

## **Hospital Corporate Criminal Liability for Electronic Medical Record Data Leak Linked to Patient Legal Protection**

**Yessy Agustina\*, Dey Ravena, Agus H. Rahim**

Universitas Islam Bandung, Indonesia

Email: [yessy\\_agst@yahoo.com](mailto:yessy_agst@yahoo.com)\*

---

### **ABSTRACT**

Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records requires Health Service Facilities, including hospitals, to organize Electronic Medical Records and are also obliged to maintain the confidentiality of the data in them. However, cases of Electronic Medical Record data leakage that occur rampantly make patient data vulnerable to exposure and even illegal trading. The objectives of this study are to analyze hospital policies on EMR confidentiality and examine the legal framework governing EMR management in Indonesia. The research method uses a normative juridical approach with descriptive research specifications involving synthetic and perspective analysis, while the data collection technique employs literature review and field studies. The results show that hospital policies for maintaining data confidentiality in Electronic Medical Record implementation must follow provisions in accordance with applicable laws and regulations as stated in Law Number 17 of 2023 concerning Health, Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records, and Law Number 27 of 2022 concerning Personal Data Protection. Hospitals must also act in accordance with the principles of good corporate governance. The corporate criminal liability model applicable to Electronic Medical Record data leaks occurring in hospitals positions the hospital as both the perpetrator of the crime and the responsible party; therefore, prosecution can be carried out and criminal sanctions can be imposed against the corporation itself.

**Keywords:** Electronic Medical Records, Hospitals, Data Confidentiality, Criminal Liability, Corporate Crime, Data Leakage

---

This article is licensed under [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/) 

## **INTRODUCTION**

Illness is one of the tests that Allah SWT gives to His servants. In the words of the Prophet *PBUH*, it is stated that if a person is sick, then healing can only occur with the permission of Allah, because Allah has prescribed a cure for every disease. Therefore, Muslims are forbidden to treat with something that is forbidden (*H.R* Abu Dawud No. 3372). This perspective emphasizes that health is not only a medical affair, but also has a spiritual dimension that connects humans to the Creator. This understanding forms the basis that efforts to obtain healing need to be accompanied by obedience to religious law (Ardinata, 2020; Hidayat, 2016; Rizki, 2020; Yulita, 2023).

Juridically, health is seen as the legal right of every citizen. Health Law Number 17 of 2023 Article 1 number 1 explains that health is not only limited to being free from disease, but also encompasses physical, mental, and social conditions that allow a person to live a productive life. This is in line with the 1945 Constitution, which guarantees the right of every citizen to obtain good health and environmental services. With the inclusion of the health clause in the 1945 Constitution, a new paradigm was formed whereby health is not just a personal matter, but the responsibility of the state.

Efforts to achieve an optimal degree of health are influenced by dynamic environmental, socio-cultural, economic, and biological factors (Ariana, 2016; Geme, 2012; Judi, 2017; Suryani, 2022). Through the National Health System, the government is committed

to providing services that are comprehensive, integrated, equitable, acceptable, and affordable for all levels of society. Initially, health efforts focused more on treatment, but now they have developed into health development that includes promotive, preventive, curative, and rehabilitative approaches. Thus, health services in Indonesia continue to be directed towards a more holistic approach (Dicky Rutanji Wing Wahyu Winarno, 2020; Indrayadi, 2023; Setiawan, 2021).

Health Law Number 17 of 2023 also affirms the role of Health Service Facilities, including hospitals, in providing comprehensive health services. A hospital is defined as a facility that provides inpatient, outpatient, and emergency services with promotive, preventive, curative, rehabilitative, and palliative approaches. In this context, doctors, hospitals, and patients are the three main subjects that are connected through medical relations as well as legal relations, with the aim of realizing optimal health for the community (Putra, 2022; Sunarso, 2012).

One of the important obligations of hospitals is the maintenance of medical records. Health Law Number 17 of 2023 Article 189 paragraph (1) letter h and *Permenkes* Number 24 of 2022 require every health service facility to maintain electronic medical records. Medical records contain the patient's identity, examination, treatment, actions, and services provided. This document has administrative, legal, financial, research, educational, and documentation values that can be accurately accounted for, known as the ALFRED AIR principle.

Digital transformation has also encouraged a change in the management of medical records from print to electronic form. Electronic medical records, as stipulated in *Permenkes* Number 24 of 2022, are created with an electronic system by ensuring data security and confidentiality. The government even requires all health facilities to implement this system no later than December 31, 2023. The digitization of medical records is expected to improve service efficiency, accelerate access to information, and minimize the risk of losing physical documents.

However, the implementation of electronic medical records is not free from challenges, especially those related to data security. Several cases of patient data leaks in Indonesia, such as at Majalaya Hospital, are evidence of weak data protection. The leakage of medical information can have serious impacts, ranging from psychological, social, and financial losses for patients, as well as eroding public trust in hospitals. This also raises potential legal sanctions for hospitals as corporations that neglect to maintain the confidentiality of medical data. The leak of electronic medical records puts hospitals in a position where they must legally account for their failures. From a criminal law perspective, hospitals as corporations can be held criminally liable for their negligence in maintaining the confidentiality of patients' medical records.

Previous studies have explored the challenges and legal implications of electronic medical record (EMR) management, but gaps remain. The first study by Sari et al. (2021) examined data security in Indonesian hospitals and found that insufficient cybersecurity protocols and lack of staff training significantly increase the risk of patient data breaches. However, the study primarily focused on technical aspects of EMR security and did not fully address the legal accountability of hospitals in the event of data leaks. The second study by Nugroho and Putri (2020) analyzed the legal framework governing patient privacy and EMR confidentiality under Health Law and the Ministry of Health regulations. While it highlighted

the normative obligations of hospitals, it lacked an in-depth discussion on the intersection of criminal liability, corporate responsibility, and patient protection in real-world scenarios. Both studies provide partial insights but do not integrate technological, legal, and ethical dimensions into a comprehensive model of hospital liability for EMR breaches (Hutauruk, 2013; Rusdiyanto, 2019; S, 2014).

Therefore, this study is important to examine the model of hospital criminal liability for the leak of electronic medical record data, especially within the framework of legal protection for patients. The urgency of this research lies in efforts to strengthen the legal, technological, and ethical systems in the management of health data in Indonesia. The study aims to provide both theoretical contributions to healthcare law and practical guidance for hospital management, regulatory bodies, and policymakers to enhance the security and legal accountability of EMR systems in Indonesia.

## **METHOD**

This study uses a normative juridical approach with literature research as the primary method (Suryana, 2010). The research focuses on analyzing laws, regulations, and secondary literature related to the criminal liability of hospital corporations for leaks of electronic medical record (EMR) data and their implications for patient legal protection. Descriptive, synthetic, and perspective analyses are applied to obtain a comprehensive understanding of the legal phenomena. Data sources include primary legal materials such as legislation and official documents; secondary sources such as books, journals, and interviews; and tertiary sources such as legal dictionaries, encyclopedias, and bibliographies. Data collection is carried out through literature review, field studies at Majalaya Hospital in Bandung Regency, interviews with relevant stakeholders, and online resources to ensure comprehensive coverage of both normative and practical aspects.

The data analysis is qualitative, focusing on grouping and interpreting information according to the research problem. Legal materials are analyzed in-depth to understand how existing laws govern corporate responsibility in cases of EMR data leaks and to evaluate the alignment of hospital practices with these regulations. This method allows for the integration of normative legal principles with empirical observations, ensuring a thorough understanding of how hospital corporate criminal liability relates to patient protection. The approach facilitates the identification of gaps in current regulations and provides a basis for recommending improvements in policy and hospital governance.

## **RESULTS AND DISCUSSION**

### **Hospital Policy in Maintaining the Confidentiality of Electronic Medical Record Data Linked to Patient Legal Protection**

Majalaya Hospital is one of the Health Service Facilities that organizes a Health Information System in an effort to achieve effective and efficient health. One of the hospital's obligations according to Article 189 of Law Number 17 of 2023 is to maintain Medical Records. The information contained in medical records is confidential because it describes the special relationship between doctors and their patients that must be protected from leakage in accordance with the medical code of ethics and applicable laws.

Majalaya Hospital has carried out its obligations regarding the implementation of Medical Records, but it is still conventional, namely in the form of medical documents in the form of paper. With the issuance of regulations regarding the obligation to implement Electronic Medical Records in accordance with the Regulation of the Minister of Health number 24 of 2022 which states that the implementation of Electronic Medical Records no later than December 31, 2023, makes Majalaya Hospital collaborate with third parties in its development. This is one of the rights of hospitals, namely to cooperate with other parties in the development of services, one of which is in the development of the Hospital Information System (SIMRS). The cooperation carried out by Majalaya Hospital with a third party, as an Electronic System Operator, is carried out in accordance with article 9 of the Regulation of the Minister of Health Number 24 of 2022 concerning Medical Records (Tamarell Vimy et al., 2022).

The collaboration made by Majalaya Hospital with a third party occurred in June 2022, while Minister of Health Regulation Number 24 of 2022 was only issued on August 31, 2022. Cooperation agreements with third parties in the development of hospitals are carried out within a period of 3 years. So when the Minister of Health Regulation on Medical Records is issued, the cooperation is still ongoing and the provisions in the Regulation of the Minister of Health must be fulfilled.

The provisions in the article are explained that the implementation of Electronic Medical Records can be through cooperation with electronic system operators who are registered as Electronic System Operators at the Ministry responsible for the field of communication and informatics in the health sector in accordance with the provisions of laws and regulations. However, until the time of the interview, the third party has not been registered as an Electronic System Operator at the Ministry responsible for the field of communication and informatics in the health sector.

Third parties are also known to have not been certified by the Reliability Certification Agency, as evidenced by the absence of a *trust mark* logo on the *home page* of the application developed by a third party in collaboration with hospitals, in accordance with article 10 of the Law of the Republic of Indonesia, Number 11 of 2008 concerning Information and Electronic Transactions, which states that every business actor who organizes electronic transactions can be certified by the Reliability Certification Institution is shown by the existence of a certification logo in the form of a *trust mark* on the *business actor's homepage*.

In addition, to maintain the security of Electronic Medical Record data, there is no integrity pact or *NonDisclosure Agreement (NDA)* attached when entering into a cooperation agreement between third parties and hospitals.

Article 297 paragraph (3) of Law Number 17 of 2023 concerning Health, reaffirms that Health Service Facilities are obliged to maintain the security, integrity, confidentiality, and availability of data contained in medical record documents. Officials and administrators who are in direct contact with third parties, namely PPK, PPTK and as a support team are less responsive to the provisions imposed in accordance with laws and regulations.

Access to the application system can be done from outside the hospital without a security system first. Access to the application that is being developed uses the *username* and *password* given to each user in the hospital. However, due to the user's ignorance of the confidentiality of access that must be maintained, in the end the *username* and *password* that

has been given to each user are known by other users and not only one user but many users. The procedure of closing access after using the application is also not always done by the previous user so that it can be used by the next user on the same device. This is contrary to Article 347 paragraph (2) of the Health Law No. 17 of 2023 concerning Health, which states that systems operated in hospitals must meet certain reliability standards, including maintaining data confidentiality and privacy, as well as establishing procedures for data access rights. Hospitals are responsible for protecting the information contained in medical records against the possibility of loss of information or falsification of data contained in medical records or used by unauthorized persons. Majalaya Hospital does not have a policy or Standard Operating Procedure (SPO) in regulating these access rights, especially the policy of who is responsible for the *database* of all *stored usernames* and passwords.

In addition, a direct connection to *the server* inside the hospital can be accessed from outside the hospital by anyone without any policy regarding who can access from outside the hospital, in what way, and what kind of access protection is used.

The above things are considered to be a loophole in the leak of Electronic Medical Record data that is being developed at Majalaya Hospital which is then traded on social media. Not only patient clinical data in the Electronic Medical Record, but also personal data that must be protected in accordance with Article 29 paragraph (1) of Law number 39 of 1999 concerning Human Rights which states that "everyone has the right to the protection of personal data, so in the statement, a conclusion can be drawn about the protection of personal data is a right (*privacy rights*) which belongs to everyone that must be protected by the state, where in *privacy rights* everyone has the right to close or keep secret matters of a personal nature".

Linear with Law number 39 of 1999 concerning Human Rights, in Article 1 number 22 of Law Number 24 of 2013 of 2006 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, states that "Personal Data is certain individual data that is stored, maintained, and maintained truthfully and protected confidentially". In the 1945 Constitution, article 28G paragraph (1) also states that "Everyone has the right to the protection of personal self, family, honor, dignity, and property under his or her control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right".

In accordance with Article 46 of Law Number 27 of 2022 concerning Personal Data Protection, namely "Failure to protect Personal Data is the failure to protect a person's Personal Data in terms of confidentiality, integrity, and availability of Personal Data, including security breaches, whether intentional, that lead to destruction, loss, alteration, unauthorized disclosure or access to the Personal Data sent, stored, or processed"

From the above statements, Majalaya Hospital is legally responsible in accordance with Article 193 of Law No. 17 of 2023, which states that the Hospital is legally responsible for all losses incurred due to negligence committed by health human resources in the hospital.

The follow-up carried out by Majalaya Hospital is in the form of checking each *personal* computer, conducting forensic hospital servers, changing *database passwords* and migrating database servers, changing passwords for all server access, checking *unknown users*, *monitoring* user, and close all server and database access so that it cannot be accessed from outside the hospital, then report it to BPJS Kesehatan and to the Bandung Regency

Communication and Information Office (Diskominfo) is a form of the hospital's responsibility for data security.

Obligations that are not fulfilled by electronic system operators in accordance with Government Regulation Number 71 of 2019 Article 24 paragraph (3) it is stated that the Electronic System Operator is obliged to secure the components of the Electronic System in the event of a failure or system disruption that has a serious impact as a result of the actions of other parties to the Electronic System, the Electronic System Operator is obliged to secure Electronic Information and/or Electronic Documents and immediately report at the first opportunity to law enforcement officials and related ministries or institutions, as well as Article 26 paragraph (1), namely that electronic system operators are obliged to maintain the confidentiality, integrity, authenticity, accessibility, availability, and traceability of electronic information and/or electronic documents in accordance with the provisions of laws and regulations.

With the case of leaking Electronic Medical Records and not communicating them to the public, hospitals do not organize good *corporate governance*, which is a prerequisite for every government to realize the aspirations of the community and achieve the goals and ideals of the nation that require the implementation of an appropriate and clear accountability system.

Hospitals do not carry out good governance, especially according to the principles stated by Sedarmayanti, namely:

- 1) Accountability, hospitals should be able to make good decisions and be accountable to the community and the owners (*stakeholders*), and are obliged to act as the responsible and the plaintiff for all actions and policies that it sets. The hospital followed up on the technical data leak and also reported it to BPJS and Diskominfo, but did not report it to BSSN (State Cyber and Cryptography Agency).
- 2) Transparency, in Article 351 of Law Number 17 of 2023 concerning Health, and Article 46 of Law Number 27 of 2022 concerning Personal Data Protection, that Health Information System Operators are obliged to inform data owners, the public and institutions if there is a failure of data protection. The hospital is not transparent to the public that there has been a leak of Electronic Medical Record data, so the public does not know that their personal data and clinical data are being sold.
- 3) Openness, due to the lack of transparency of hospitals, does not occur the principle of openness where the public cannot submit responses and criticisms to the case of leaking Electronic Medical Record data.
- 4) Legal Rules, hospitals do not fully comply with the rules that have been set by law in the implementation of cooperation with third parties, and hospitals do not be careful in developing SIMRS, especially regarding the security of Electronic Medical Record data in accordance with the mandate contained in laws and regulations, so that there is a leak of Electronic Medical Record data.

Not only hospitals, accountability must also be carried out by the Regional Government through the Head of the Health Office because the implementation of SIMRS in hospitals is carried out by the Regional Government through the Head of the Health Office in accordance with the Regulation of the Minister of Health Number 82 of 2013 concerning Hospital Management Information System Article 10.

**Hospital Corporate Criminal Liability Model for Electronic Medical Record data leak in an effort to provide legal protection for patients.**

It is stated in Article 351 of Law Number 17 of 2023 concerning Health and Law Number 27 of 2022 concerning Personal Data Protection Article 46, that Health Information System Operators are obliged to inform data owners if there is a failure in data protection. This is also regulated in Law Number 19 of 2016 concerning Information and Electronic Transactions, in Article 26 paragraphs (1) and (2) which states that any information through electronic media that concerns a person's personal data must be done with the consent of the person concerned, and every person whose rights are violated can file a lawsuit for the losses caused. The stipulated provisions have given the right to the owner of personal data to maintain the confidentiality of his personal data, if his personal data has been spread and can be misused by other parties, then the owner of personal data can file a lawsuit in court.

In the case of criminal liability, the delicacies in the Criminal Code cannot necessarily be applied, because there is a principle of legality as stated in article 1 paragraph (1) of the Criminal Code which states that *"no act can be punished, except based on the strength of the provisions of the law that pre-existed"*.

The leak of Electronic Medical Records that occurred at Majalaya Hospital is included in criminal law, because it fulfills two main things in accordance with the theory put forward by Sudarto, namely:

***An act that meets certain conditions.***

In Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, in article 40 it is stated that "The Government determines agencies or institutions that have strategic electronic data that must be protected". It is very clearly emphasized in the Regulation of the Minister of Health number 24 of 2023 concerning Medical Records, in Law number 17 of 2023 concerning Health that Electronic Medical Record data is confidential. In fact, because the Electronic Medical Record contains personal data, Law Number 27 of 2022 concerning the Protection of Personal Data and Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration also apply. Not only that, because Electronic Medical Records contain Electronic Transactions which is a legal act, Law number 11 of 2008 concerning Information and Electronic Transactions also applies. And all of the provisions mentioned above state that Electronic Medical Record data is confidential and must be protected. Meanwhile, in the development of Electronic Medical Records carried out at Majalaya Hospital, data that should be kept confidential in accordance with the applicable laws and regulations above, in fact there was a leak.

***Punishment***

There are criminal sanctions that regulate the consequences of the leak of Medical Records. Hospitals are legal subjects in the form of corporations that can be held accountable. Majalaya Hospital can also be prosecuted as a criminal perpetrator based on the provisions of article 193 of the Health Law Number 17 of 2023 which states that the Hospital is legally responsible for all losses incurred due to negligence committed by the Hospital Health Resources. Administrators in hospitals can be held accountable for criminal acts committed

due to negligence, in accordance with Law No. 1 of 2023 concerning the 2023 Criminal Code Law Article 36. This also falls into the objective element of a criminal event according to Van Apeldorn, which is an act that is contrary to positive law, which causes consequences that are prohibited by law with the threat of punishment. According to Sauer, if the criminal defendant in his actions does not try to be careful, so as to cause unintended consequences, but which he can know in advance, then there is a "mistake" (in the narrow sense. In the case of a data leak at Majalaya Hospital, the officials involved were not careful in maintaining the confidentiality of the Electronic Medical Record data so that the leak occurred.

The leakage of Electronic Medical Record data is due to a lack of care from administrators and/or officials who are directly related to and involved in the procurement of Electronic Medical Record Development, and a lack of special attention to the risk of data leakage. Management and officials neglect the provisions of the laws that have been set. This is in accordance with the theory put forward by Wirjono, and is included in the term *Culpa* which is the fault of the management due to his lack of carelessness so that bad consequences are accidental, and the theory according to Van Hamel quoted by Andi Hamzah that negligence is divided into 2 types, namely "lack of necessary foresight" and "lack of necessary care" While according to Law Number 1 of 2023 concerning the Criminal Code in The explanation of Article 474 paragraph (1) explains that forgetfulness shows that the perpetrator does not want a great deal of his deeds to occur. However, in actual occurrence it is difficult to determine that an act can be called forgetfulness. Therefore, based on these considerations, the definition of forgetfulness is left to the judge's consideration to assess the case at hand.

Majalaya Hospital is a form of corporation with a legal entity in the form of a regionally owned business entity. Loebby Loqman in one of his opinions stated that corporations that can be held criminally accountable are corporations that have been incorporated into law, because the composition of the management and the extent of the rights and obligations in the corporation are clear. Meanwhile, H. Setiyocono stated that "Corporation is a term commonly used by criminal law and criminology experts to refer to a legal entity (*rechtspersoon*), *Legal Body* or *Legal Person*".

The perpetrators of the crime in this case are administrators and officials who are within the scope of the hospital as a corporation. Criminal acts that occur at Majalaya Hospital, which is a corporation, are criminal acts committed by management/officials who have functional positions in the corporate organizational structure and based on employment relationships who act for and on behalf of the corporation in accordance with Article 45 and Article 46 of Law number 1 of 2023 concerning the Criminal Code.

Referring to article 1365 of the Civil Code, that every person who violates the law and causes damages, will be responsible for providing compensation for the losses caused, this liability can be replaced or charged to the party responsible for a person for the actions carried out by the party who is his dependents or known as *vicarious liability*. This also applies to the case of leakage of Electronic Medical Record data at Majalaya Hospital. Managers and officials who have been negligent are the dependents of the hospital that employs them. So the responsibility does not lie with individuals, but is charged to hospitals as corporations. This is also in line with the *doctrine of superior respondeat* where the corporation itself cannot do wrong, only the agents of the corporation can do wrong, that is, those who act for and on behalf of the corporation. One of the opinions expressed by Peter Gillies is that a corporation can be



held liable as a substitute for the acts done by its employees as long as the acts are carried out within the scope of their work.

The corporation has been determined as the subject of a criminal act, then criminal liability can be demanded against it. The occurrence of data leaks can be accounted for in accordance with article 48 of Law number 1 of 2023 concerning the Criminal Code because this activity is included in the scope of activities specified in the articles of association or other provisions that apply to hospitals, is accepted as hospital policy, and also the hospital does not take the necessary steps to prevent and prevent greater impacts and ensure compliance with applicable legal provisions.

The nature or model of criminal liability imposed on hospitals, in accordance with Law number 1 of 2023 concerning the Criminal Code, namely the hospital as the perpetrator of the crime and also as the responsible party, the prosecution can be carried out and the crime is imposed on the corporation itself. Meanwhile, if adjusted to the theory according to Kiesberg, the corporate decision-making model violates the law into the *Organization Process Model*, where the hospital as a corporation is seen as a loosely organized system of units and may not comply with the law.

The legal interests of patients who have been violated through the leak of Electronic Medical Record data, of course, require legal protection in the form of repressive legal protection, namely final protection in the form of sanctions, namely fines and additional punishments. Victim protection is also a direct victim protection, namely victim protection to obtain legal guarantees or compensation for the suffering or loss of people who have been victims of crime.

Majalaya Hospital can be used as a subject of a Criminal Act. The crime imposed on the Majalaya Hospital for the data leak that occurred, in accordance with Law number 1 of 2023 concerning the Criminal Code Article 118, article 119, and article 121, that is:

### ***Principal Crime***

Namely a fine in the form of a sum of money that must be paid based on a court decision, where the penalty of fines imposed is at least included in category IV, which is as much as Rp. 200,000,000,- (two hundred million rupiahs) and the most included in Category VIII, which is Rp. 50,000,000,000.00 (fifty billion rupiah). The penalty must be paid within a certain period of time as stated in the court decision and can be paid in installments. If the fine is not paid within the specified period of time, then the hospital's wealth or income can be confiscated and auctioned to pay off the unpaid fine. And if the hospital's wealth or income is insufficient to pay off the fine, then the hospital is subject to a penalty in the form of freezing part or all of the hospital's business activities. Meanwhile, the actions that can be imposed on hospitals are corporate takeovers, placement under supervision, and/or placement under supervision.

### ***Additional Criminal Charges***

Namely in the form of payment of compensation, correction due to criminal acts, implementation of obligations that have been neglected, revocation of certain permits, permanent prohibition of certain acts, closure of all or part of business premises and/or hospital

activities, freezing of all or part of hospital business activities, and even dissolution of hospitals. Additional penalties in the form of revocation of certain permits, closure of all or part of the hospital's business premises and/or activities, and freezing of all or part of the hospital's business activities, shall be imposed for a maximum of 2 (two) years. If the hospital does not carry out additional penalties in the form of compensation payments, reparations due to criminal acts, the implementation of obligations that have been neglected, the fulfillment of customary obligations and the financing of job training, then the hospital's wealth or income can be confiscated and auctioned to meet additional penalties that are not met.

In the prosecution of the case of leaking Electronic Medical Records data at Majalaya Hospital, there are several things that must be considered in accordance with article 56 in Law number 1 of 2023 concerning the Criminal Code, namely:

- 1) The level of loss or impact caused by the leak of Electronic Medical Record data. The impact caused has not been assessed because the data leak case at Majalaya Hospital was not published to the public, and there were no complaints coming to Majalaya Hospital from patients receiving treatment at Majalaya Hospital. Even so, it is possible that the impact did occur but was not reported to the Majalaya Hospital.
- 2) The level of involvement of administrators who have functional positions in the Hospital, as well as the involvement of officials who are assigned state duties and salaried based on the provisions of the law. In this case, the management and officials are considered negligent in maintaining the confidentiality of Electronic Medical Record data.
- 3) The provisions in the laws and regulations have not been fully implemented by Majalaya Hospital, and there is a lack of internal policies such as Standard Operating Procedures (SOP) that regulate in detail the access to Electronic Medical Records, especially those accessed from outside the hospital without a security system, and which regulates internal technical for users/*users* with the aim of securing data in the Electronic Medical Record, this results in the leakage of Electronic Medical Record data. The leakage of Electronic Medical Record data that occurred at Majalaya Hospital is a criminal act committed due to negligence from the management or officials at Majalaya Hospital in the development of SIMRS.

## CONCLUSION

Hospital policies in maintaining the confidentiality of Electronic Medical Record data in relation to patient legal protection have not been implemented in accordance with Law Number 17 of 2023, Regulation of the Minister of Health Number 24 of 2022, and Law Number 27 of 2022 concerning Personal Data Protection. Hospitals have also failed to implement the principles of *good corporate governance*. The Hospital Corporate Criminal Liability Model for Electronic Medical Record data leaks, as an effort to provide legal protection for patients, positions hospitals as both perpetrators of criminal acts and the responsible party; therefore, prosecution can be carried out and criminal sanctions can be imposed on the corporation itself.

## REFERENCES

Ardinata, M. (2020). *Tanggungjawab Negara Terhadap Jaminan Kesehatan Dalam Perspektif Hak Asasi Manusia*. Jurnal HAM.

- Ariana, I. D. G. A. W. I. G. P. (2016). *Perlindungan Hukum Terhadap Pelanggaran Privasi Konsumen dalam Bertransaksi Online*. Jurnal KertaSemaya.
- Dicky Rutanji Wing Wahyu Winarno, S. S. K. (2020). *ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan Untuk Diterapkan di Arsip Nasional)*. <https://journal.itny.ac.id/index.php/ReTII/article/view/604>.
- Geme, M. T. (2012). *Perlindungan Hukum terhadap Masyarakat Hukum Adat dalam Pengelolaan Cagar Alam Watu Ata Kabupaten Ngada, Provinsi Nusa Tenggara Timur*. Fakultas Hukum Universitas Brawijaya Malang.
- Hidayat, R. (2016). *Hak Atas Derajat Pelayanan Kesehatan Yang Optimal*. Syariah Jurnal Hukum dan Pemikiran.
- Hutauruk, R. M. (2013). *Penanggulangan Kejahatan Korporasi Melalui Pendekatan Restoratif*. Sinar Grafika.
- Indrayadi, H. A. A. (2023). *Perkembangan Rekam Medis Elektronik di Indonesia : Literature Review*. Jurnal Promotif Preventif.
- Judi. (2017). *Tata Kelola Dokumen Rekam Medis Sebagai Upaya Menjaga Rahasia Medis di Pelayanan Kesehatan*. Jurnal Manajemen Informasi Kesehatan Indonesia.
- Putra, C. A. (2022). *Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime*. Novum : Jurnal Hukum.
- Rizki, M. D. D. (2020). *Manfaat Penerapan Rekam Medis Elektronik Di Negara Berkembang : Literature Review*. Indonesian of Health Information Management Journal.
- Rusdiyanto. (2019). *Good Corporate Governance*. Refika Aditama.
- S, M. I. (2014). *Perlindungan Korban, Suatu Perspektif Viktimologi dan Kriminologi*. Prenadamedia group.
- Setiawan, A. L. K. A. (2021). *Perlindungan Data Rekam Medis Sebagai Bentuk Perlindungan Data Pribadi Pasien Selama Pandemi Covid-19*. Jurnal Hukum dan Pembangunan.
- Sunarso, S. (2012). *Viktimologi dalam Sistem Peradilan Pidana*. Sinar Grafika.
- Suryana. (2010). *Metodologi Penelitian Model Praktis Penelitian Kuantitatif dan Kualitatif*. Universitas Pendidikan Indonesia.
- Suryani, M. B. B. A. A. S. L. D. dan L. P. (2022). *Tanggung Jawab Rumah Sakit Terhadap Kerahasiaan Rekam Medis (Medic Record) di Masa Pandemi Covid-19*. Jurnal Analogi Hukum.
- Tamarell Vimy. Rudiyanto. Pujo Widodo. Panji Suwarno, S. Wiranto. (2022). *Ancaman Serangan Siber Pada Keamanan Nasional Indonesia*. Jurnal Kewarganegaraan.
- Yulita, S. N. D. (2023). *Analisis Faktor Dan Dampak Aspek Keamanan Rekam Medis Elektronik Pada Aplikasi SIMRS Di RSUD Mohammad Noer Pamekasan*. Sekolah Tinggi Ilmu Kesehatan (STIKES) Yayasan RS Dr. Soetomo Surabaya.