Legal Liability of Health Care Facilities for Leakage of Patient Electronic Medical Records

Adi Herisasono

adiherisasono@gmail.com

Universitas Sunan Giri Surabaya

Article Info

Received: 2024-03-02
Revised: 2024-06-21
Accepted:2025-03-01

Keywords:
Electronic Medical Record Breach, Legal Responsibility, Healthcare Services, Patient Privacy, Data Security

Abstract

Electronic medical record (EMR) data breaches have become an increasingly significant issue in healthcare, as the use of digital technology for patient data management rises. EMRs provide healthcare professionals with faster and more efficient access to patient information. However, this convenience also introduces the risk of data breaches, which could harm patients. This article aims to explore the legal responsibilities of healthcare facilities in managing EMR data breaches and the consequences resulting from such breaches. The research employs a qualitative approach and literature review, analyzing various legal regulations, legislation, and case studies of data breaches. The findings indicate that while legal protections exist, there are still significant challenges in implementing effective data security systems in healthcare facilities. Therefore, enhancing oversight, security systems, and legal awareness among stakeholders is essential to prevent data breaches that could cause significant harm to multiple parties.

1. Introduction

The development of information technology and digitalization has brought about a significant transformation across various sectors, including healthcare. In Indonesia, the use of Electronic Medical Records (EMR) has been expanding in recent years as part of efforts to improve the healthcare system. EMR replaces the traditional paper-based medical records that have long been used for documenting

and managing patient data. The adoption of this digital system allows healthcare facilities to access, manage, and share patient medical information more quickly, efficiently, and accurately, thereby speeding up the diagnostic and treatment processes.

Initially used only in large hospitals, EMRs are now being implemented in various healthcare facilities such as clinics, public health centers, and doctor's offices. One of the main benefits of the EMR system is the ease of accessing integrated medical information. For example, a patient moving between different doctors or hospitals can easily carry their medical data in an electronic format that can be accessed by the healthcare providers treating them. This not only reduces the likelihood of medical errors due to incomplete information but also accelerates administrative processes and treatment (Hasana, 2023).

However, despite the numerous benefits, the use of this electronic system also brings new challenges, particularly regarding the security and privacy of patient data. Medical data breaches, including the leakage of electronic medical records, have become a major risk as digital technology advances. These data breaches can occur due to various factors, ranging from human error and negligence in system management to external threats such as increasingly sophisticated cyberattacks. A breach of EMR not only jeopardizes patient privacy but can also result in significant financial, psychological, and reputational damage to the healthcare facility involved.

In response to this threat, the Indonesian government, through Law No. 17 of 2023 on Health and Law No. 27 of 2022 on Personal Data Protection (PDP), has established regulations mandating healthcare facilities to safeguard the confidentiality and security of patient data. Under these laws, healthcare providers are required to protect patient personal data and ensure that medical information does not fall into the wrong hands (Siti Ashira Salvina Day & Rahayu Subekti, 2024). This responsibility includes the obligation to implement stringent security measures for systems that store and manage EMRs, as well as to ensure that all staff involved

in data management are properly trained to maintain the confidentiality of patient information.

Despite the existing regulations to protect patient data, medical data breaches continue to occur. In recent years, several cases of medical data leaks have been reported, caused either by internal negligence or external cyberattacks. For instance, leaked patient data can be misused for fraudulent activities, other crimes, or even for commercial purposes that violate patient privacy rights. The impact of such breaches is wide-ranging, causing material losses to patients and their families, emotional distress, and a decline in trust in the healthcare system. Furthermore, medical data breaches can damage the reputation of the healthcare facility, potentially leading to legal actions that harm the institution both financially and reputationally.

Healthcare facilities, including hospitals, clinics, and other medical centers, bear a significant legal responsibility in protecting patient data. Therefore, it is crucial for each healthcare provider to not only comply with existing regulations but also proactively safeguard their systems from data breach risks. This responsibility involves not just technical aspects, such as using advanced security systems, but also organizational and internal policy factors that support the effective implementation of personal data protection (Indra et al., 2024).

Additionally, the regulations under the Personal Data Protection Law (PDP) require healthcare providers to take necessary steps in the event of a data breach. Patients also have the right to be notified clearly about any data breach and may seek compensation or further preventive measures. This underscores the importance of transparency and accountability for healthcare facilities that store and manage electronic medical records.

In light of this, this article aims to delve deeper into the legal responsibilities of healthcare facilities in managing breaches of electronic medical records. The article will discuss in detail the legal aspects governing the protection of medical data, the causes of medical data breaches, and the steps that can be taken to prevent

such breaches and improve existing systems. The research also aims to provide an overview of the impact of medical data breaches on patients and healthcare facilities, as well as the importance of collaboration among various stakeholders in maintaining a secure and trustworthy medical information system (Erwin Tumpal Ferdinand Tampubolon et al., 2024).

As the use of digital technology in healthcare continues to increase, it is vital for all parties involved in managing patient data to raise awareness about the importance of safeguarding medical privacy and security. Therefore, this research is expected to contribute to clarifying the legal responsibilities of healthcare facilities and offer solutions for reducing the risks of medical data breaches, which can harm both patients and healthcare institutions as a whole.

2. Research Method

This study adopts a qualitative approach using a literature review method to analyze the legal responsibilities of healthcare facilities regarding electronic medical record (EMR) breaches. A qualitative approach was chosen to gain a deeper understanding of the phenomena occurring within the healthcare sector, particularly concerning the security and protection of patient medical data. The literature review method was selected because this research does not involve direct primary data collection but focuses on analyzing existing sources, such as regulations, academic articles, journals, and relevant case study reports.

The data sources used in this study are divided into two main categories. The first category consists of primary sources, including regulations related to medical data protection, such as Law No. 17 of 2023 on Health, Law No. 27 of 2022 on Personal Data Protection, and guidelines published by other relevant government agencies. The second category consists of secondary sources, including journal articles, books, and reports discussing medical data protection and electronic medical record breaches. Several case studies of medical data breaches in healthcare facilities, both domestic and international, are also

analyzed to explore the causes of breaches and the steps taken to address them.

The data collection technique in this research employs a library research approach, where the researcher explores and gathers various relevant literature and legal documents. The researcher also uses case studies of medical data breaches in various healthcare facilities to analyze the causes of the breaches and their impact on patients and the facilities themselves. By examining these case studies, the researcher can better understand the roles and responsibilities of healthcare facilities in managing and protecting patient electronic medical records. Additionally, journal articles and other academic sources are used to provide a broader perspective on the issue of medical data breaches in the healthcare sector.

To analyze the collected data, this study uses a descriptive qualitative analysis technique. This analysis aims to describe the phenomenon of medical data breaches, identify key themes, and evaluate existing regulations and policies. The researcher will examine the legal aspects governing medical data protection and assess whether these regulations are sufficiently effective in reducing the risk of data breaches. The analysis also includes a discussion of the steps taken by healthcare facilities to prevent medical data breaches and how well their internal policies have been implemented.

Furthermore, case study analysis is used to explore the causes of medical data breaches at specific healthcare facilities. The researcher will investigate how the breaches occurred, whether due to internal errors or cyberattacks, and how healthcare facilities responded to these breaches. This process aims to identify potential gaps in the data protection systems applied by healthcare facilities and provide recommendations for preventive measures to enhance patient medical data security.

To ensure the quality and validity of the research, only credible sources are used, including legally recognized and valid legal sources, as well as academic literature that has undergone a peer-review process. By adopting this approach,

the research aims to make a significant contribution to the development of policies and practices for medical data protection in healthcare facilities and clarify the legal responsibilities of healthcare facilities in maintaining the confidentiality and integrity of patient electronic medical records.

3. Results and Discussion

Concept of Electronic Medical Records (EMR) in the Healthcare System

Electronic Medical Records (EMR) are a digital system that replaces traditional manual recording in managing patient medical data. EMR allows medical information such as health history, laboratory test results, medical diagnoses, and treatments received by patients to be stored electronically and easily accessed by authorized healthcare professionals. In this system, all patient-related information can be accessed by doctors, nurses, or other healthcare staff via computers or mobile devices, facilitating coordination between various healthcare facilities (SUMITRA et al., 2023).

One of the main goals of implementing EMR is to improve the quality of healthcare services by speeding up the flow of information and medical decision-making. When medical data can be accessed in real-time by healthcare professionals, the process of diagnosis and treatment becomes quicker and more accurate. For instance, if a patient is referred to another hospital or visits multiple doctors, their entire medical history can be easily accessed by the new healthcare provider (Lalu Anugrah Nugraha et al., 2023). This reduces the likelihood of diagnostic or treatment errors caused by incomplete or delayed information.

Moreover, EMR also facilitates integration between various healthcare facilities, such as hospitals, clinics, and other health centers. This integration enables smoother data flow between institutions, eliminating the need for patients to carry physical documents, which are sometimes lost or damaged. Additionally, data stored in the EMR system can be analyzed more deeply to support medical research and enhance public health policies. For example, patient data can be used

to map health trends in a region, monitor disease outbreaks, and design more effective prevention programs.

However, despite its various benefits in enhancing healthcare efficiency, the use of EMR also presents significant challenges, particularly regarding the security and privacy of patient medical data. EMR stores highly sensitive information, which, if not properly protected, can lead to data breaches. Leaked medical data could be misused for various purposes, ranging from criminal activities and fraud to the exploitation of data for commercial gain without the patient's consent (Sultan et al., 2025).

Additionally, EMR systems that lack adequate security measures can become easy targets for cyberattacks. Cases of medical data breaches due to hacking or data theft by malicious actors are increasingly common in many countries, including Indonesia. Leaked data could include personal information such as names, addresses, phone numbers, and crucial medical history. The impact of such breaches not only harms patients but can also diminish public trust in the healthcare system and damage the reputation of the involved medical facilities.

One of the greatest advantages of EMR is its ability to reduce human error in medical record-keeping. Previously, handwritten notes or physical forms, which were prone to human errors, are now minimized with the more accurate and systematic EMR system. Using EMR reduces the risk of data entry errors or misinterpretations of medical information. For instance, in the case of medication administration, the EMR system can issue alerts if there is a dangerous drug interaction or incorrect dosage, thus ensuring patient safety.

However, despite the many benefits offered by the EMR system, implementing this technology still faces major challenges concerning data protection. Without adequate security measures, the medical data stored in EMR systems is highly vulnerable to breaches. Patient data breaches can occur due to various factors, both internal, such as staff negligence, and external, such as cyberattacks. Even if the system is equipped with high-level security, data breaches

can still happen if access management and staff training are not handled properly. Therefore, it is crucial for healthcare facilities to ensure that the EMR systems they implement are equipped with stringent security measures, including data encryption, proper access control, and regular staff training on the importance of safeguarding patient medical data confidentiality.

Overall, although EMR has the potential to improve healthcare quality, the significant challenges related to privacy and medical data security must remain a top priority. As threats to medical data security become more complex, healthcare facilities must continually adapt to technological developments and strengthen their internal policies to protect patient data from potential breaches. Medical data security and privacy are not only technical responsibilities but also require legal and ethical awareness in managing such sensitive medical data.

Legal Regulations on Patient Data Protection

In Indonesia, the protection of patient medical data has become a crucial issue regulated by various legal provisions that require healthcare facilities to safeguard the security and confidentiality of patient medical information. One of the primary laws addressing this matter is Law No. 17 of 2023 on Health, This Law regulates health by setting limits on the terms used in its regulation. This Law contains general provisions, rights and obligations, responsibilities of the central government and regional governments, health administration, health efforts, health service facilities, health human resources, health supplies, pharmaceutical and medical device security, health technology, health information systems, extraordinary events and outbreaks, health funding, coordination and synchronization of health system strengthening, community participation, guidance and supervision, investigation, criminal provisions, transitional provisions and closing provisions (Elektronik & Bukti, n.d.).

Furthermore, the Health Law also stipulates the obligation of healthcare facilities to implement adequate protection for patient medical records. This includes the responsibility to establish secure systems for storing and managing

medical data, ensuring that access to this data is only granted to authorized individuals, such as healthcare professionals directly involved in patient care. In cases where a data breach occurs due to negligence or error by the responsible party, healthcare facilities can be held accountable in accordance with applicable regulations.

However, while Law No. 17 of 2023 regulates the protection of medical data, the rapid advancement of information technology, particularly in the use of Electronic Medical Records (EMR), requires more detailed and comprehensive regulations regarding personal data protection. To address this, Indonesia enacted Law No. 27 of 2022 on Personal Data Protection (PDP), which provides a more robust legal framework for safeguarding individual rights concerning personal data, including patient medical data. This law was designed to meet the challenges that arise from the digitalization of personal data, including electronic medical records (Sri Murcittowati et al., 2023). One of the primary goals of this law is to offer enhanced protection for individuals' personal data and establish stricter rules on how personal data should be managed, stored, and protected by those who access or process it.

The PDP Law specifies in detail the rights of individuals, such as the right to access, modify, delete, and suspend the processing of their personal data, including medical data. The law also emphasizes that any entity managing personal data, including healthcare facilities, must implement adequate policies to protect this data from breaches or misuse. Healthcare facilities processing patient medical data are required to have robust security systems to protect electronic medical records from unauthorized access, hacking, or breaches caused by internal negligence.

Additionally, Law No. 27 of 2022 imposes severe penalties for violations related to the protection of personal data, including medical data. If a data breach occurs due to negligence or mismanagement of data by a healthcare facility, the institution may face significant administrative fines. Furthermore, legal actions

may be taken, including criminal sanctions, if there is evidence of intentional misconduct or negligence that harms individuals. These penalties are intended to serve as a deterrent and ensure that healthcare facilities take greater care in handling and securing patient medical data. These sanctions are expected to encourage healthcare institutions to improve their data security systems, implement better data management practices, and conduct ongoing training for staff regarding the protection of personal data and the importance of maintaining patient confidentiality (Melyanti et al., 2023).

It is important to note that the PDP Law also requires healthcare facilities to establish clear procedures for collecting, storing, and processing personal data, including medical data. One of the obligations outlined in this law is that healthcare providers must regularly audit or inspect their data security systems to ensure that personal data under their management remains secure and protected. Proper management of medical data in compliance with these regulations will not only mitigate the risk of data breaches but also build patient trust in the healthcare systems they use.

Moreover, in cases of medical data breaches, the PDP Law provides patients with the right to seek compensation if their personal data is leaked or misused. Patients who feel their medical data has been compromised can report the incident to the relevant authorities and claim their legal rights under applicable laws. In such cases, mediation or dispute resolution mechanisms can be employed to ensure that victims of data breaches receive fair compensation.

Overall, Law No. 17 of 2023 on Health and Law No. 27 of 2022 on Personal Data Protection provide a solid legal foundation for protecting patient medical data in Indonesia. These two laws complement each other, with the Health Law outlining healthcare facilities' obligations to maintain the confidentiality of medical data, while the PDP Law offers more detailed protection regarding individuals' rights in managing and safeguarding their personal data. With clear regulations and strict penalties in place, it is hoped that healthcare facilities will be more

proactive in securing patient medical data and reducing the risk of data breaches that can harm both patients and healthcare institutions.

Factors Contributing to Electronic Medical Record (EMR) Leaks

The leakage of electronic medical records (EMRs) is a serious issue in the healthcare system, particularly in today's digital age. The factors causing patient medical data leaks can be divided into two main categories: internal and external factors. Both of these categories play a significant role in influencing the security of medical data stored electronically and require serious attention from all parties involved in data management, both at healthcare facilities and the regulatory level (Meilia et al., 2019).

1. Internal Factors Causing Medical Data Leaks

   Internal factors that contribute to the leakage of medical data often stem from weaknesses in the information systems management used by healthcare facilities. One primary cause is the inability of healthcare facilities to properly manage and secure the information systems used to store patient data. Poor data management may include a lack of planning in selecting and implementing the appropriate technology to secure data. For example, healthcare facilities may use outdated software or systems without adequate security updates. The use of software or systems that are vulnerable to cyberattacks or lack security features such as encryption or protection against unauthorized access is a major contributor to data leaks.

   Additionally, negligence in using security measures like data encryption, password management, and access restrictions also contributes to medical data leaks. In many cases, healthcare facilities fail to implement strong encryption to protect stored medical data. Without proper encryption, sensitive patient data, such as medical histories, test results, and personal information, can be easily accessed by unauthorized individuals if a data

breach occurs. Weak or easily guessable passwords can also allow unauthorized access to information systems with minimal barriers. Furthermore, the enforcement of access control policies for healthcare professionals and staff is often lax. Loose access restrictions allow anyone within the facility to access patient data that should only be available to authorized personnel.

A lack of staff training is another contributing factor to data leaks. Medical and administrative staff at healthcare facilities may not fully understand the importance of maintaining the confidentiality and security of patient data. Insufficient awareness of the regulations related to personal data protection and how to safeguard patient data can lead to careless or unintentional actions that result in data breaches. For example, staff might accidentally leave devices containing patient medical data unsecured or fail to lock access to medical information systems when leaving their workspace. Simple mistakes such as sending medical data via unencrypted email or sharing passwords without caution can also lead to data leaks.

2. External Factors Causing Medical Data Leaks

In addition to internal factors, external factors also play a major role in medical data breaches. One of the greatest threats is cyberattacks by external parties with malicious intent to illegally obtain patient data. Although many healthcare facilities have implemented multiple layers of security to protect data, increasingly sophisticated cyberattacks continue to threaten the integrity of these security systems. Examples include phishing, ransomware, and malware attacks aimed at hacking into and exposing patient medical data, which have become more frequent in the healthcare sector.

Hacking is one of the most common threats encountered. In this attack, unauthorized individuals can gain access to medical information systems through vulnerabilities or weaknesses. For instance, if a healthcare facility

does not regularly update its software, it becomes an easy target for hackers exploiting known system flaws. Using advanced techniques, such as advanced persistent threats (APT), hackers can infiltrate systems over long periods without detection and steal large amounts of medical data.

Besides direct attacks on the system, unauthorized access can also come from third parties attempting to infiltrate healthcare facility systems. This could involve hacking into networks connecting hospitals or healthcare facilities with other entities, such as insurance companies or pharmacies. If there is inadequate protection for the network systems that link these parties, sensitive medical data can easily fall into the wrong hands. Therefore, securing external access with strong firewalls, virtual private networks (VPNs), and regular checks for potential network vulnerabilities is crucial.

In addition to cyberattacks, negligence by third parties with access to patient medical data can also be an external factor contributing to data leaks. For example, in some cases, patient data stored in the cloud or managed by third-party technology providers can be exposed due to inadequate security measures. If healthcare facilities rely on third-party providers to store medical data, they must ensure that these providers meet strict security standards. Without proper control over relationships with third-party service providers, data stored outside healthcare facilities can become highly vulnerable to breaches.

3. Prevention and Mitigation Efforts

To reduce the risk of medical data breaches, both internal and external factors must be given serious attention. Internally, healthcare facilities should ensure they implement up-to-date data security systems and provide ongoing staff training on the importance of maintaining the confidentiality of medical data. All medical and administrative personnel must be clearly

informed about personal data protection policies and the technologies used to store medical data.

Externally, healthcare facilities must ensure their systems are equipped with strong security measures, such as encryption, robust firewalls, and cybersecurity detection and prevention systems that can quickly identify suspicious activities. Furthermore, it is essential for healthcare facilities to establish close cooperation with technology service providers and ensure that they meet the same security standards. Implementing regular audits and monitoring of information systems can also help ensure systems remain protected against emerging threats.

In conclusion, the leakage of electronic medical data is caused by various factors, both from internal system weaknesses and external threats. A comprehensive mitigation effort, which includes enhancing internal security, providing adequate staff training, and protecting against external threats, is necessary to prevent medical data breaches that could harm both patients and healthcare facilities.

Legal Responsibility of Healthcare Facilities

Healthcare facilities bear significant legal responsibility in maintaining and protecting the confidentiality and security of patient medical data. As institutions that handle sensitive health-related information, healthcare facilities are required to comply with various legal regulations governing the protection of personal data. In Indonesia, the protection of patient medical data is regulated by Law No. 17 of 2023 on Health and Law No. 27 of 2022 on Personal Data Protection (PDP), which provides a clear legal foundation regarding the obligations of healthcare facilities to protect the confidentiality and integrity of patient medical data.

Under Law No. 17 of 2023 on Health, This Law regulates health by setting limits on the terms used in its regulation. This Law contains general provisions, rights and obligations, responsibilities of the central government and regional governments, health administration, health efforts, health service facilities, health

human resources, health supplies, pharmaceutical and medical device security, health technology, health information systems, extraordinary events and outbreaks, health funding, coordination and synchronization of health system strengthening, community participation, guidance and supervision, investigation, criminal provisions, transitional provisions and closing provisions.

Meanwhile, Law No. 27 of 2022 on Personal Data Protection outlines more detailed requirements regarding healthcare facilities' obligations in managing patient personal data, including medical data. This law stipulates that any entity collecting and managing personal data, such as hospitals or clinics, must implement strict data security measures to protect the data from leakage, misuse, or theft. Healthcare facilities are required to provide adequate protective mechanisms, such as data encryption, strict access control, and staff training on how to safeguard data confidentiality.

When a data breach occurs, the legal responsibility of healthcare facilities becomes clearer. Based on the provisions of both laws, healthcare facilities may face a variety of legal penalties, including fines, administrative sanctions, or even criminal charges if the breach occurs due to negligence or serious errors. According to (Saliman & Zulkifli, 2023)the sanctions imposed depend on the severity of the violation. For example, if the data breach is caused by internal errors, such as insufficient staff training or neglecting data security procedures, the healthcare facility may face administrative fines. Criminal sanctions, which are more severe, may be applied if it is proven that the breach resulted from intentional misconduct or malicious use of patient data, such as selling patient data to third parties.

In addition to legal penalties, healthcare facilities are also obligated to address data breaches in a transparent and responsible manner. One of the key requirements in Law No. 27 of 2022 on Personal Data Protection is that healthcare facilities must promptly report data breaches to the relevant authorities and notify the affected patients. This report must be made as soon as possible, providing details on the type of data that was exposed, the potential impacts, and the steps

taken to prevent further breaches (Saputra, 2024).

Notifying patients whose data has been compromised is a crucial step to help them take preventive actions. For instance, patients whose data has been breached may be provided with information on how to avoid identity theft, such as changing identification numbers, monitoring financial statements, or blocking financial accounts that may be affected. Additionally, patients should be informed about the legal actions they can take to protect themselves from potential harm caused by the data breach. By providing timely notifications and clear information, healthcare facilities can assist patients in taking necessary measures to minimize the impact of the breach.

Healthcare facilities must also ensure they have a documented and clear mitigation procedure for managing data breaches. This includes preventive measures that can be taken before a breach occurs, such as enhancing security systems, conducting regular audits, and providing continuous staff training on the importance of data confidentiality. Furthermore, healthcare facilities should have an emergency plan in place to address data breaches, which includes immediate action to handle the breach, investigating the cause, and improving systems to prevent similar incidents in the future (Puteri et al., 2024).

Ultimately, the legal responsibility of healthcare facilities regarding medical data breaches is to ensure the security of patient data by implementing strict security standards. This also includes the obligation to report any data breaches with full transparency, protecting affected patients, and being held accountable for the legal consequences resulting from the breach. Therefore, healthcare facilities are not only responsible for the medical services they provide but also have an obligation to protect the confidentiality and security of patient medical data as part of their professional and ethical responsibilities.

The Impact of Electronic Medical Record (EMR) Breaches on Patients

The breach of Electronic Medical Records (EMR) has significant and far-reaching consequences for patients, affecting both personal data security and trust

in the healthcare system. Exposed or leaked medical data can lead to a series of serious problems that not only harm patients but also impact the healthcare facilities responsible for managing the data. These effects are not only immediate and concrete but can also have long-term consequences that adversely affect all parties involved (Prisusanti & Afifah, 2022).

1. Misuse of Medical Data for Criminal Activities

   One of the most direct and obvious impacts of a data breach is the misuse of information that can financially and legally harm patients. Leaked medical data can be accessed by unauthorized individuals, who can then use it for fraudulent or identity theft purposes. In some cases, medical details such as patient ID numbers, addresses, phone numbers, medical histories, and even financial information can be exploited by criminals to file fraudulent insurance claims. This misuse of insurance claims can cause financial losses for patients if false claims are paid out, or may even result in legal actions against them.

   Moreover, leaked medical data can also be used in other crimes, such as document forgery or online fraud. For example, medical identity theft could be used to create fake identities for illegal activities. Such crimes not only pose a financial risk to patients but also have the potential to tarnish their personal reputation. Patients who fall victim to identity theft or medical data misuse may find it difficult to prove that they were not involved in criminal actions committed by those using their stolen identity.

2. Psychological Impact on Patients

   Beyond the financial and legal effects, a breach of medical data can cause significant psychological harm to patients. When highly personal medical information such as records of serious illnesses, mental health conditions, or other sensitive medical details becomes publicly accessible without permission, patients may feel deeply violated. In some cases, feelings of shame and anxiety can arise, particularly if the exposed data relates to

sensitive or embarrassing conditions like contagious diseases or psychological disorders. Patients who feel their private health information has been exposed may experience emotional stress, insecurity, or a sense of being threatened.

A data breach can also undermine trust in the healthcare system as a whole. Patients may begin to doubt the ability of healthcare facilities to safeguard their private information, which could make them feel uncomfortable seeking further care. As a result, affected patients may become reluctant to continue their treatment or may even avoid the healthcare facility involved, which could worsen their health conditions.

3. Impact on Trust in Healthcare Facilities

One of the most damaging long-term effects of a data breach is the loss of public trust in the healthcare facilities involved. Healthcare providers, including hospitals, clinics, and other medical institutions, carry a significant responsibility to protect the confidentiality of patient data. When a breach occurs, the reputation and credibility of these facilities can be permanently damaged. Patients who had previously trusted these institutions with their medical data may feel disappointed and insecure about using their healthcare services.

This loss of trust not only harms patients but also negatively impacts the operations of the healthcare facility itself. Many patients may hesitate to provide their medical information in the future or may seek care from other facilities that they perceive as safer. The decision to find an alternative healthcare provider could lead to a decline in patient visits, which in turn can affect the facility's revenue and operational stability.

In the long run, the loss of public trust could further damage the facility's image in the community and the media. News about data breaches often spreads quickly through social media and mainstream outlets, exacerbating the reputational impact. In an increasingly digital world, transparency and

data security are critical factors in maintaining patient trust. Therefore, healthcare facilities must prioritize data protection and develop clear policies for managing breaches to minimize these negative effects.

4. Economic Impact for Patients and Healthcare Facilities

   In addition to psychological and reputational consequences, medical data breaches can result in significant economic impacts for both patients and healthcare facilities. For patients, one immediate financial consequence is the cost of identity recovery, which may involve services like credit monitoring or identity theft protection. Patients whose identities have been stolen or misused may incur additional expenses to address the issues arising from the breach.

   For healthcare facilities, the financial burden can include legal fines for violating personal data protection regulations. A medical data breach may also lead to additional legal costs, such as lawsuits from patients who feel harmed by the incident or the expense of restoring public image. Additionally, healthcare facilities may need to allocate extra resources to improve their security systems to prevent similar breaches in the future, which comes with significant financial implications.

5. Prevention and Mitigation Measures

   To mitigate these impacts, healthcare facilities must take proactive measures to enhance data security. This includes employing the latest technology, such as robust encryption, dual authentication systems, and regular training for staff on personal data protection. Furthermore, healthcare facilities should have clear emergency procedures in place for managing data breaches, including quickly notifying affected patients and collaborating with relevant authorities to resolve the issue efficiently.

In conclusion, the impact of medical data breaches is extensive and can significantly affect various aspects of patients' lives, from psychological and financial consequences to public reputation. Therefore, it is crucial for healthcare

facilities to ensure maximum data protection to prevent such damaging effects from occurring.

Efforts to Address Data Breaches and Enhance EMR Security

The breach of medical data involving Electronic Medical Records (EMR) is a serious issue that requires prompt attention and action from healthcare facilities. To minimize the risk of medical data breaches and strengthen data protection systems, various countermeasures must be implemented effectively. Healthcare facilities must adopt comprehensive, ongoing measures to enhance information technology security and ensure staff awareness and competence in safeguarding medical data (Fitriyah, 2022).

1. Strengthening Information Technology Security Systems

   One of the most crucial steps in preventing data breaches is strengthening the information technology security systems used by healthcare facilities. The security of information systems depends on the implementation of advanced technologies that can ensure patient data remains secure from both internal and external threats. One key technique that must be applied is data encryption. This ensures that patient data remains secure during transmission and storage, making it unreadable or unusable to unauthorized parties.

   Additionally, multi-factor authentication (MFA) should be implemented to ensure that only authorized individuals can access medical data. MFA requires two or more identity verifications before access is granted, such as a combination of a password and a verification code sent via SMS or a specialized app. The use of MFA significantly reduces the risk of unauthorized access from both within the organization and from external sources.

   Monitoring system access is another vital part of a data protection strategy. Healthcare facilities must track and control who can access EMR and which parts of the data they are permitted to view. For example, a doctor handling a specific patient may only need access to the medical data relevant to that patient's condition, while administrative staff may only require limited access to payment

or treatment schedule information. Role-Based Access Control (RBAC) is an effective method to ensure that only authorized personnel can access the data that is pertinent to them.

2. Regular Security Audits and Simulations

   Preventive efforts to reduce data breaches must include regular audits of the information systems in use. These audits are designed to assess the strength of existing security systems and identify potential vulnerabilities that could be exploited by unauthorized individuals. The audit process includes reviewing the hardware and software used to manage EMRs, as well as testing existing security protocols and policies.

   In addition to audits, healthcare facilities should conduct simulated cyberattacks or penetration testing to test their information systems' resilience against external threats. These simulations replicate the types of attacks commonly performed by hackers to determine how effective the current security systems are in dealing with potential threats. Regular testing and evaluation of systems help identify gaps that may not be evident during routine monitoring and provide insight into the system's robustness in the face of cyber threats.

3. Staff Training and Awareness

   Training and raising awareness about managing sensitive medical data must be a top priority. All healthcare workers and staff involved in managing patient data should receive regular training on security protocols that must be followed. This training covers various aspects, from how to access medical data securely to how to handle patient information responsibly. Training should also emphasize professional ethics and the legal responsibility to protect patient privacy.

   Not only medical personnel but also administrative staff and IT technicians involved in managing the EMR system must receive ongoing education about potential security threats and the latest techniques in data protection. This education can take place internally through workshops, seminars, and online learning sessions tailored to the specific needs of the healthcare facility.

4. Collaboration with Competent Third Parties

   Healthcare facilities should also collaborate with third-party experts in cybersecurity to ensure that the systems they use are constantly updated and protected from external threats. Many healthcare facilities, particularly small and medium-sized ones, may lack the internal resources or expertise to manage the increasingly complex cyber threats. Therefore, partnerships with companies specializing in cybersecurity can be a strategic move to enhance the protection of medical data.

   Cybersecurity companies can help healthcare facilities assess their vulnerabilities and offer appropriate technological solutions to strengthen their defenses. These companies can provide the latest security software, advise on improving security procedures, and ensure that data protection policies comply with industry standards and applicable regulations. By involving external experts, healthcare facilities can ensure their systems are protected from potential threats that may not be detected by internal teams.

5. Development of Clear Security Policies and Procedures

   Healthcare facilities must develop well-documented, clear security policies and procedures. These policies should include guidelines for managing medical data, access controls, system maintenance, and actions to take in the event of a data breach. Additionally, clear emergency response procedures must be prepared to handle data breaches quickly and efficiently. These policies should be regularly updated to keep up with technological advancements and regulatory changes, such as those outlined in the Personal Data Protection Act (PDP) and relevant healthcare regulations.

6. Raising Patient Awareness about Data Security

   In addition to the internal measures taken by healthcare facilities, it is also important to raise patient awareness about the importance of protecting their data privacy. Healthcare facilities can provide clear information to patients about how their medical data is managed, the measures taken to protect it, and what steps

patients should take if they suspect their data has been exposed. This transparency will build patient trust and educate them on the importance of monitoring the use of their medical data.

4. Conclusion

The breach of Electronic Medical Records (EMR) is a serious issue that can have widespread consequences for patient privacy and reduce trust in healthcare facilities. Leaked medical data is at risk of being misused by unauthorized individuals, either for fraudulent purposes or other criminal activities. The psychological impact is also significant, as patients may feel their privacy rights have been violated. Therefore, maintaining the confidentiality and integrity of patient medical data must be a top priority for every healthcare facility.

Healthcare providers have clear legal responsibilities under the Health Law and the Personal Data Protection Law, which mandate them to protect patient medical data. In the event of a data breach, healthcare facilities may face penalties, including fines or even criminal sanctions, depending on the severity of the violation. Therefore, healthcare facilities must proactively design policies and procedures that govern the management and protection of patient data in a strict and responsible manner.

However, despite existing regulations protecting personal data, challenges in implementing and managing secure information systems remain high. Weaknesses in system management, insufficient staff training, and increasingly sophisticated cyber threats are risk factors that need to be carefully managed. Therefore, strengthening information security systems, tightening monitoring, and providing continuous training for medical personnel and administrative staff are crucial steps to minimize the risk of medical data breaches and ensure better protection of patient data.

Refrences

Elektronik, R. M., & Bukti, A. (n.d.). *ALAT BUKTI DALAM SUATU SENGKETA MEDIS Sekolah Tinggi Hukum Militer , Jakarta ,*

Erwin Tumpal Ferdinand Tampubolon, Andika Persada Putera, & M. Khoirul Huda. (2024). Pertanggungjawaban Hukum Rumah Sakit Terkait Kebocoran Data Pribadi Pasien Berdasarkan Peraturan Perundang-Undangan. *Syntax Idea*, *6*(3), 1388–1402. https://doi.org/10.46799/syntax-idea.v6i3.3121

Fitriyah, Y. (2022). Analisis Tingkat Kesiapan implmentasi Tanda Tangan Digital Untuk Autentikasi Dokumen Rekam Medis ELektronik di Instalasi Rawat Jalan RSUD Kota Yogyakarta. *Journal of Information Systems for Public Health*, *7*(2), 53. https://doi.org/10.22146/jisph.73666

Hasana, N. (2023). Terhadap Keselamatan Pasien Pada Rekam Medik Elektronik Berbasis Nilai Keadilan. *Seminar Nasional*, 361–386. https://conference.untag-sby.ac.id/index.php/shnbc/article/view/3662

Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan Kerahasiaan Data Pasien vs Kewajiban Membuka Akses Rekam Medis Elektronik. *Soepra*, *10*(1), 97–117. https://doi.org/10.24167/sjhk.v10i1.11542

Lalu Anugrah Nugraha, Sutarno, S., Nugraheni, N., & Putra, A. P. (2023). Perlindungan Hukum Rumah Sakit Atas Penggunaan Data Pasien Dalam Peresepan Elektronik. *Unizar Law Review*, *6*(2). https://doi.org/10.36679/ulr.v6i2.45

Meilia, P. D. I., Christianto, G. M., & Librianty, N. (2019). Buah Simalakama Rekam Medis Elektronik: Manfaat Versus Dilema Etik. *Jurnal Etika Kedokteran Indonesia*, *3*(2), 61. https://doi.org/10.26880/jeki.v3i2.37

Melyanti, H., Lindawaty Suherman Sewu, P., & Author, C. (2023). Perlindungan Data Pribadi Dalam Pengaturan Rekam Medis Elektronik Berdasarkan Perundang-Undangan Indonesia Dihubungkan Dengan Asas-Asas Hukum. *JIM: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah*, *8*(3), 1415–1422.

Prisusanti, R. D., & Afifah, L. (2022). *Tinjauan Yuridis : Tantangan Kerahasiaan Rekam Medis*

Elektronik Berdasarkan pada Permenkes Nomor 24 Tahun 2022 Juridical Review : Challenges for Confidentiality of Electronic Medical Records Based on Minister of. *24*, 258–266.

Puteri, D., Pramesti, A., Ayuningtyas, D., & Verdi, R. (2024). *KEAMANAN DAN KERAHASIAAN DATA MEDIS PASIEN DALAM IMPLEMENTASI REKAM MEDIS ELEKTRONIK : 8*, 7691–7702.

Saliman, A. R., & Zulkifli, M. A. (2023). *Tinjauan Yuridis tentang Tanggung Jawab Hukum Klinik FRAYA Dental dalam Pengelolaan Jaminan Kerahasiaan Data Pribadi Pasien*. *01*(02), 1–13. https://doi.org/10.58819/jurnallegalitas(jle).v1i2

Saputra, T. E. (2024). *Penggunaan Rekam Medis Elektronik Dalam Mewujudkan Perlindungan Hukum Keamanan Data Pribadi Pasien The Use of Electronic Medical Records in Realizing Legal Protection of Patient Personal Data Security*. *13*, 57–75.

Siti Ashira Salvina Day, & Rahayu Subekti. (2024). Pertanggungjawaban Penyedia Sistem Rekam Medis Elektronik Dari Partner System Terhadap Kebocoran Data. *Demokrasi: Jurnal Riset Ilmu Hukum, Sosial Dan Politik*, *1*(3), 92–101. https://doi.org/10.62383/demokrasi.v1i3.253

Sri Murcittowati, P. A., Wirajaya, M. K. M., Astuti, I. W., Kartika, I. G. A., & Farmani, P. I. (2023). Pengaturan Pengaktifan Kembali Rekam Medis Elektronik pada Rumah Sakit X Kota Denpasar. *Jurnal Kesehatan Vokasional*, *8*(4), 244. https://doi.org/10.22146/jkesvo.89228

Sultan, M., Boling, H., & Asyhadie, Z. (2025). *DATA PASIEN DALAM PRAKTEK KESEHATAN MENURUT HUKUM POSITIF INDONESIA Legal Analysis of Patient Data Confidentiality Protection in Health Practices under Indonesian Positive Law*. *1*(1).

SUMITRA, S., Yuyut Prayuti, Y. P., & Arman Lany, A. L. (2023). Kewajiban Dan Tanggung Jawab Hukum Perdata Dalam Perlindungan Privasi Data Pasien Dalam Layanan Kesehatan Digital. *Jurnal Hukum Media Justitia Nusantara*, *14*(1), 43–52. https://doi.org/10.30999/mjn.v14i1.2968