

ISBN: 978-602-72150-9-2

# INTERNATIONAL SYMPOSIUM PROCEEDING



Cyber crime: Viewed from various perspectives of science and seminar results of research community services

Grandhika Hotel  
169 Dr. Mansyur St. Medan, Indonesia, 20122.

*February 15th, 2018*

**RESEARCH INSTITUTIONS AND COMMUNITY SERVICE  
UNIVERSITY OF MUSLIM NUSANTARA AL WASHLIYAH  
MEDAN**

# INTERNATIONAL SYMPOSIUM PROCEEDING

2018

Cyber crime: Viewed from various perspectives of science and seminar results of research community services

RESEARCH INSTITUTIONS AND COMMUNITY  
SERVICES (LP2M)  
UNIVERSITY MUSLIM NUSANTARA  
AL WASHLIYAH  
MEDAN  
2018

## INTERNATIONAL SYIMPOSIUM PROCEEDING 2018

Editor:

Prof. Dr. Dian Armanto, M.Pd., M.A., M.Sc (UNIMED)  
Dr. H. Yusnar Yusuf, M.S (PB. Al Washliyah)  
H. Hardi Mulyono, SE. M.AP (UMN)  
Asst. Prof. Dr. Worapat Paireekreng (Universitas Thailand)  
Prof. Dato' Dr. Abdul Rahman B Abdul Aziz (UUM)  
Prof. Dr. Ku Ruhana Ku-Mahamud (UUM)  
Senior Asst Prof. Dr. Hjh. Fatimah Binti Haji Awang Chuchu (Univ. Brunai)  
Prof. Hj. Sri Sulistyawati, SH, M.Sc, Ph.D (UMN)  
Prof. Dr. Ahmad Laut Hasibuan, M.Pd (UMN)  
Dr. H. Firmansyah, M.Si (UMN)  
Prof. Edi Warman, SH, M.Hum (USU)  
Prof. Dr. Khairil Ansari, M.Pd (UNIMED)  
Dr. Dahlia Lubis, MA (UIN-SU)  
Dr. Agus Sudibyso, S.I.P., M.Hum ( )  
Petrus Setyo Prabowo, S.T., M.T (Univ. Sanata Dharma)  
Dr. Risnawaty, M.Hum (UMN)  
Dr. Susi Deliani, M.Hum (UMN)

Reviewer:

Prof. Syamsul Arifin, SH, MH  
Dr. Mutsyohito Solin, M.Pd

Language Editor:

Dr. Yulia Arfanti, M.Hum  
Nelvitia Purba, SH, M.Hum, Ph.D  
Dra. Rosmawati Harahap, M.Pd, Ph.D  
Dr. Ridwanto, M.Si  
Dr. Anwar Sadat, SH, M.Hum  
Dr. Bambang Hermanto, M.Si  
Drs. Samsul Bahri, M.Si  
Drs. Hidayat, M.Ed  
Dr. Anggi Tyas Pratama  
Alkausar Saragih

Cover Design and Layout:

Dimas, Enny Fitria, Mariatul Suhaibah

Publisher:

LP2M UMNAW

Redaksi:

Kampus Abdul Rahman Shihab  
Jl. Garu II No. 52 Medan Telp. (061) 7867044  
Email: [lppmumn@gmail.com](mailto:lppmumn@gmail.com)  
Website: <http://lp2m-umnaw.ac.id/>

Distributor:

PT. Abdi Utama Perkasa  
Jl. Sisingamangaraja No. 124 Simp. Limun-Medan  
First print, Pebruari 2018

Anything involving licensing of quotations or the use of computer software for the making of manuscripts or other issues related to the intellectual property rights of the author of the article, and the legal consequences hich may arise thereof, shall be the sole responsibility of the author of the article.

## FOREWORD

Praise the presence of Allah SWT, who continuously pours His mercy and grace to us all, so International Symposium with theme "Cyber crime: seen from various perspectives of science and seminar result of research community services", can be done well so this Proceeding can be published. The theme was chosen with the reason to give the academic world attention in various scientific perspectives about the importance of cyber crime that still beum the attention of many people, including the world of college.

Researchers of higher education have produced much research both national and international research results related to issues of education, economics, language, communication and politics in facing the era of globalization, but still many have not been disseminated and published widely, accessible to people in need. On the basis of this, National Seminar The results of this research became one of the national Academics event to present their research, as well as exchange information and deepen the problem of research, and develop sustainable cooperation.

The seminar was attended by researchers from various fields of science from various universities in North Sumatra and other areas outside North Sumatra, which discussed various fields of study in economics, communications and politics in order to provide ideas and solutions to strengthen Indonesia's role in global competition and strengthen national identity.

Finally, we would like to thank the Head of the Muslim University Nusantara Al Washliyah, the Speakers, the Speakers, the Participants, the Organizing Committee, and the Sponsors who have sought to succeed the International Seminar on the Results of this Research. May Allah SWT give His blessings to all of us.

Medan, Pebruari 2018

Nelvitia Purba, SH, M.Hum, Ph.D

chairman of the committee

## PATIENT DATA SECURITY SYSTEM IN DIGITAL ERA (A REVIEW OF HEALTH POLICY)

Anggriani, Roni Gunawan  
Stikes Siti Hajar Medan, [anggriani@gmail.com](mailto:anggriani@gmail.com)  
Stikes Siti Hajar Medan, [roni.creation99@gmail.com](mailto:roni.creation99@gmail.com)

### *Abstract*

*The current digital era is a very dynamic development period including health care, especially in accessing and disseminating data on health services. Preliminary document studies show that patient data security is not fully maintained in this digital age, can be caused by the behavior of health workers, it can also be caused by illegal data retrieval through the internet system. This condition is currently not supported by an integrated policy, therefore a policy study that integrates patient data security systems in the digital age. The method of writing this article using literature review approach, where relevant policy documents will be tracked and analyzed integrally then using secondary data that support the results of writing this article. This study resulted that one of regulation of health only mentioned electronic data term as one kind of patient data, but not build up of security system that is Regulation of Minister of Health Number 269 year 2008 about Utilization of Medical Record. The digital patient data security system can be associated with electronic data strictly regulated in Law Number 11 of 2008 about Information and Electronic Transactions. Although not directly related to health, but this law is considered able to answer the digital patient-based data security system.*

**Keywords:** *data, patient, digital, policy*

### 1. INTRODUCTION

Electronic documents constitute any electronic information created, forwarded, transmitted, received or stored in digital, electromagnetic, optical or the like, which at any given time may be accessed for a particular interest understood by the public. The development of the fourth industrial revolution requires all organizations in the world to use digital technology directly as part of the Administration within their organizations.

Institutions of health services such as hospitals, clinics, and health offices are among the institutions that also directly follow the stream of digitalization in the development of the organization, because the efficiency and speed of information will be needed in the institutions mentioned above. In the context of

medical documents, in health terms can be applied to several things, one of which is patient data on health services institutions, or commonly used is medical record data.

The digital world also entered into the health system so that digital-based medic record processing became one of its development. Many of the benefits gained by memafaatkan digital technology on record medic, including electronic-based health record allows access and dissemination of a broad and comprehensive. It is also timely to obtain health information for health workers and other authorities, while maintaining patient's personal confidentiality and information from health personnel. In addition digital systems can also increase data protection against the confidentiality of information because it requires the

key and access control. The digitization of this data can improve the sustainability of services and play an important role as a resource for management of health care systems in knowledge development (CBPRI, 1999).

Policy of Health Ministry number 269 of 2008 concerning the use of medical records says that medical records are legal evidence in the process of law enforcement, discipline of medicine and dentistry and the enforcement of medical ethics and ethics of dentistry. Therefore, medical records are legal documents that are confidential. So the security of the file becomes very important to be maintained their otetication

One of the big problems if digitized is the problem of data security, this becomes one of the important aspects in an information system. This security issue is also a big concern for owners and managers of information systems that should be considered important and should be solved problem solving. In hospitals one of the less attention is the security of data on patient medical record applications.

Hospitals today are particularly vulnerable to Cyber attacks. Whereas today many hospitals in Indonesia are still many who keep the old IT devices that are not updated for years. For years hospitals have spent their budgets on patient care or medical equipment, thus setting aside a small budget for the development of Information Technology. Hospitals at the local level are particularly vulnerable because many try to install a large electronic medical record system, but with their own networks are often not ready to deal with security threats. Many lack of advanced firewall,

intelligence threats, data loss prevention tools, or access management tools.

This may be the cause of the data security vulnerability of the patient. Some articles also mention that the sale of patient medical record data in some countries occurs in the web market. All obtained from the results of the security breach of the patient's data are sold at with estimated price of about Rp. 10 million to Rp. 15 million per medical record. The patient's data can then be used in identity theft or fraudulent insurance claims (Aisyahisaura, 2018).

Based on these conditions, aka very absolute system of electronic data security to be stored in an integrated system, in addition to facilitate access, also keep the data security because it is a document of legal value. If we observe the current policy dynamics, there is no integrated policy that regulates the patient data security system, especially the medic record in Indonesia, so it is necessary to review a policy document that regulates the security of patient data in Indonesia.

This study aims to analyze the patient data security system in Indonesia in policy review. So through the writing of this article is expected to be useful as an input in the strengthening of policies in digital patient-based data security system. In addition, the writing of this article is also expected bermanfaat in the development of research kebijakan, especially the implementation of policies related to the security of data.

## **2. LITERATURE STUDY**

### **Data Security**

According Sabarguna (2008) that security in computerisation system consists of four aspects of

privacy, integrity, authentication, availability, while for the health world there are other aspects that are also not ak akhat important to note that access control and non-repudiation. Simply described below,

a) Privacy  
Privacy is an attempt to keep information from parties who do not have the right to access that information. Medical record data containing the patient's medical history which is a confidential document must always be kept confidential, because that information is owned by the patient. While the documents are owned by doctors, dentists, or health care facilities as set forth in Article 47 of the Act of Medicine No. 29 of 2004.

b) Integrity  
Regulation of the Minister of Health 269 of 2008, article 5, paragraph 6 states that "The correction as referred to in paragraph (5) can only be done by way of deletion without removing the corrected records and by the specified physicians, dentists or certain health workers. Therefore, it is not possible to write out the bias in electronic health records. Therefore, more security or protection is needed, that is not just delete the data stored in the electronic health record and all the changes can be known.

c) Authentication  
The medical record explains that not all health workers can enter data or make changes to data therefore electronic data must have an easy and specific accessibility called authentic. Each health worker must have their own capacities, therefore there is a need to restrict access only to certain people who can access it.

Article 46 of the Medical Practice Law No. 29 of 2004 states

that "every medical record should be marked with names, times and signatures of officers providing services or actions". In the same paragraph (3) states "if in the record recording medic using electronic information technology, the obligation of signing can be changed by using personal identity number (PIN)".

d) Availability  
Availability is an aspect that emphasizes that information when linked by related parties is available in just in time. As a medical record information tools must also terseedia quickly and can menampilkan back data that has been stored previously. Therefore, an electronic medic record should also have the nature of availability in the process.

e) Control of access  
Access control is an emphasis on the process and the technicalities that must be done in regulating access to information. Control over access also regulates parties or individuals who are entitled to access information in accordance with the will of data storage. This is done to limit the access of parties who are not ning who want to take advantage of data record digital medic.

f) Non-Denial  
In this aspect it is closely related to a transaction or change of information. This aspect helps prevent a person from disputing that he or she has made a transaction or change to an information.

### 3. RESEARCH METHODS

The methods used in the preparation of this article are library search and policy documents relating to digital-based data security systems. All data and information produced are

secondary because they come from the literature.

#### 4. RESULT AND DISCUSSION

##### Related policies

Some policies related to digital-based data security system, among others,

- a) Medical practice Act No. 29 of 2004
- b) Law No. 36 of 2009 on Health
- c) Law Number 11 Year 2008 on Information and Electronic Transactions
- d) Act No. 44 of 2011 on Hospitals
- e) Government Regulation number 46 of 2014 on Health Information System
- f) Permenkes 269 of 2008 on the use of medical records

The health law does not directly regulate the patient data system either manually or electronically. However, this law only regulates the rights and duties of patients in relation to the data. This is stated in article 8 concerning the right of the patient with the sound "Everyone is entitled to information about his or her health data including the actions and treatment he or she has received or will receive from the health worker".

This law only regulates the patient's rights in relation to the data, as this law is the principal law concerning health. In medical practice law is almost the same as health law, relating to patient data or medical records only regulates rights and obligations, only in medical practice laws is more detailed than ever before.

The regulation of medical records can be found in Article 46 paragraph (1) which states that "Every doctor or dentist in performing medical practice shall

establish medical records". The meaning of the medical record itself according to the explanation of Article 46 paragraph (1) of the Medical Practice Law is a file containing records and documents concerning patient identity, examination, treatment, action, and other services that have been given to the patient.

Furthermore, Article 47 of the Medical Practice Law provides that:

(1) The medical record as referred to in Article 46 shall be the property of the physician, dentist or health care facility, while the contents of the medical records shall be the property of the patient. (2) Medical records as referred to in paragraph (1) must be kept and kept confidential by doctors or dentists and leaders of health service facilities. (3) Provisions concerning medical record as referred to in paragraph (1) and paragraph (2) shall be regulated by Ministerial Regulation.

The patient's right to the contents of this medical record is also affirmed in Article 52 of the Medical Practice Law: "Patients, in receiving services to medical practice, have the right:

- a. To obtain a complete explanation of medical action as referred to in Article 45 paragraph (3);
- b. Ask for opinions from other doctors or dentists;
- c. Obtain services according to medical needs;
- d. Refuse medical treatment; and
- e. Getting medical records. "

Permenkes No.269 of 2008 on Compulsory Store of Medical Secrets. Everyone should be able to seek medical help with a feeling of security and freedom. The patient must be able to tell with open heart all the disturbing grievances, both

physical and spiritual, in the belief that the right is useful to heal himself.

Therefore the arena, every hospital always strives to maintain the security and confidentiality of medical records data with the best. One attempt to preserve medical record data is to write a secret word on the medical record file folder to explain that the contents of the folder are confidential. Then if the medical record file will be taken out of storage space then the carrier must be closed. Then when the medical record file is used in the care wards it is stored in a locked special cabinet.

Permenkes also regulates patient rights and obligations relating to medic record data. Based on the provisions of Article 12 paragraph (4) Permenkes 269/2008 it can be seen that the entitled to get a summary of medical records or medical resume are: 1). Patient, 2). Family Patients, 3). Persons authorized by patient or patient's family, 4). Persons who have written consent from the patient or the patient's family. So that out of these four subjects the hospital can be prosecuted if giving the patient medical record data to others who are not interested.

Then if you have done the request the contents of the medical record turned out to the hospital and / or the doctor did not want to give it. The Patient and / or Family may conduct legal efforts which are, among others, by suing and / or prosecuting the Hospital both civil and criminal (Article 32 letter q Law No.44 year 2009 on Hospital) and complaining about hospital services not in accordance with the standard of service through print and electronic media in accordance with the provisions of legislation (Article 32

letter r Law No.44 of 2009 on Hospital).

Of the overall policies that are directly related to health there is nothing directly related to electronically managing patient data. Permenkes is what directly says about electronic data, although not sepsifik set its security system. Permenkes said in Article 2 that 1) medical records should be made in writing, complete and clear or electronically. 2) The conduct of medical records using electronic information technology is further regulated by a separate regulation.

The results of the policy document search found no single article in the existing rules governing the patient data security system. So that the application of the patient's digital security system will be difficult if there are no rules that regulate digitally.

Document search conducted found that electronic data including health data, medical record data directly regulated in law No. 11 on Information and Electronic Technology.

In this law specifically regulate data security system. In the Electronic Health Record also must be given a signature for accountability. This is regulated in article 11 of the ITE Law, namely: Electronic signatures have legal force due to law as long as they meet the following requirements: 1) Electronic signature-related data is only attached to the signatory. 2) The data of electronic signature at the time of electronic signing process shall only be in the signatory term. 3) Any changes to electronic signatures occurring after the signing time are known. 4) Any change to electronic information relating to the electronic

signature after the date of signing may be known.

5) There are certain ways in which to identify who the signing is.

6) There is a certain way to indicate that the signatory has given approval to related electronic information.

In addition to other matters governed by Article 16 of the ITE Law, namely: 1. As long as it is not provided otherwise by a separate law, any Electronic System Enhancement shall operate an electronic system that meets the following minimum requirements:

1) Displays electronic Information and / or electronic documents in full according to the retention period applied in the laws and regulations.

2) Can protect the availability, wholeness. The discontinuance, confidentiality and accessibility of electronic information in the Electronic Systems Administration.

3) Can operate in accordance with the procedures or instructions in the Electronic Systems Holding.

4) Comes with any published procedures or instructions with language, information, or symbols that can be understood by the party concerned with the Electronic Systems Maintenance.

5) Have an ongoing mechanism to maintain the novelty, clarity, and responsibility of procedures or guidelines.

The Electronic Information and Transaction Act of 2008 is like the "broom of the universe" law which is a law that mangetur electronic system for all fields not yet set, including in the health field.

This law is very helpful for the development of digital patient-based data in Indonesia itself, although in the management of Electronic Medical Record itself, as

in article 13 paragraph (1) letter b Permenkes Number 269 of 2008 on the use of medical records "as legal evidence in law enforcement processes, medical and dental disciplines and the establishment of medical ethics and dental ethics ". Because medical records are legal documents, file security is very important to maintain the authenticity of data both Conventional Health Record and Electronic Medical Record. Since the enactment of the Electronic Information and Transaction Act (UU ITE) Number 11 Year 2008, the patient digitizing system is safer and answers the answers to the doubts. This law has provided an opportunity for the implementation of digitized patient data.

## 5. CONCLUSION

The conclusion in writing this iliah work is; there is no specific regulation in the health sector that regulates the digital patient-based data security system.

One health regulation only mentions the term electronic data as one type of patient data, but not mengatus security system that is Regulation of the Minister of Health No. 269 of 2008 on Utilization of Medical Record

The digital patient data security system can be associated with electronic data strictly regulated in Law Number 11 of 2008 Information and Electronic Transactions. Although not directly related to health, but this law is considered able to answer the digital patient-based data security system.

The government should improve the socialization of the implementation of ITE legislation in all aspects of the life of the nation, so

that the public understands the rights and obligations associated with the digitalization system in Indonesia. The government also specifically issues other regulations that support the application of specialized digitalization systems in the health sector, since the health sector has different characteristics compared to other aspects.

## 6.REFERENCE

- Aishayisaura. 2018.  
<https://www.aisyahisaura.com/menjaga-keamanan-data-pasien/>. Diakses tanggal 02 Februari 2018 pukul 21.22
- Computer-based Patient Record Institute .1999. CPRI Toolkit : Managing information System in Health care. Computer-based Patient Record Institute .Bethesda.
- Peraturan Pemerintah nomor 46 Tahun 2014 tentang Sistem Informasi Kesehatan
- Permenkes 269 tahun 2008 tentang pemanfaatan rekam medis
- Sabarguna, Boy. 2008. Manajemen Pelayanan Rumah Sakit berbasis Sistem Informasi. Yogyakarta. Konsorsium Rumah Sakit Islam Jawa Tengah . Semarang
- Undang-undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Undang-undang nomor 36 tahun 2009 tentang Kesehatan
- Undang-Undang Nomor 44 tahun 2011 tentang Rumah Sakit
- Undang-undang praktik kedokteran no 29 tahun 2004