Hospital Legal Responsibilities Against Misuse of Patient Personal Data in Electronic Medical Records

Dian Ayu Lukitasari[1], Mokhamad Khoirul Huda[2], Asmuni[3]
[1,2,3]Universitas Hang Tuah Surabaya, Surabaya, Indonesia
dianayu@gmail.com[1*], khoirulhuda@gmail.com[2], asmuni@gmail.com[3]

Abstract

The purpose of this study was to analyze the patient's personal data protection law in the electronic medical record and to analyze the legal responsibility of the hospital for the misuse of patient's personal data in the electronic medical record. This research uses normative research methods and uses statutory and conceptual approaches. The issuance of Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records which requires hospitals to maintain electronic medical records no later than December 31, 2022. The transition from conventional medical records to electronic medical records carries the risk of misusing patient personal data. The results of this study conclude that hospitals as personal data controllers and electronic system operators are required to implement Law Number 27 of 2022 concerning the Protection of Personal Data in organizing electronic medical records except those specifically regulated by other laws and regulations and hospitals as corporations have legal responsibilities for misuse of patient personal data in electronic medical records, namely administrative liability, civil liability, and criminal liability.

Keywords: electronic medical records, hospitals, liability, misuse of personal data

INTRODUCTION

The protection of personal data in the provision of health services, at the regulatory level, can be said to be very comprehensive. This protection is primarily related to patient medical record data, which from the start according to Law Number 29 of 2004 concerning Medical Practice (hereinafter referred to as the Medical Practice Law) has regulated the protection of patient medical records. Article 47 paragraph (2) of this law reads: "Medical records as referred to in paragraph (1) must be kept and kept confidential by doctors or dentists and heads of health service facilities."

Doctors or dentists are obliged to store, safeguard and protect all information obtained from their patients. Law Number 36 of 2009 concerning Health (hereinafter referred to as the Health Law) also regulates the obligation to protect a person's personal data. This confirmation also includes the protection of medical record data referred to and regulated in Law Number 44 of 2009 concerning Hospitals (hereinafter referred to as the Hospital Law), Law Number 18 of 2014 concerning Mental Health (hereinafter referred to as the Mental Health Law), Law Law Number 36 of 2014 concerning Health Personnel (hereinafter referred to as the Health Personnel Law), Law Number 38 of 2014 concerning Nursing (hereinafter referred to as the Nursing Law) and Law Number 35 of 2009 concerning Narcotics also guarantee the protection of personal data. To implement the above statutory regulations regarding medical records, information systems, hospitals, hospital and patient obligations, the Ministry of Health has also issued a number of derivative regulations.[1]

Health service facilities are required to keep electronic medical records and only certain bodies and people are allowed to open them. Electronic medical records stored by health service facilities must be connected/interoperable with the interoperability and health data integration service platform created by the Ministry of Health.

According to Article 28 paragraph (1) of the Minister of Health's Regulation on Medical Records, it states that "Health service facilities must provide access to all contents of a patient's Electronic Medical Record to the Ministry of Health." By providing access to the Ministry of Health, medical records will no longer be private information between patients and health service facilities, but will become public information. This has given rise to pros and cons among experts and the granting of considerable authority from the state to the Ministry of Health without being accompanied by strict rules regarding responsibility for the data and contents of medical records.[2]

Based on data from the Ministry of Communication and Information (hereinafter referred to as Kominfo) from 2019 to May 2021 there were 29 cases of violations of personal data protection. Among them, 93% are leaks of personal data, and 7% are violations of other personal data protection principles. And 92% of what causes personal data to be leaked is due to cyber crime.[3]

In 2021, Kominfo reported that there was a data leak of 279 million data which was confirmed from BPJS Health data. It is suspected that the leaked data was traded on a hacker forum called Raid Forums. All of the problems mentioned above require the Indonesian government to provide personal data security and regulate personal data protection and must immediately formulate laws and regulations that specifically provide legal protection for personal data.[4]

---

[1]Mirnayanti, Judhariksasawan, Analysis of Personal Data Security Regulations in Indonesia, Living Law Journal, Number 1, Volume 15, 2023. P.22.

[2]Tongon Fernando Hutasoit, Pan Lindawaty Suherman Sewu, Op.Cit. p.18355.

[3]Kominfo, 2022, Kominfo Responds to Alleged Data Leak of the Ministry of Health.https://aptika.kominfo.go.id. Accessed on February 20 2023, at 20.03 WIB.

[4]Ibid.

Many incidents of personal data being leaked have occurred both domestically and abroad. This leak of personal data has caused losses to society, especially to data owners whose data was leaked. The leak of personal data was also followed by misuse of personal data, including embezzlement of customer accounts, personal data being traded, fraud against other people using other people's personal data, and many other cases that have not been officially reported to Law Enforcement Officials. Many people do not yet understand the negative impact of misuse of their personal data by irresponsible people.[5]

Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the Personal Data Protection Law) which was ratified by President Joko Widodo on 17 October 2022 is a law drafted to provide legal protection for the personal data of Indonesian citizens.

In 2019, as reported by the Breach Industry Forecast by Experian Data Breach Resolution, there were three areas that frequently experienced personal data leaks, namely health, government and finance. The health sector has a high risk of personal data leakage because in the health sector it is closely related to health information and data which is very closely related to the confidentiality of patient personal data.[6]

And the latest is the sale of Covid-19 patient data on the darkweb forum Rapid Forums. The data stolen included name, citizenship status, date of birth, age, telephone number, home address, Population Identification Number (NIK), complete address and corona test results, where the patient provided this personal data information to the health facility when registering.[7]

The issue of protecting personal data arises because of concerns about privacy violations that could be experienced by individuals and/or legal entities. This violation of privacy can cause losses that are not only material but also moral, namely in the form of destroying the good name of a person or institution. Personal data in the health sector is not free from the possibility of misuse. It will be even more dangerous if the personal data is trace data of the patient's medical record which is very confidential.[8]

For the patient himself, if there is misuse of personal data such as NIK, cellphone number, and home address, this can be used by the perpetrator for crimes such as online loans or for false insurance rights claims, and for patients who have a history of diseases such as HIV and spread to the public, this will be at risk. ostracized by society because of his illness. If the public already knows that the hospital is experiencing misuse of patient personal data, this will greatly affect the image of hospital services and will have a big impact on the hospital.

RESEARCH METHODS

This research is normative juridical research, namely research that focuses on discussing the application of rules or norms in positive law.[9]Normative juridical research is research conducted based on primary legal materials by examining theories, concepts, legal principles and statutory regulations related to this research. This research is also known as library research, namely by studying books, statutory regulations and other documents related to research. This research uses a statutory approach and a conceptual approach. The statutory approach is generally used to examine statutory regulations whose norms still contain

[5]Government explanation (Ministry of Communication and Information) regarding the Personal Data Protection Bill in a working meeting with Commission I DPR RI, Jakarta, 25 February 2020.https://dpr.go.id. Accessed February 15, 2023.

[6]Muhammad Nur Afif, Information Security in Hospitals, Sabhanga Journal. Number 1, Volume 2, 2020, p.18.

[7]Ibid.

[8]Handryas Praseyo Utomo, Elisatris Gultom, Anita Afriana, The Urgency of Legal Protection of Patient Personal Data in Technology-Based Health Services in Indonesia, Galuh Justiti Scientific Journal, Number 2, Volume 8, 2020, p.4.

[9]Johny Ibrahim, Theory and Methodology of Normative Legal Research, Bayumedia, Malang, 2006, p.295.

deficiencies or can cause deviations at a technical level or in their implementation. This approach is carried out by analyzing all statutory regulations related to problems (legal issues) that are currently occurring and raised in this research. For example, this legislative approach is carried out by studying the conformity and synchronization between the Constitution and the Laws, or between one Law and another Law.[10]

RESULT AND DISCUSSION

A. Hospital Legal Responsibility for Misuse of Patient Personal Data in the Implementation of Electronic Medical Records

Personal data cannot be separated from the risk of misuse in the health sector, it is even more dangerous if the personal data is patient medical record data which is very confidential. Misuse of personal data that violates patient privacy can result not only in material losses but also moral losses such as damaging the good name of a person or institution.[11]

Based on Article 46 of the Hospital Law, hospitals have legal responsibility for misuse of electronic medical records and are legally responsible for losses incurred as a result of negligence by health workers at the hospital. This includes loss of medical records, damage, falsification of medical records and/or use of medical record data by other unauthorized persons.[12]

Based on the formulation in Article 46 of the Hospital Law, it can be concluded several things, firstly, that hospitals are responsible for losses that are limited to those caused by negligence in the absence of a security system that can prevent misuse of patient personal data in electronic medical records.

Second, the hospital is not responsible for the entire loss, if it turns out there was no negligence committed by the health workers or staff at the hospital. Third, the hospital is not responsible for actions carried out by health workers intentionally that cause harm to a patient. Fourth, the hospital must be responsible for all actions and decisions taken and carried out by health workers as long as these actions are proven to have been carried out and occurred at the hospital.[13]

The legal responsibility of hospitals in implementing health services, including providing protection for patients' personal data in electronic medical records, can be seen from the aspects of administrative law, civil law and criminal law.

The types of hospital legal responsibility for misuse of patient personal data in electronic medical records are as follows:

1. Administrative legal responsibility

The implementation of administrative law in the legal relationship between hospitals and patients is related to provisions which are requirements for the administration of quality and standardized health services. Violations of administrative law can be subject to administrative sanctions, including revocation of business permits or revocation of legal entity status for hospitals.[14]"In general, administrative sanctions in statutory regulations are associated with or as a consequence of a norm formulated in the form of a prohibition, order (necessity) or

[10]Ibid. p.321

[11]HP Utomo. E. Gultom, and A. Afroana. The Urgency of Legal Protection of Patient Personal Data in Technology-Based Health Services in Indonesia, Galuh Justiti Journal, Volume 8, Number 2, 2020, p.168-185.

[12]Basyarudin, Juridical aspects of electronic medical records used as evidence if health service errors occur, Cakrawala Ilmiah Journal, Volume 1 Number 12, 2022, p.3406.

[13]Calvin Anthony Putra, Analysis of Hospital Liability Regarding Potential Leakage of Electronic Medical Record Data Due to Cyber Crime, Novum Journal, Volume 1, number 1, 2022, p.7.

[14]Basyarudin, Op.Cit, p.3506.

obligation (obligation) which, if not accompanied by sanctions, will be difficult to apply effectively."[15]

Based on Permenkominfo 20/2016 PDPSE Article 36, every person who obtains, collects, processes, analyzes, stores, displays, announces, transmits and/or disseminates personal data without rights or does not comply with the provisions of this ministerial regulation or other statutory regulations subject to administrative sanctions in the form of: verbal warning; written warning; temporary suspension of activities; and/or announcements on sites within the network (online websites).[16]

Rizky PP Karo and Teguh Prasetyo in their book mention forms of administrative sanctions for electronic system operators which include but are not limited to not being able to maintain the confidentiality of personal data as regulated in PP 71/2019 Electronic System Operators article 100 consisting of written warnings, administrative fines, temporary suspension , termination of access and removal from the list.[17]

The Hospital Law, Health Law, and Medical Practice Law require hospitals to maintain safe medical records and protect the confidentiality of patient data. If a hospital does not fulfill these administrative obligations or requirements, then based on Article 46 of the Hospital Law, the hospital can be given administrative sanctions in the form of a reprimand. verbally or in writing, revocation of practice permits, non-renewal of operational permits, and/or fines and revocation of permits.

Regulations regarding administrative sanctions against the Personal Data Protection Law are regulated in Article 57 as follows: "Article 57 paragraph (1): Violation of the provisions of Article 20 paragraph (1), Article 21, Article 24, Article 25 paragraph (2), Article 26 paragraph (3), Article 27, Article 28, Article 29, Article 30, Article 31, Article 32 paragraph (1), Article 33, Article 34 paragraph (1), Article 35, Article 36, Article 37, Article 38, Article 39 paragraph (1), Article 40 paragraph (1), Article 41 paragraph (1) and paragraph (3), Article 42 paragraph (1), Article 43 paragraph (1), Article 44 paragraph (1), Article 45, Article 46 paragraph (1) and paragraph (3), Article 47, Article 48 paragraph (1), Article 49, Article 51 paragraph (1) and paragraph (5), Article 52, Article 53 paragraph (1), Article 55 paragraph (2), and Article 56 paragraphs (2) to paragraphs (4) are subject to administrative sanctions." "Article 57 paragraph (2) of the Personal Data Protection Law: Administrative sanctions as referred to in paragraph (1) are in the form of: written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines. Provisions for administrative sanctions for deleting and erasing personal data if the case occurs in a hospital and the personal data referred to are medical records, of course the deletion needs to be studied further because medical record data belongs to the hospital and is required to be stored in accordance with applicable statutory provisions. "

"Article 57 paragraph (2) letter a of the Personal Data Protection Law uses written administrative sanctions as warnings, which are more of a proof mechanism in trials or in the application of heavier administrative sanctions because the written administrative sanctions are not heeded by the violators." In the Personal Data Protection Law, Article 57 paragraph (2) letters b and letter c, administrative sanctions are included in the classification of government coercive measures, namely

[15]Wicipto Setiadi, Administrative Sanctions as a Law Enforcement Instrument in Legislation, Indonesian Legation Journal, Volume 6, Number 4, 2009, p. 606.
[16]Indah Maria Maddalena Simamora, Op.Cit, p. 1097.
[17]Rizky PP Karo and Teguh Prasetyo, Loc. Cit.

administrative fines or forced money (dwangsom).[18]

Article 57 paragraph (3). "Administrative sanctions in the form of administrative fines as intended in paragraph (2) letter d are a maximum of 2 (two) percent of the annual income or annual receipts for the violation variable." Article 57 paragraph (4) of the Personal Data Protection Law, "...the imposition of administrative sanctions as referred to in paragraph (2) is given by the institution." Administrative sanctions in the form of warnings or verbal/written warnings are the initial stage before moving on to the next stage of administrative sanctions. Administrative sanctions are carried out in stages from the lightest to the heaviest administrative sanctions.

Administrative sanctions can be directly applied to hospitals that violate established provisions. The implementation of administrative sanctions is faster than the imposition of criminal sanctions which must first go through a court process.[19]There is currently no implementation of administrative sanctions for hospitals that violate the provisions of the Personal Data Protection Law by a personal data protection supervisory agency/authority.

2. Civil law liability

A hospital is a legal entity or corporation whose existence and authority to carry out legal actions is recognized by civil law. So, in this case "the hospital can be sued and held accountable regarding every action, deed and policy carried out by medical personnel within the hospital."[20]

Civil lawsuits for misuse of personal data are intended to provide a form of compensation for misuse of the law. Civil lawsuits are based on an element of fault (fault liability, liability based on fault principle), this is regulated in Article 1365 BW. This civil lawsuit is based on two things, namely violating the law and error. People who cause harm to other people can be sued as long as the harm is the result of a violation of a norm (an act that violates the law) and the perpetrator can be regretted for violating that norm (a mistake). As explained in Article 1365 of the Civil Code which states that an act can be held legally responsible as long as it fulfills 4 (four) elements, namely the existence of an act, the existence of an element of error, the existence oflosses and the existence of a causal relationship between errors and losses.[21]

In this case, patients who have entrusted their personal information to the hospital have been harmed by the threat of misuse of the patient's personal data in the electronic medical record due to the hospital's negligence and there is a causal relationship between the error that occurred and the loss caused, namely an unlawful act.

According to M. Zamroni "hospital liability suffered by patients can be divided into two types, namely hospital liability due to the negligence of the hospital as a corporation and hospital liability due to the negligence of health workers in the hospital." The hospital is directly liable if it cannot carry out its obligations, causing harm to the patient. And it is also stated in article 46 of the Hospital Law that hospitals are responsible for all losses arising from the negligence of health workers in

[18]Teguh Prasetyo, Jamalum Sinambela, Application of Administrative Sanctions and Criminal Sanctions for the Theft of Personal Data from the Perspective of the Theory of Dignified Justice. LEGAL SPECTRUM JOURNAL, Volume 20, Number 1, 2023. p.65-66.

[19]Ibid.

[20]Sahat Maruli Tua Situmeang, Op.Cit. h. 38 - 52

[21]Ibid.

hospitals.[22]

Based on the description above, hospitals that are unable to carry out their obligations to provide protection for patient personal data in electronic medical records which results in misuse of patient personal data so that patients are harmed must be responsible for the loss. If there is negligence by hospital staff in processing personal data resulting in harm to the patient, the patient can sue the hospital for compensation. "This lawsuit can be filed regardless of the existence or non-existence of a contract between the two parties that creates an unlawful act."[23]

Rizky PP Karo and Teguh Prasetyo in their book mention the legal basis for a civil lawsuit if there is an alleged misuse of personal data (an unlawful act), namely Article 26 of the ITE Law which states that every person whose rights have been violated can file a lawsuit for losses incurred based on the law. In Perkominfo 20/2016 PDPSE Article 32, if consensus deliberation cannot resolve a dispute over a failure to protect personal data, then the owner of the personal data and the electronic system operator can file a lawsuit over the failure to protect the confidentiality of personal data.[24]In the Personal Data Protection Law, Article 12 states that personal data subjects in this paper, including patients, have the right to sue and receive compensation for violations of processing personal data about themselves in accordance with statutory regulations.

3. Criminal legal responsibility

Criminal responsibility means that every person who commits a criminal act or violates the law, as formulated in the law, that person should be held responsible for his actions in accordance with his fault, in other words the person who commits a criminal act will be held criminally responsible if he has a fault. , a person has a mistake if when he commits an action, it is seen from the perspective of society as showing a normative view regarding the mistake that the person has committed.[25]

"The basis for a criminal act is the principle of legality, while the basis for the perpetrator being punished is the principle of error." This shows that "the perpetrator of a criminal act will only be punished if he is guilty of committing the criminal act." "A person is declared to have committed a crime if he commits a criminal act, is above a certain age and is capable of responsibility, has a form of error in the form of intention or negligence and there is no excuse."[26]

Hospitals and health workers are obliged to maintain medical records. If this obligation is not carried out, the hospital or health workers may be subject to sanctions in the form of imprisonment or a fine. This is in accordance with the provisions of Article 79 of the Medical Practice Law which states that: "...Shall be punished with imprisonment for a maximum of 1 (one) year or a fine of a maximum of IDR 50,000,000.00 (fifty million rupiah)."[27]

If you do not keep medical secrets, you may be subject to criminal sanctions as regulated in the provisions of Article 322 paragraph 1 of the Criminal Code which states that "anyone who deliberately discloses secrets which he is obliged to keep because of his position or employment, whether current or former, is threatened with imprisonment for a maximum of nine month or a maximum fine of nine thousand

[22]M. Zamroni, Op. Cit. h. 79.
[23]Nasution, Bahder Johan, Health Law: Doctors' Liability. Rineka Cipta. Jakarta, 2013
[24]Rizky PP Karo fdan Teguh Prasetyo, Op. Cit. p. 100.
[25]Moeljatno, Op. Cit. p.41.
[26]Moeljatno, Principles of Criminal Law, Sixth Edition, PT. Rineke Cipta, Jakarta, 2000, p.5.
[27]Prilian Cahyani, Astutik, Op.Cit., pp. 220-221.

rupiah."[28]

Prior to the enactment of the Personal Data Protection Law, the application of criminal sanctions for misuse of personal data in electronic medical records by other people had previously been regulated in the ITE Law, Article 32, namely making "...parties who intentionally change, add, reduce, transmit, damage , removing, moving, hiding electronic information and/or electronic documents which causes the disclosure of confidential electronic information and/or electronic documents to be accessed by the public may be subject to sanctions in the form of imprisonment for a maximum of 10 (ten) years and/or a fine of up to a lot of IDR 5,000,000,000.00 (five billion rupiah)." These provisions are regulated in Article 48 paragraph 3 of the ITE Law. Thus "...the fulfillment of the elements is deliberate; change, add, reduce, transmit, damage, delete, move, hide electronic information and/or electronic documents; disclosure of confidential electronic information and/or electronic documents; can be accessed by the public, can be threatened with criminal sanctions and/or fines."

The Personal Data Protection Law also provides criminal sanctions against perpetrators of misuse of personal data. Criminal sanctions in the Personal Data Protection Law are imprisonment and fines and additional penalties can also be applied, namely confiscation of all profits obtained unlawfully from crimes against personal data.

Regulations regarding criminal sanctions regarding misuse of patient personal data in electronic medical records are contained in Article 67 in conjunction with Article 69 of the Personal Data Protection Law as follows:

Article 67 paragraph (1):

"Any person who intentionally and unlawfully obtains or collects personal data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the subject of personal data as intended in Article 65 paragraph (1) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000,- (five billion rupiah)."

Article 67 paragraph (2):

"Any person who intentionally and unlawfully discloses personal data that does not belong to him as intended in Article 65 paragraph (2) shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000,- (four billion rupiah)."

Article 67 paragraph (3):

"Any person who intentionally and unlawfully uses personal data that does not belong to him as intended in Article 65 paragraph (3) shall be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000,- (five billion rupiah)."

Article 68:

"Any person who deliberately creates false Personal Data or falsifies personal Data with the intention of benefiting himself or another person which may result in harm to others as intended in article 66 shall be sentenced to imprisonment for a maximum of 6 (six) years and/or a fine of a maximum a lot of IDR 6,000,000.00 (six billion rupiah)"

[28] *Ibid.*

Article 69: "In addition to being sentenced to criminal penalties as intended in Article 67 and Article 68, additional criminal penalties may also be imposed in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts and payment of compensation."

If misuse of a patient's personal data in an electronic medical record at a hospital is carried out intentionally by a health worker or hospital employee, thereby causing harm to the patient in accordance with the provisions stipulated in the Personal Data Protection Law, the health worker or hospital employee may be subject to sanctions. criminal penalties as stated in Article 67 in conjunction with Article 69 of the Personal Data Protection Law.

The criminal sanctions are in accordance with the Personal Data Protection Law Article 67 Paragraph 1 if a health worker or hospital employee "...deliberately and unlawfully obtains or collects personal data..." of patients in electronic medical records "...which do not belong to them with the intention of benefiting themselves himself or another person who may cause loss to the subject of personal data will be punished with imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000,000,000 (five billion rupiah)."

Based on Article 67 Paragraph 2, if a health worker or hospital employee "...deliberately and unlawfully discloses personal data that does not belong to him..." in this case the patient's personal data in an electronic medical record then "...will be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of IDR 4,000,000,000 (four billion rupiah)."

Based on Article 67 paragraph 3, if a health worker or hospital employee "...deliberately and unlawfully uses personal data that does not belong to him..." in this case the patient's personal data in an electronic medical record "...will be punished with a maximum imprisonment of 5 (five) years and/or a maximum fine of IDR 5,000,000,000 (five billion rupiah)."

Based on Article 68, if a health worker or hospital employee "...deliberately creates false Personal Data or falsifies personal data..." of a patient in an electronic medical record "...with the intention of benefiting themselves or another person which could result in harm to the person, they will be sentenced to imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp. 6,000,000.00 (six billion rupiah)."

It is also stated in Article 69 of the Personal Data Protection Law that in addition to being sentenced to criminal penalties as intended in Article 67 and Article 68, health workers or hospital employees "...intentionally misuse personal data..." patients in electronic medical records can also "...be subject to additional criminal penalties in the form of confiscation of profits and/or assets obtained or proceeds from criminal acts and payment of compensation."

After the lex specialis Personal Data Protection Law was passed, the application of criminal sanctions for criminal acts relating to personal data follows the provisions of the Law. The Personal Data Protection Law states the definition of "Every person is an individual or corporation". So that misuse of personal data by legal entities can be carried out by corporations, in this case including hospitals and third party Electronic System Operators

(PSE) who collaborate with hospitals.

"Corporations can be the subject of criminal acts, if they are committed by people based on work relationships or other relationships, whether carried out individually or jointly acting for and on behalf of the corporation both inside and outside the corporate environment." A corporation is subject to criminal sanctions if it can be proven that as a result of the violation of law the corporation obtained a profit or the criminal act was carried out for the benefit of the corporation, and it can be proven that the corporation allowed the criminal act to occur or whether the corporation did not take preventative steps, ensuring the implementation of applicable legal provisions to avoid the occurrence of a criminal act.[29]

Judges can impose criminal penalties against corporations or management, or corporations and management, but corporations can only be prosecuted for fines and additional penalties and/or disciplinary action. "The imposition of a crime against a corporation and/or its management does not preclude the possibility of a criminal being imposed on other perpetrators who, based on the provisions of the law, are proven to be involved in the criminal act."[30]

Based on the description above, hospitals as corporations can be held criminally liable due to misuse of patient personal data in electronic medical records in accordance with the criminal provisions of Article 67 and Article 69 of the Personal Data Protection Law as mentioned above. Based on Article 70, if the criminal offense referred to in Article 67 and Article 68 is committed by a hospital, "...crimes can be imposed on the management, control holder, order giver, beneficial owner..." and/or the hospital. The only penalty that can be imposed on a hospital is "...a fine of a maximum of 10 (ten) times the maximum fine threatened."

"In Article 70 of the Personal Data Protection Law, it is stated that apart from being sentenced to a fine, hospitals can be subject to additional penalties in the form of;

a. confiscation of profits and/or assets obtained or proceeds from criminal acts;
b. freezing all or part of the hospital business;
c. permanent prohibition on carrying out certain acts;
d. closure of all or part of business premises and/or hospital activities;
e. carrying out obligations that have been neglected;
f. payment of compensation;
g. revocation of hospital license; and/or
h. dissolution of the hospital."

Minister of Communication and Information Regulation Number 5 of 2020 concerning Private Electronic System Operators, states that "an electronic system operator is every person, state administrator, business entity, and community who provides, manages, and/or operates an electronic system individually or jointly to users. electronic system for his own needs and/or the needs of other parties." Private electronic system operators (hereinafter referred to as Private Scope PSE) are those operating electronic systems by people, business entities and the public, including hospitals.

[29]Asa Intan Primanta, Criminal Liability for Misuse of Personal Data, Jurist-Diction Journal, Volume 3, Number 4, 2020, p.1448-1451.
[30]Ibid.

Based on the discussion mentioned above, in accordance with the Minister of Health's Regulation on Medical Records, Article 9, hospitals "...can maintain electronic medical records using an electronic system developed by the Ministry of Health, the hospital itself or the electronic system provider through cooperation..." in this case is Private Scope PSE. The Private PSE must be registered and register the electronic system it uses with the Ministry of Health in accordance with statutory regulations.

If misuse of a patient's personal data in an electronic medical record at a hospital is carried out intentionally by a third party who collaborates with the hospital in administering electronic medical records, in this case Private Scope PSE, thereby causing harm to the patient in accordance with the provisions regulated in the Personal Data Protection Law, then Private Scope PSEs are legal entities so that misuse of personal data by legal entities can be carried out by corporations, in this case including PSEs that collaborate with hospitals.

Based on the description above, a third party that collaborates with a hospital in organizing electronic medical records, namely PSE. Private scope as a corporation, if they intentionally misuse a patient's personal data, can be held criminally liable in accordance with the criminal provisions of Article 67 and Article 69 of the Personal Data Protection Law as mentioned above. . Based on Article 70, criminal acts referred to in articles 67 and article 68 are committed by a Private Scope PSE as a criminal corporation and can be imposed on the management, control holder, order giver, beneficial owner, and/or the Private Scope PSE. The only penalty that can be imposed on Private Scope PSEs is a fine of a maximum of 10 (ten) times the maximum fine threatened. In Article 70 of the Personal Data Protection Law, it is stated that apart from being sentenced to a fine, Private Scope PSE as a corporation can be subject to additional penalties.

Apart from criminal sanctions, Private Scope PSEs who misuse personal patient data can also be subject to administrative sanctions based on Permenkominfo 20/2016 PDPSE Article 36, namely "...written warning; temporary suspension of activities; and/or announcements on sites in the network (online websites)." In PP 71/2019 Electronic System Operators article 100 consists of "...written warning, administrative fine, temporary suspension, termination of access and removal from the list...". In the Personal Data Protection Law, administrative sanctions are regulated in Article 57 in the form of: "...written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data, and/or administrative fines."

In the transitional provisions of Article 74 of the Personal Data Protection Law, hospitals as personal data controllers who process personal data in electronic medical records are obliged to adapt to the provisions for processing personal data based on the Law no later than 2 (two) years after the Law is promulgated or no later than October 17 2024.

CONCLUSION

Based on the research conducted, researchers can conclude thatProtection of patient personal data in the administration of electronic medical records has previously been regulated in various statutory regulations. And after the enactment of Law Number 27 of 2022 concerning Personal Data Protection which specifically regulates the protection of personal data for people in Indonesia, hospitals as personal data controllers and electronic system operators are obliged to implement this Law in protecting patients' personal data in electronic medical records except for those specifically regulated by other statutory regulations.

Based on the Personal Data Protection Law, forms of misuse of patient personal data include, firstly, disclosing medical record data without the patient's consent and not in accordance with statutory regulations, secondly, patient personal data is collected or obtained in an unauthorized manner without permission to access and without the patient's consent, thirdly The patient's personal data is used without the patient's permission, fourthly using fake

data or falsifying patient data to gain profit. In accordance with the Personal Data Protection Law, the hospital's legal responsibility as a corporation for misuse of patient personal data in electronic medical records is in the form of administrative responsibility, civil legal responsibility and criminal legal responsibility.

The implementation of administrative sanctions is carried out by a personal data protection supervisory institution/authority that has not yet been established by the Government. Meanwhile, civil legal responsibility hospitals for misuse of patient personal data in electronic medical records resulting in losses for patients, namely that patients can sue the hospital for compensation and also if a hospital as a corporation intentionally and unlawfully makes a mistake related to the misuse of a patient's personal data in electronic medical records, the hospital can be held liable for a criminal fine of up to 10 (ten) times the maximum fine threatened. Apart from being sentenced to fines, hospitals can be sentenced to several additional penalties, some of which include confiscation of profits and/or assets obtained or proceeds from criminal acts, closure of all hospital activities; revocation of hospital permits, and others.

REFERENCES

Legislation

Civil Code (KUHPerdata), Burgerlijk Wetboek Indonesia Staatsblad 1847 Number 23. Translated by R. Subekti and R. Tjitrosudibio, Cet.41, Balai Pustaka, Jakarta, 2014.

Criminal Code (KUHP), Translated by Moeljatno. Bumi Aksara, Jakarta, 2021.

Law Number 8 of 1999 concerning Consumer Protection. State Gazette of 1999 Number 22. Supplement to State Gazette Number 3821.

Law Number 39 of 1999 concerning Human Rights. State Gazette of 1999 Number 165. Supplement to State Gazette Number 3886.

Law Number 29 of 2004 concerning Medical Practice. 2004 State Gazette Number 166. Supplement to State Gazette Number 4431.

Law Number 11 of 2008 concerning Information and Electronic Transactions. State Gazette of the Republic of Indonesia 2008 Number 58. Supplement to State Gazette of the Republic of Indonesia Number 4843.

Law Number 35 of 2009 concerning Narcotics. State Gazette of the Republic of Indonesia 2009 Number 143. Supplement to State Gazette of the Republic of Indonesia Number 5062.

Law Number 18 of 2014 concerning Mental Health. 2014 State Gazette Number 185. Supplement to State Gazette Number 5571.

Law Number 36 of 2009 concerning Health. 2009 State Gazette Number 128. Supplement to State Gazette Number 6236.

Law Number 44 of 2009 concerning Hospitals, State Gazette of the Republic of Indonesia of 2009 Number 153. Supplement to State Gazette of the Republic of Indonesia Number 5072.

Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration. State Gazette of the Republic of Indonesia 2013 Number 232. Supplement to State Gazette of the Republic of Indonesia Number 5475.

Law Number 38 of 2014 concerning Nursing, State Gazette of the Republic of Indonesia of 2014 Number 307. Supplement to State Gazette of the Republic of Indonesia Number 5612.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. State Gazette of the Republic of Indonesia 2016 Number 251. Supplement to State Gazette of the Republic of Indonesia Number

5952.
Law Number 27 of 2022 concerning Personal Data Protection. State Gazette of the Republic of Indonesia for 2022 Number 196, Supplement to State Gazette of the Republic of Indonesia Number 6820.
Government Regulation Number 40 of 2019 concerning Implementation of Law Number 23 of 2006 concerning Population Administration as amended in Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration. State Gazette of the Republic of Indonesia 2019 Number 102. Supplement to State Gazette of the Republic of Indonesia Number 6354.
Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. State Gazette of the Republic of Indonesia Number 1829.
Regulation of the Minister of Health of the Republic of Indonesia Number 4 of 2018 concerning Hospital Obligations and Patient Obligations. State Gazette of the Republic of Indonesia Number 416.
Minister of Communication and Information Technology Regulation Number 5 of 2020 concerning Implementation of Private Scope Electronic Systems. State Gazette of the Republic of Indonesia 2020 Number 1376.
Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records. State Gazette of the Republic of Indonesia Number 829.
Decree of the Minister of Health, Number HK.01.07/MENKES/1423/2022 concerning Guidelines for Variables and Meta Data in the Implementation of Electronic Medical Records.

Book

Abdul Kadir Muhamad, Indonesian Company Law, First Edition, Citra Aditya Bakti, Bandung, 2010.
Indriyatno, Privacy and Personal Data Protection, Banyumurti.net, Jakarta, 2018.
Johny Ibrahim, Theory and Methodology of Normative Legal Research, Bayumedia, Malang, 2006.
Moeljatno, Principles of Criminal Law, Sixth Edition, PT. Rineke Cipta, Jakarta, 2000.
Moeljatno, Criminal Acts and Responsibility in Criminal Law, Rinneka Cipta, Jakarta, 1993.
M. Zamroni, Health Law: Liability of Doctors and Hospitals in the Practice of Medical Services, Scopindo Media Pustaka, Surabaya, 2022.
Nasution, Bahder Johan, Health Law: Doctors' Liability. Rineka Cipta, Jakarta, 2013
Peter Mahmud Marzuki, Introduction to Legal Studies, Kencana, Jakarta, 2008.
Rasyid Ariman & Fahmi Raghib, Criminal Law, Second printing, Setara Press, Malang, 2016.
Rizky PP Karo Karo, Teguh Prasetyo, Personal Data Protection Regulations in Indonesia Perspective of the Theory of Dignified Justice, Nusa Medika, Bandung, 2020.
Soekidjo Notoadmojo, Health Ethics and Law, First Edition, Rineke Cipta, Jakarta, 2010.
Titik Triwulan and Shinta Febrian, Legal Protection for Patients, Second Printing, Achievement Pustaka, Jakarta, 2010.

Thesis

Bagus Satryo Ramadha, Ability of Criminal Law Against Cyber Related to Personal Data Protection in Indonesia, Thesis, Master of Law, Islamic University of Indonesia. 2021.
Sri Lestari, The Role of Electronic Medical Records as Evidence of Therapeutic Transactions, Thesis, Master of Law University 17 August 1945 Semarang, 2021.

Journal

Afifaah Fitri Apsari, Anifatun Lutfiyah, et al, Protection of Patient Personal Data against Cyber Crime Attacks, Sansakara Journal of Law and Human Rights, Volume 1, Number 2, 2022.

Anggraeni Endah Kusumaningrum, Juridical Review of the Rights and Obligations of Patients as Consumers in Medical Services, Journal of the Supremacy of Law, Volume 2, Number 1, 2013.

Asa Intan Primanta, Criminal Liability for Misuse of Personal Data, Jurist-Diction Journal, Volume 3, Number 4, 2020.

Basyarudin, Juridical aspects of electronic medical records used as evidence if health service errors occur, Cakrawala Ilmiah Journal, Volume 1 Number 12, 2022.

Calvin Anthony Putra, Analysis of Hospital Liability Regarding Potential Leakage of Electronic Medical Record Data Due to Cyber Crime, Novum Journal, Volume 1, number 1, 2022.

Edy Santoso, Andriana, Insecurity in Consumer Data Protection in the eHealth Sector, De Jure Legal Research Journal, Volume 23, Number 1, 2023.

Endison Ravindo, Ariawan Gunadi, Legal Protection of Health Data Through Ratification of the Personal Data Protection Bill, Adigama Law Journal, Volume 4, Number 2, 2021.

Eriawan Agung Nugroho, Implementation of Republic of Indonesia Law No. 11 of 2008 regarding Information & Electronic Transactions on Electronic Medical Records, Juristic Journal, Volume 1, Number 3, 2020.

Evelyn Angelita Pinondang Manurung, Emmy Febriani Talib, Juridical Review of Personal Data Protection Based on Law Number 27 of 2022, Saraswati Law Journal, Volume 4, Number 2, 2022.

Faiz Rahman, Legal Framework for Personal Data Protection in the Implementation of Electronic-Based Government Systems in Indonesia, Indonesian Legislation Journal, Volume 18, Number 1, 2021.

Handryas Praseyo Utomo, Elisatris Gultom, Anita Afriana, The Urgency of Legal Protection of Patient Personal Data in Technology-Based Health Services in Indonesia, Galuh Justiti Scientific Journal, Number 2, Volume 8, 2020.

HP Utomo. E. Gultom, and A. Afroana. The Urgency of Legal Protection of Patient Personal Data in Technology-Based Health Services in Indonesia, Galuh Justiti Journal, Volume 8, Number 2, 2020.

Indah Maria Maddalena Simamora, Legal Protection of the Right to Privacy and Confidentiality of Disease Identity for Covid-19 Patients, Sibatik Journal Faculty of Law, Taumanagara University. Volume 1, number 7, 2022.

Jessy Anastasia Aruan, Legal Responsibility of Electronic Health System Managers in Indonesia as Electronic Providers in Relation to Data Protection, Dharmasisya Journal of the Master of Law Program, Faculty of Law, University of Indonesia, Volume 1, 2022.

Krista Yunita, Yuni Purwati, Sajiyati, Bambang Sukarjono, Implications and Socialization of the Law on Personal Data Protection in Maintaining the Confidentiality of One's Personal Data, DAYA-MAS Journal, Volume 7 Number 2, 2022.

Mirnayanti, Judhariksasawan, Analysis of Personal Data Security Regulations in Indonesia, Living Law Journal, Number 1, Volume 15, 2023.

Muhamad Hasan Rumlus, Hanif Hartadi, Policy for Combating Personal Data Theft in Electronic Media. Human Rights Journal, Volume 11, Number 2, 2020.

Muhammad Nur Afif, Information Security in Hospitals, Sabhanga Journal. Number 1, Volume 2, 2020.

Naya Amin Zaini, Legal Study of the Obligation to Fulfill and Protect Human Rights in the

Indonesian Constitution, Legal Panorama Journal, No. 2 Volume 1, 2016.
Neng Sari Rubiyanti, Implementation of Electronic Medical Records in Hospitals in Indonesia: Juridical Study, Alilah: Journal of Politics, Social, Law and Humanoria, Number 1, Volume 1, 2023.
Prilian Cahyani & Astutik, Criminal Liability for Misuse of Electronic Medical Records in Health Services, Soepra Health Law Journal, Volume 5, Number 2, 2019.
Sahat Maruli Tua Situmeang, Misuse of Personal Data as a Perfect Form of Crime from a Cyber Law Perspective, SASI Journal, Volume 27, Number 1, 2021.
Sekaring Ayumeida Kusnadi, Andy Usmina Wijaya, Legal Protection of Personal Data as a Right to Privacy, Al-Wasath Journal, Volume 2, Number 1, 2021, p.27
Siti Yuniarti, Legal Protection of Personal Data in Indonesia, BECOSS Journal, Volume 1, Number 1, 2019.
Teguh Prasetyo, Jamalum Sinambela, Application of Administrative Sanctions and Criminal Sanctions for Theft of Personal Data from the Perspective of the Theory of Dignified Justice. Legal Spectrum Journal, Volume 20, Number 1, 2023.
Tongon Fernando Hutasoit, Pan Lindawaty, Suherman Sewu, The Principle of Lex Specialis Derogate Legi Generalis is Linked to the Principle of Lex Superioti Derogat Legi Inferiori in Electronic Medical Records in Indonesia. Syntax Literate: Indonesian Scientific Journal. Number 12, Volume 7. 2022.
Wicipto Setiadi, Administrative Sanctions as a Law Enforcement Instrument in Legislation, Indonesian Legation Journal, Volume 6, Number 4, 2009.

Page

Ananthia Ayu, et al, Protection of Privacy Rights over Personal Data in the Digital Economy Era, Research Results of the Center for Case Research and Study and Library Management of the Registrar's Office and Secretariat General of the Constitutional Court, 2019.https://mkri.idaccessed on May 20 2023 at 19.30 WIB.
Government explanation (Ministry of Communication and Information) regarding the Personal Data Protection Bill in a working meeting with Commission I DPR RI, Jakarta, 25 February 2020.https://dpr.go.id. Accessed February 15, 2023.
Kominfo, 2022, Kominfo Responds to Alleged Data Leak of the Ministry of Health.https://aptika.kominfo.go.id. Accessed on February 20 2023, at 20.03 WIB.
KBBI. "Understanding Data".https://kbbi.web.id.Accessed on February 22 2023 at 19.00 WIB.
KBBI. “Personal Understanding.https://www.kbbi.idaccessed on February 22 2023 at 19.08 WIB.
Wahyudi Djafar, Paper presented as material in the public lecture "Legal Challenges in the Era of Big Data Analysis", Postgraduate Program, Faculty of Law, Gadjah Mada University, Yogyakarta, 26 August 2019.https://law.ugm.ac.id. accessed on May 15 2023 at 18.30 WIB.