

Table 11. shows that there is a lack in changing patients' medical record history data. If certain data is changed/corrected, the previous/wrong one must

not be deleted but be struck through so that health workers are able to recognize whether the data has been changed or not.

B. Hospital B

Table 12. Patient Identity

Contents of Electronic Medical Records		Completeness	
		Available	Not available
Patient Identity	Name	√	
	Place and Date of Birth	√	
	ID Numbers	√	
	Gender	√	
	Ethnic group / Race	√	
	Occupation	√	
	Home Address	√	
	Home Phone numbers		√
	Work address		√
	Cellular phone numbers	√	

Table 12. shows that home phone numbers and work address formats are not available.

Table 13. Required Medical Data

Contents of Electronic Medical Record		Completeness	
		Available	Not available
Medical Data that require attention	Blood type		√
	Blood pressure	√	
	Heart disease	√	
	Diabetes	√	
	Haemophilia		√
	Hepatitis		√
	Gastrin		√
	Other diseases	√	
	Drug allergy	√	
	Food allergy	√	

Table 13. shows that blood type, haemophilia, hepatitis and gastrin formats are not available.

Table 14. Odontogram and Intra-oral Examination

Contents of Electronic Medical Record		Completeness	
		Available	Not available

Odontogram	Map images of odontogram	√
	Writing of odontogram	√
	Application/server for writing odontogram	√
Intra-oral Examination	Occlusion	√
	Torus palatinus	√
	Torus mandibularis	√
	Palatum	√
	Diastema	√
	Dental anomaly	√
	Others	√

Table 14. shows that intra-oral examination format is not available.

Table 15. Treatment Table

Contents of Electronic Medical Record		Completeness	
		Available	Not available
Treatment Table	Date	√	
	Teeth being treated	√	
	Symptoms and diagnosis	√	
	ICD – 10 Codes	√	
	Treatment	√	
	Dentist's signature		√
	Annotation	√	

Table 15. shows that dentist's signature format is not available. However, it will be replaced with User IDs and Passwords.

Table 16. Supplementary Attachment

Contents of Electronic Medical Record		Completeness	
		Available	Not available
Supplementary Attachment	(informed/refusal consent)		√
	Laboratory and Radiology	√	

Table 16. shows that patient's informed/refusal consent format is not available.

Table 17. Privacy or Confidentiality

Security System	Security System	
	Available	Not available
The security of accounts of doctors	√	

or health workers are guaranteed or not (using cryptography technology)	
User IDs or Passwords for doctors are provided to access	√

Table 17. shows that doctors, dentists and other health workers have User IDs and Passwords.

Table 18. Integrity

Security System	Security System	
	Available	Not available
Information in electronic medical records cannot be changed without the consent from doctors or health workers who filled them first	√	
There is electronic signature of a doctor when he/she is writing in electronic medical records		√

Table 18. shows that electronic signature is not available.

Table 19. Authentication

Security System	Security System	
	Available	Not available
The authenticity of information in electronic medical record can be accounted for (the people filling in forms with information are the doctors who treat patients)	√	
There is doctor's electronic signature when writing electronic medical record/ There are doctors' User IDs and Passwords for access	√	

Table 19. shows that patients will visit to their desired polyclinics.

Table 20. Availability

Security System	Security System	
	Available	Not available
There is availability of information when needed	√	
There are supplementary systems in electronic medical records	√	

Table 20. shows that information is available, connection access is fast and formats of Electronic Medical Records are available in each polyclinic.

Table 21. Access Control

Security System	Security System	
	Available	Not available
User IDs and Passwords are secured	√	
How is the procedure of logging into the electronic medical records? Are User IDs and Password required?	√	

Table 21. shows that the first display before accessing into Electronic Medical Record consists of a login menu containing User ID and Password forms.

Table 22. Non-repudiation

Security System	Security System	
	Available	Not available
Digital track records can be viewed	√	
When a patient's data in his/her medical record is changed, health workers can ensure that such change does not erase other medical data history (any wrong data must not be deleted but be struck through with one line)		√

Table 22. shows that there is a lack in changing patients' medical record history data. If certain data is changed/corrected, the previous/wrong one must not be deleted but be struck through so that health workers are able to recognize whether the data has been changed or not.

DISCUSSION

The research was carried out in Hospital A and Hospital B, Batam City, by collecting data using observational techniques of the descriptive observational research in form of checklist sheets for determining the completeness of format and the

security system of the electronic medical records that were adapted to the Guidebook for Dental Medical Records¹. The checklist sheets were filled in by direct visits to the hospitals. The research results indicate that the two hospitals are still in the system development stage: their electronic medical record systems are not yet complete in terms of format and security.

The observation results show that office address format is not available in Hospital A and ID Numbers, ethnicity/race, occupation, home telephone and office address formats are not available in Hospital B (Table 1 and Table 12). Patient identity includes the process of collecting patient data or differentiation which includes patient's medical record numbers and identity. A complete patient identity form which includes name, place and date of birth, ID numbers, gender, ethnicity/race, age, home address, home telephone and medical record numbers administered to patients must be filled in completely and can be used as the main evidence that a patient has received care and treatment. One of important data in patient identity is age because it determines drug dosing. A wrong drug dosing will threaten patient's safety and hospital's name. Data about ethnicity/race is also very important in medical records because they can be used as ante mortem and post mortem data in forensic odontology. Ante mortem and post mortem data are used to determine a person's identity².

In this research it was shown that there were no odontogram and an intra-oral examination format in Hospital A and there was no intra-oral examination format in Hospital B (Table 3 and Table 14). Writing odontogram is very important for patient identification, especially in providing ante mortem and post mortem data. This is in accordance with The Regulation of The Ministry of Health

269/Menkes/PER/III/2008 concerning Medical Records Article 3 paragraph (1) letter I which states that dental medical records are equipped with odontogram. Intra-oral examination is needed to determine other characteristics in individual identification through forensics, namely the location of teeth protected by soft tissues such as lip muscles, cheek muscles, and gums so that in individuals who have trauma, their teeth will hit parts of the soft tissues¹³. This proves that writing odontogram and conducting an intra-oral examination is very important in assisting the process of investigating criminal and civil cases¹³.

The observation results show that both Hospital A and Hospital B do not yet have dentist's signature format in the treatment table (Table 4 and Table 15). The treatment table must be filled out by a dentist at the time of examination until the time of patient treatment. The treatment table contains treatment date, teeth being treated, symptoms and diagnoses, ICD – 10 codes, treatment, dentist signature and annotation formats. The Article 11 of the Republic of Indonesia Law Number 19 of 2016 states that electronic signatures are considered valid in the eyes of the law as long as they follow certain conditions. In the Medical Record Manual in Chapter V concerning Procedures for Organizing Medical Records, it is stated that the application of writing electronic medical record must include a signature and it can be replaced with a personal identification numbers (PIN)¹⁴.

In this research, it is shown that Hospital A provides complementary attachment (Table 5) and in the section of the informed/refusal consent there is a format for uploading scanned informed/refusal consent documents. In Hospital B, however, there is no format for uploading scanned informed/refusal consent documents (Table 16) because the hospital is still developing the system.

The privacy or confidentiality aspect involves the ownership of patient's personal data. For this, security system has access restriction because it is related to patient's rights. This research shows that every doctor, dentist, nurse and employee in Hospital A and Hospital B has a User ID and Password to ensure data security of electronic medical records and each hospital has firewalls and document archives as protectors so that there is no patient data leakage¹⁴ (Table 6 and Table 17).

Regarding the integrity aspect, data in electronic medical records that have been stored cannot be changed without acknowledgement of related doctor or dentist who wrote the medical records. The integrity aspect of electronic medical records as valid, appropriate documents in form of data storage and as verification for patient medical records is accompanied by the names of doctors, dentists, or other health workers involved, the name of the department/policlinic, the date and time of inputting patient's medical record which serve as substitutes for signature/barcode of doctor or dentist. This aspect is stated in Article 47 paragraph (1) of the Law of the Republic of Indonesia Number 29 of 2004 concerning the Medical Practice which states that medical records belong to doctors, dentists, or health care facilities, while the contents of medical records belong to patients. This research shows that Hospital A and Hospital B do not yet have electronic signatures of doctors or dentists (Table 7 and Table 18). Hospital A can apply for a program data improvement to the Hospital IT Unit with the approval of the Service and Medical Support Manager. In Hospital B, doctors or dentists can change already written data under 24 hours according to the name of the registrar. In the application of writing electronic medical record, it is obligatory to put a signature and it can be replaced with personal identification numbers (PIN)¹⁴.

Authentication aspect is related to patient rights. The authenticity of information can be accounted for so that the electronic medical record is correctly filled out by the doctor or dentist who treated the patient. In this research, Hospital A and Hospital B show that every doctor, dentist, or other health workers has User IDs and Passwords for logging into the system for writing medical records (Table 8 and Table 19). Article 1 paragraph 12 of the Law of the Republic of Indonesia Number 19 of 2016 concerning Electronic Information and Transactions states that electronic signatures are means of verification and authentication. However, electronic signatures can be replaced with personal identification numbers (PIN)¹⁴. Names of the registrars (doctors, dentists or other health workers), the name of the department/policlinic, and the date and time of the medical record input on the Electronic Medical Record display are required for data storage, verification of the patient's medical record, proving that it was properly recorded by the health worker concerned so that the record can be verified for its authenticity¹⁵.

The Availability aspect covers the availability of information in data processing that is available when it is needed and the use of an easy and fast system to be accessed from Electronic Medical Record data. Operations in the availability aspect are stated in Article 16 of the Republic of Indonesia Law Number 19 of 2016 concerning Information and Electronic Transactions. In this research, it is shown that Hospital A can access and use the application easily, with fast connection, and the application has various formats according to the medical record guidelines from the Electronic Medical Record that is available for each department/policlinic. The application can also allow users to upload documents in folders or scanned document format according to the patient's medical record numbers. Hospital A has a server in

form of firewall to prevent viruses entering the storage system (Table 9). Hospital B has good information availability, fast connection, various formats of the Electronic Medical Record that are available for each polyclinic, a data back-up feature for electronic medical record and a server in form of firewall to prevent viruses entering the storage system¹⁴ (Table 20).

The control access aspect emphasizes authentication and privacy issues in its consideration for regulating user access. Health workers are required to use User IDs and Passwords or other mechanisms for accessing the application to add or save information¹⁵. The Article 12 Paragraph (4) of the Minister of Health of the Republic of Indonesia Number 269 of 2008 states that the summary of the medical record belongs to patients. In this research, Hospital A and Hospital B show that their worker access to electronic medical record systems are secured as their workers can only log into the systems by using their User IDs and Passwords¹⁵ (Table 10 and Table 21).

The non-repudiation aspect covers digital track record that can be viewed by health workers. Changes in patient's medical record history data and the doer must be clearly recognized. This proves that an individual cannot deny his/her action after making changes in the system. The system will always record the time when certain data is being accessed until the data is saved. In this research, Hospital A and Hospital B indicated that there is no data change track feature that allows users to strike through certain data to be changed (Table 11 and Table 22). This data change track is in line with the Article 5 paragraph (6) of the Minister of Health of the Republic of Indonesia Number 269 of 2008 which states that:

“Correction as referred to in paragraph (5) can only be made by striking through the wrong

data with a line without deleting it, adding in new data and the signature of the doctor, dentist or certain health worker concerned.”

This is difficult to implement in electronic medical records. Therefore, there needs to be protection or ways to anticipate changes in data without deleting the previous data so that someone who conducts electronic transactions to obtain information in the Electronic Medical Record can be accounted for¹⁵.

CONCLUSION

1. The format of the electronic medical record in Hospital A is not complete since patient identity, required medical data, odontogram, intra-oral examination, and treatment table formats are not available. The security system of the electronic medical record in Hospital A has not met the integrity and non-repudiation aspects.
2. The format of the electronic medical record in Hospital B is not complete since patient identity, required medical data, intra-oral examination, treatment table, and complementary attachment formats are not available. The security system of the electronic medical record in Hospital B has not met the integrity and non-repudiation aspects.

REFERENCES

1. Kemenkes RI. Panduan Rekam Medis Kedokteran Gigi. 2015. 70 p.
2. Murniwati M. *Peran Rekam Medik Gigi Sebagai Sarana Identifikasi*, *Majalah Kedokteran Andalas*. 2012;36(2):163.
3. Karimah RN, Nurmawati I. *Kualitas Informasi Terkait Penerapan Hasil Desain Rekam Medis Gigi Di Klinik Sakinah Kabupaten Jember*. *J Ilm Inov*. 2016;16(2):109–15.
4. Nugraheni SW. *Aspek Hukum Rekam Medis Elektronik di RSUD Dr Moewardi*. 2018;1:92–7.

5. Budiayanti RT, Herlambang PM, Nandini N. *Tantangan Etika dan Hukum Penggunaan Rekam Medis Elektronik dalam Era Personalized Medicine*. J Kesehatan Vokasional. 2019;4(1):49.
6. Ningtyas AM, Lubis IK. *Literatur Review Permasalahan Privasi Pada Rekam Medis Elektronik*. Pseudocode. 2018;5(2):12–7.
7. Samandari NA, Chandrawila S W, Rahim AH. *Kekuatan Pembuktian Rekam Medis Konvensional Dan Elektronik*. Soepra. 2016;2(2):154–64.
8. Erawantini F, Nugroho E, Sanjaya GY, Hariyanto S. *Rekam Medis Elektronik: Telaah Manfaat dalam Konteks Pelayanan Kesehatan Dasar*. 2013;1(1):1–10.
9. Liu K, Acharya A, Alai S, Schleyer TK. *Using Electronic Dental Record Data for Research: A Data-mapping Study*. J Dent Res. 2013;92(May 2013):S90–6.
10. Komisi Akreditasi Rumah Sakit. *Instrumen survei. Instrumen Survei Standar Nas Akreditasi Rumah Sakit Ed 1*. 2018;
11. Joint Commission International. *Joint Commission International Standar Akreditasi Rumah Sakit. Standar Akreditasi Rumah Sakit. Jt Commission Int Ed 5*. 2014;(April).
12. Agung Prasetya Gunawan. *Gambaran Rekam Medis Gigi Puskesmas Bahu Kota Manado Ditinjau dari Standar Nasional Rekam Medik Kedokteran Gigi*. Jurnal e-GIGI. 2012;1, No 2:1–7.
13. Trisnowahyuni ., Rahim AH, Doloksaribu EI. *Rekam Medis Odontogram Sebagai Alat Identifikasi Dan Kepentingan Pembuktian Di Pengadilan*. Soepra. 2017;3(1):117.
14. Konsil Kedokteran Indonesia. *Manual Rekam Medis-Konsil Kedokteran Indonesia*. Buku Man Rekam Medis [Internet]. 2006;23.
15. Sutandra L. *Pengaruh Sistem Pengamanan Data Pasien di Rumah Sakit Menuju Era Revolusi Industri 4.0*. J Heal Sci Physiother. 2019;1(2):106–14.