

Juridical Analysis of Cyber Crime Offenses in Hacking Hospital Management Information Systems (SIMRS)

Redyanto Sidi*
redysidi@gmail.com

Graduate Program, Panca Budi Development University, Medan, Indonesia

Article Info

Received:2023-3-14

Revised:2023-11-24

Accepted:2024-03-20

Keywords:

Criminal Acts; Cyber Crime; Hacking; Hospital Management Information System.

Abstract

In the current digital era, the increasing reliance on information technology in the healthcare sector, especially through the use of Hospital Management Information Systems (SIMRS) as an effort for administrative orderliness and also to avoid medical disputes in health services, brings significant risks related to cybercrime. SIMRS, which integrates the management of sensitive health data such as medical records and financial information, has become a primary target for cybercriminals. Cybercrime, particularly hacking, is a real threat that not only disrupts hospital operations but also damages public trust in the healthcare system and threatens the loss or misuse of data. This study aims to identify the legal vulnerabilities in SIMRS in Indonesia, analyze the legal implications of cybercrime hacking, and evaluate the effectiveness of existing regulations against hacking as an evaluation and protection for the present and the future. The research method used is doctrinal, focusing on the normative analysis of relevant regulations and legal documents, including the Indonesian Law No. 11 of 2008 as amended by Indonesian Law No. 19 of 2016 on Information and Electronic Transactions, and the Minister of Health Regulation of the Republic of Indonesia No. 82 of 2013 on Hospital Management Information Systems. This approach involves data collection through literature studies and analysis of existing regulations to identify gaps and the need for legal reforms. The results of the research show that although the ITE Law provides a strong legal foundation, there is still a need for revision and adaptation to accommodate technological developments

and the ever-changing hacking practices. Based on these findings, the recommendations proposed include revising the ITE Law to include more specific aspects of health data security, adopting international cybersecurity standards, enhancing human resource capacity, and fostering closer cooperation between sectors in developing cybersecurity solutions. The implementation of these recommendations is expected to strengthen data security in SIMRS and improve the resilience of the health sector against cyber threats. Thus, the integrity and privacy of patient data can be maintained, ensuring smooth hospital operations.

1. Introduction

In the current digital era, technological advancements have enabled the extensive integration of information systems across various sectors, including the healthcare sector. The Hospital Management Information System (hereinafter referred to as SIMRS) is one crucial technology implementation designed to optimize the quality of healthcare services through efficient and effective data management. SIMRS encompasses various aspects, from managing patient medical records to hospital resource management, all of which rely on the integrity and security of processed data. The existence of SIMRS also ensures administrative orderliness to avoid medical disputes. In practice, various types of medical disputes can occur simultaneously and interrelatedly. For instance, a medical malpractice case may also involve the violation of patient rights. Or, a medical billing dispute might involve ethical and legal issues, such as billing for unnecessary or non-performed procedures.¹

Article 3 of the Minister of Health Regulation of the Republic of Indonesia No. 82 of 2013 on Hospital Management Information Systems (Permenkes SIMRS) states that every hospital is required to implement SIMRS, which can use open-source applications provided by the Ministry of Health or applications developed by the hospitals themselves, as long as these applications meet the minimum requirements set by the Minister of Health.²

Based on the Permenkes SIMRS, SIMRS is a communication information technology system that processes and integrates all hospital service workflow processes in the form of a coordination network, reporting, and administrative

¹ Sienny Rusli, 'Implementasi Sistem Informasi Manajemen Rumah Sakit Dalam Pengolahan Data Rumah Sakit', *JKM (Jurnal Kesehatan Masyarakat) Cendekia Utama*, 10.2 (2022), 158 <<https://doi.org/10.31596/jkm.v10i2.1036>>.

² Pricillia T. Tangel, Aaltje E. Manampiring, and Nova H. Kapantow, 'Penerapan Sistem Informasi Manajemen Rumah Sakit Di RSUD Dr. Sam Ratulangi Tondano', *E-Clinic*, 12.2 (2023), 121–33 <<https://doi.org/10.35790/eci.v12i2.52755>>.

procedures to obtain accurate and precise information, and is part of the Health Information System. SIMRS is also an integrated information system prepared to handle the entire hospital management process, from diagnosis and treatment services for patients, medical records, pharmacies, and pharmaceutical warehouses, to the hospital's computerization systems including hardware and software. This includes the hospital's computer/internet network system, website, billing system for patient services, and computer/printer repairs.³

However, the existence of this system also brings significant risks, particularly related to cybercrime. Hacking, or the activity involving illegal penetration into systems with the intent to alter, steal, or destroy data, poses a real threat to SIMRS. Hacking not only threatens the privacy and security of patient data but also has the potential to disrupt hospital operations, which can affect overall healthcare services. Hospitals are obligated to provide safe, quality, and effective healthcare services by prioritizing patient interests in accordance with hospital service standards.⁴

In Indonesia, several significant hacking incidents have shocked the public and demonstrated the vulnerabilities of digital era information systems. One of the most notable examples is the Bjorka case that occurred in 2022, where the perpetrator claimed to have accessed and disseminated the personal data of millions of citizens, including sensitive data from government databases. Another case involved the hacking of the DPR (House of Representatives) website, causing a shutdown of the legislative information system and the replacement of the homepage with a political message. The Tokopedia case also gained attention when the personal data of 91 million users was leaked to the dark web, as reported by Tirto.id in 2020.⁵

These cyber attack threats highlight the importance of safeguarding systems and data. At a basic level, cyber crimes like hacking can be carried out through various methods, including but not limited to malware installation, social engineering, and DDoS attacks. Hackers often exploit vulnerabilities in security configurations to infiltrate hospital networks and access sensitive data without authorization.⁶

Given these risks, it is crucial for healthcare institutions in Indonesia to strengthen their data security and ensure that information security policies and practices are regularly updated to protect patient data and ensure smooth

³ Riyan Putri Kumorowani and Dety Mulyanti, 'Analisis Penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan Pendekatan HOT FIT: Systematic Literature Review', *DIAGNOSA: Jurnal Ilmu Kesehatan Dan Keperawatan*, 1.2 (2023), 25–33 <<https://doi.org/10.59581/diagnosa-widyakarya.v1i2.174>>.

⁴ Youce Albertus Wilar, Kristia Yulianwan, and Akhmad Amiruddin Natsir, 'Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire', *MAHESA : Malahayati Health Student Journal*, 3.10 (2023), 3365–74 <<https://doi.org/10.33024/mahesa.v3i10.11246>>.

⁵ Indah Sari, 'Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya', *Jurnal Sistem Informasi Universitas Suryadarma*, 10.2 (2014) <<https://doi.org/10.35968/jsi.v10i2.1086>>.

⁶ Yogi Oktafian Arisandy, 'Penegakan Hukum Terhadap Cyber Crime Hacker', *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1.3 (2021), 162–69 <<https://doi.org/10.18196/ijclc.v1i3.11264>>.

operations. This study aims to identify vulnerabilities in SIMRS in Indonesia, analyze the legal implications of cybercrime hacking, and evaluate the effectiveness of current regulations in addressing and preventing cyber crimes in the healthcare sector.⁷

2. Research Method

This study uses a doctrinal method focusing on normative analysis of regulations and legal documents relevant to hacking in the Hospital Management Information System (SIMRS). Data will be collected through a literature study that includes laws such as Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Information and Electronic Transactions, the Minister of Health Regulation of the Republic of Indonesia No. 82 of 2013 on Hospital Management Information Systems, and other relevant regulations, as well as related academic literature, including journals and legal books.⁸ The analysis will be conducted to evaluate the effectiveness of existing regulations in addressing cybercrime, and the results will be used to identify gaps in the law that require reform. This data and analysis will be processed to develop legal recommendations and solution-oriented recommendations aimed at evaluating and improving the security of systems and data in SIMRS in hospitals across Indonesia.⁹ References will include books and scholarly works such as Edi Setiawan's comprehensive book on data protection law in Indonesia, and an article by Karina Mulya Putri discussing national cybersecurity policies.

3. Results and Discussion

Hospital Management Information System (SIMRS) and Patient Data Protection

The Hospital Management Information System (SIMRS) is a critical infrastructure that integrates processes, information technology, and personnel to effectively manage hospital operational data. SIMRS encompasses the management of patient medical records, human resources, finances, and pharmaceutical supplies, all of which must be protected from unauthorized access. The importance of SIMRS lies not only in operational efficiency but also in its ability to facilitate decision-making based on accurate and real-time data,

⁷ Mohammad S Jalali and Jessica P Kaiser, 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective', *Journal of Medical Internet Research*, 20.5 (2018), e10059
<<https://doi.org/10.2196/10059>>.

⁸ Irwansyah, *Penelitian Hukum; Pilihan Metode Dan Praktik Penulisan Arikel* (Yogyakarta: Mitra Buana Media, 2020).

⁹ Ani Purwati, *Metode Penelitian Hukum: Teori Dan Praktek* (Surabaya: CV. Jakad Media Publishing, 2020); Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Perss, 2020).

which is essential for improving the quality of healthcare services and ensuring compliance with data security and confidentiality standards.¹⁰

The Minister of Health Regulation of the Republic of Indonesia No. 24 of 2022 on Electronic Medical Records (hereinafter referred to as Permenkes EMR) has established mandatory standards for the electronic digital management of health data, which must be protected from cybercrime. This regulation aims to enhance patient data security by requiring hospitals to implement adequate systems for managing and storing electronic medical records. With EMR, it is expected that patient data can be managed in a more structured and integrated manner; however, this also presents significant cybersecurity challenges, given the risks of cyber hacking and information leaks that could threaten patient privacy and the integrity of healthcare institutions.¹¹

Article 12 of the Minister of Health Regulation of the Republic of Indonesia No. 24 of 2022 on Electronic Medical Records (Permenkes EMR) states that Health Service Facilities managing Electronic Medical Records or Electronic System Providers as referred to in Article 9, paragraph (1), are required to register their Electronic Systems with the Ministry of Health. This registration must include documents that at least consist of the name of the Electronic System, system documentation, available features/functions, data storage location, and variable and metadata.¹²

In the context of cybersecurity, SIMRS must be equipped with robust security mechanisms to protect patient data from cyber hacking attacks. Data encryption, two-factor authentication, and the use of audit trails are some techniques implemented to enhance security. However, studies show that there are still security gaps that hackers can exploit, highlighting the importance of regular security updates and comprehensive cybersecurity education for hospital staff.

Cyber attacks, especially hacking, pose a threat to systems in SIMRS. Hackers can exploit weak system vulnerabilities to steal or damage patient data, potentially harming patients and damaging the hospital's reputation. Incidents such as massive data breaches in the healthcare industry have shown the importance of having security systems that not only comply with current standards but are also proactive in addressing new threats. With the evolution of technology and hacking methodologies, hospitals need to continuously analyze and improve their network security, as well as involve cybersecurity experts to

¹⁰ Tati Sudiarti, Soedarto Soepangat, and Teguh Wiyono, 'Analisis Implementasi Sistem Informasi Manajemen Rumah Sakit Di Instalasi Rawat Jalan Klinik Paru Rumah Sakit Paru Cirebon', *Jurnal Manajemen Kesehatan Yayasan RS.Dr. Soetomo*, 5.1 (2019), 57
<<https://doi.org/10.29241/jmk.v5i1.138>>.

¹¹ Rospita Adelina Siregar, 'Penerapan Permenkes Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Efektivitas Pelayanan Kesehatan', *Jurnal Ilmu Hukum Kyadiren*, 5.2 (2024).

¹² Yohnly Boelian Dachban, Redyanto Sidi, and Yasmirah Mandasari Saragih, 'Tinjauan Yuridis Kesiapan Rumah Sakit Dan Tanggungjawab Rumah Sakit Pasca Peraturan Menteri Kesehatan Nomor: 24/2022 Tentang Rekam Medis Dan Kesiapan Rumah Sakit', *Jurnal Ners*, 7.1 (2023), 232–39
<<https://doi.org/10.31004/jn.v7i1.13001>>.

regularly audit and test their systems to ensure they remain protected and that healthcare services are not disrupted or compromised.¹³

The implementation of EMR has transformed the way hospitals manage health information, but it also brings new challenges in data security. Although EMR can enhance accessibility and efficiency, its vulnerability to cyberattacks requires significant investment in security technology, personnel training, and the development of effective policies for risk mitigation. Awareness and training in cybersecurity are critical aspects that are often overlooked but are essential for protecting health data from the constantly evolving cyber threats. Through an integrated and layered approach to cybersecurity, SIMRS can protect itself from the increasing threats while ensuring that the integrity and privacy of patient data are maintained. The implementation of effective and sustainable security strategies will be key in addressing the challenges of cybercrime hacking against SIMRS in the digital era.¹⁴

Cyber Crime Hacking in the Context of Criminal Law

Hacking is an art of penetrating computer systems to understand how they work and their structure, as described by Revelation Loa-Ash: *"Hacking is the act of penetrating computer systems to gain knowledge about the system and how it works. Hacking is illegal because we demand free access to ALL data, and we get it. This pisses people off and we are outcasted from society, and in order to stay out of prison, we must keep our status of being a hacker/phreaker a secret."*

Hacking is illegal because accessing and reading someone's data without permission in a covert manner is akin to deceiving or offending people, which is why hackers/phreakers often conceal their identities. However, a deeper examination reveals that within hacker communities, there are specific cultures and rules, and hackers have different motives and goals. According to hacker expert Emmanuel Goldstein from the United States; *"One of the common misconceptions is that anyone considered a hacker is doing something illegal. It's a sad commentary on the state of our society when someone who is basically seeking knowledge and the truth is assumed to be up to something nefarious. Nothing could be further from the truth. Hackers, in their idealistic naiveté, reveal the facts that they discover, without regard for money, corporate secrets or government cover-ups"*.¹⁵

Although hacking is illegal, not all hackers are malicious. Some hackers, motivated purely by challenge and enjoyment, aim to prove their ability to penetrate systems. As stated by Eric Steven Raymond; *"Being a hacker is lots of fun,*

¹³ Karma Maha Wirajaya and I Nyoman Adikarya Nugraha, 'Evaluasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan Metode HOT-Fit Di Rumah Sakit Daerah Mangusada', *Jurnal Manajemen Kesehatan Yayasan RS.Dr. Soetomo*, 8.1 (2022), 124 <<https://doi.org/10.29241/jmk.v8i1.934>>.

¹⁴ Muhamad Ganda Saputra and others, 'Evaluasi Implementasi Sistem Informasi Manajemen Rumah Sakit Dengan Metode HOT-Fit Di RSU Muhammadiyah Babat', *J-REMI : Jurnal Rekam Medik Dan Informasi Kesehatan*, 4.4 (2023), 248–56 <<https://doi.org/10.25047/j-remi.v4i4.4047>>.

¹⁵ Rafi Septia Budianto Pansariadi and Noenik Soekorini, 'Tindak Pidana Cyber Crime Dan Penegakan Hukumnya', *Binamulia Hukum*, 12.2 (2023), 287–98 <<https://doi.org/10.37893/jbh.v12i2.605>>.

but it's a kind of fun that takes lots of effort. The effort takes motivation. Successful athletes get their motivation from a kind of physical delight in making their bodies perform, in pushing themselves past their own physical limits. Similarly, to be a hacker you have to get a basic thrill from solving problems, sharpening your skills, and exercising your intelligence."

The methods used by hackers and crackers (malicious hackers) are similar, but their motivations differ. Crackers aim to damage and steal, while phreakers, who have similar motivations to crackers, differ in their methods and targets. Crackers focus on computer networks and software, whereas phreakers target telephone networks and phone billing software.¹⁶

True hackers can serve as partners to law enforcement in investigating crackers and phreakers and bringing them to justice. Notable contributions by true hackers include: writing open-source software that is non-commercial, allowing anyone to use and develop it, such as the Demigods software, where anyone can freely write and use it; helping to test weaknesses in open-source software; publishing useful information in BBS's (Bulletin Board Systems) and FAQs (Frequently Asked Questions) lists; and assisting in maintaining the proper functioning of network infrastructure.

Hacking has frequently occurred in Indonesia, often targeting specific websites or systems. Examples of hacking cases in Indonesia include attacks on government sites, educational institutions, and private companies, with aims ranging from data theft and system damage to simply demonstrating security weaknesses. These attacks involve website defacement, personal data theft, and malware dissemination. Additionally, Distributed Denial of Service (DDoS) attacks, which cripple online services by overwhelming target servers with excessive internet traffic, are also common.¹⁷

Notable hacking cases in Indonesia include attacks on the KPU (General Elections Commission) website, resulting in voter data breaches; ransomware attacks on various companies demanding ransom to restore access to encrypted data; and attempts to hack banks and financial institutions to steal financial information. All of these incidents highlight the need for enhanced cybersecurity and collaboration between the government, private sector, and ethical hacking communities to protect Indonesia's digital infrastructure:

1. Hacking of BPJS Kesehatan Website

In May 2021, the website of the Social Security Agency for Health (BPJS Kesehatan), namely bpjs-kesehatan.go.id, was reportedly hacked. This breach led to the leak of data from 279 million Indonesians, which was sold

¹⁶ I Gusti Ayu Suanti Karnadi Singgi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiarta, 'Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)', *Jurnal Konstruksi Hukum*, 1.2 (2020), 334–39 <<https://doi.org/10.22225/jkh.2.1.2553.334-339>>.

¹⁷ Musa Darwin Pane and Sahat Maruli tua Situmeang, 'Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi', *Jurnal Loyalitas Sosial: Journal of Community Service in Humanities and Social Sciences*, 3.2 (2021), 93 <<https://doi.org/10.32493/JLS.v3i2.p93-105>>.

on the online forum Raid Forums by an account named “Kotz.” The dataset, which included National Identification Numbers (NIK), phone numbers, emails, addresses, and salaries, was sold for 0.15 bitcoin, equivalent to approximately IDR 84.4 million. To prevent further spread, the Ministry of Communication and Information Technology (Kominfo) requested the suspension of access to the link for downloading the personal data and blocked Raid Forums.

2. BRI Life Insurance Data Leak

Another hacking incident involved BRI Life insurance company. In July 2021, approximately 2 million BRI Life customer records were allegedly leaked and sold online for \$7,000, or about IDR 101.6 million. This was first reported by the Twitter account @UnderTheBreach, which claimed that hackers had stolen 250 GB of data from BRI Life, including 2 million customer records in PDF format and 463,000 additional documents. The data included ID card photos, bank account information, taxpayer numbers, birth certificates, and medical records. It is suspected that the data leak occurred due to a security vulnerability in BRI Life’s electronic system, exploited by irresponsible parties.

3. Defacement Attack on the Cabinet Secretariat RI Website

At the same time, the website of the Cabinet Secretariat of the Republic of Indonesia, setkab.go.id, was subject to a defacement attack. This type of attack allows hackers to alter the appearance of the targeted website. It is suspected that this hack was conducted for economic gain, such as selling a backdoor script from the victim’s website to interested parties. Initially, the Setkab.go.id site was hacked to the extent that it became inaccessible.

Hackers are generally individuals who access a computer system in an unauthorized or incorrect manner. This act is often driven by curiosity and admiration for technology, which then evolves into a challenge to test the limits of the computer system. Although often regarded as a violation, a hacker’s initial motive may stem from a desire to gain a deeper understanding or even to improve the system they encounter.¹⁸

In practice, hackers can be categorized as either good (white hat) or bad (black hat). However, regardless of their intentions, their actions are still considered illegal due to the unauthorized access, which is legally classified as an intrusion into a computer system. Hacker activities typically involve several stages, such as identifying the target system, infiltrating and intercepting passwords, exploring the system, creating backdoors, and erasing traces. This crime in the real world can be analogized to entering a territory without

¹⁸ Budi Kristian Bivanda Putra, ‘Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia’, *Pamulang Law Review*, 1.1 (2019), 1 <<https://doi.org/10.32493/palrev.v1i1.2842>>.

permission, and under the Indonesian Penal Code (KUHP), such actions are regulated under Article 167.

Article 167 of the Indonesian Penal Code (KUHP) can be a relevant analogy for cyber crimes committed by hackers, even though the article specifically addresses physical intrusion into a person's house, enclosed room, or property. According to this article, anyone who forcibly or unlawfully enters a place used by another person, or who does not leave the place immediately after being asked by the rightful owner, can be punished with imprisonment or a fine. In a cyber context, a hacker's unauthorized access to a computer system can be compared to someone entering another person's property without permission. Just like physical intrusion, illegal access to computer systems is often carried out through specific methods, such as using intercepted passwords or backdoors, which can be analogized to the physical methods mentioned in the article, like breaking in or climbing. Therefore, although Article 167 KUHP does not explicitly mention cyber crimes, its principles can be applied to describe hacking actions as a similar form of intrusion and thus considered within a modern legal framework for addressing technological crimes.¹⁹

To categorize hacking into the offense regulated by Article 167 of the Criminal Code, we need to elaborate the elements as mentioned in Paragraphs (1) and (2). In Paragraph (1), the elements include: "Whoever goes against the rights of others," which in the context of hacking means that the perpetrator accesses without the permission of the system owner; "Entering by force," which can be interpreted as the act of infiltrating the system in an unauthorized way; "Into a closed house or room or yard, which is used by another person," which can be analogized to a computer system used by another person; "Or being there without his rights," which reflects the perpetrator being in the system without authorization; and "Not leaving the place immediately, at the request of the person entitled or on behalf of the person who has the right to leave," which refers to the perpetrator who remains in the system even though he has been asked to leave.

Meanwhile, Paragraph (2) adds elements such as: "Whose goods; Enter; By breaking or climbing, using fake keys, fake orders, or fake official clothes," which in a cyber context can mean using methods such as cracking passwords, using fake identities, or creating backdoors; and "By ignorance of the right and other than because of confusion; Enter the place earlier," which describes the actions of the perpetrator who entered the system without the knowledge of the owner or the legitimate authority. By outlining these elements, it can be seen that hacking has similarities with the act of physical infiltration regulated in Article 167 of the

¹⁹ Hairan Hairan and Rahmat Datau, 'Kebijakan Formulasi Hukum Pidana Terhadap Tindak Pidana Pertanahan Di Indonesia', *Gorontalo Law Review*, 3.1 (2020), 17
<<https://doi.org/10.32662/golrev.v3i1.907>>.

Criminal Code, so that the legal principles in the article can be applied to assess cybercrime.²⁰

Cyber Crime Hacking in Hospital Management Information Systems (SIMRS)

In the current digital era, the increased reliance on information technology in the healthcare sector, particularly through the use of SIMRS, brings significant risks related to cybercrime. Hacking, as a specific form of cybercrime, is a major concern because it threatens the integrity and confidentiality of sensitive medical data. Under Indonesian law, such actions are regulated and penalized under Law No. 11 of 2008 as amended by Law No. 19 of 2016 on Electronic Information and Transactions (commonly referred to as the ITE Law).

Indonesia has a legal foundation for addressing various aspects of cybercrime through the ITE Law, even though hacking specifically targeting Hospital Management Information Systems (SIMRS) may not have occurred or been revealed as cases. The ITE Law addresses various forms of cybercrime, including hacking, by detailing relevant elements of the offense. Article 30 paragraph (1) of the ITE Law states, "Any person who intentionally and without right or against the law accesses another person's computer and/or electronic system in any way." This provision specifically criminalizes unauthorized access to computer systems, including SIMRS, aimed at protecting sensitive and operational data of hospitals from irresponsible hacking activities.

Furthermore, Article 30 paragraph (2) in conjunction with Article 46 paragraph (2) of the ITE Law states that unauthorized access with the intent to obtain electronic information and/or electronic documents is subject to a maximum prison sentence of 7 years and/or a fine of up to IDR 700 million. This underscores the seriousness of the Indonesian government in addressing cybercrime, including hacking that can impact critical systems like SIMRS. Therefore, even though no cases of SIMRS hacking have been reported, the existing legal framework is sufficient to impose severe penalties on offenders, providing strong legal protection for the integrity and security of electronic systems in Indonesia.²¹

The impact of hacking on Hospital Management Information Systems (SIMRS) is extensive and multifaceted. Beyond the direct losses such as data loss that can harm hospital operations, there are also significant secondary impacts

²⁰ Abiyyu Ghaly and Maria Silvy E. Wangga, 'Analisis Tindak Pidana Pencabulan Atau Memasuki Rumah Tanpa Izin Menurut Kuhp (Putusan Nomor 137/PID.B/2020/PN RKB)', *Reformasi Hukum Trisakti*, 5.4 (2023), 1154–63 <<https://doi.org/10.25105/refor.v5i4.18552>>; Gunawan Djajaputra, Endang Pandamdari, and Endyk M. Asror, 'Analisis Hak Atas Tanah Dalam Sengketa Kepemilikan Tanah Beserta Penyelesaiannya', *Synotic Law: Jurnal Ilmu Hukum*, 1.1 (2022), 45–56 <<https://doi.org/10.56110/sl.v1i1.4>>.

²¹ Ahmad Aryo and Hatarto Pakpahan, 'Tindak Pidana Turut Serta Mengakses Komputer Dan/Atau Sistem Elektronik Dengan Modus Skimming', *Bhirawa Law Journal*, 2.2 (2021), 122–29 <<https://doi.org/10.26905/blj.v2i2.6822>>.

like service disruptions, which can hinder patient care and hospital operations. The loss of patient trust is a major risk, as cyberattacks that steal personal data can diminish public confidence in the security and integrity of the hospital. Additionally, hospitals may face potential legal actions from affected patients and must notify them of breaches in accordance with applicable regulations, which can result in sanctions from regulators. The recovery process from a cyberattack often involves significant time and resources, including comprehensive security audits to identify and close security gaps, repairing affected systems, and enhancing security measures to prevent similar incidents in the future. All of these factors contribute to high costs and long-term impacts on the hospital's reputation and reliability.

Facing the risk of cyber crime, hospitals must implement a multi-protection security strategy that includes both technical and human aspects. This strategy includes software updates, ensuring all operational systems and security software are always updated to close security loopholes that hackers may exploit. In addition, employee training is essential, with a regular cybersecurity awareness training program for all hospital staff to increase awareness of cyber threats and how to deal with them. Security audits and monitoring should also be carried out regularly, using monitoring tools capable of detecting suspicious activity in the system in real-time to provide a quick response to potential threats. No less important, backup and recovery policies must be implemented strongly, ensuring that important hospital data can be recovered quickly in the event of a cyber attack or system failure, so that hospital operations continue to run with minimal disruption. The comprehensive implementation of this strategy will help hospitals reduce the risk of cyberattacks and protect highly sensitive patient data and information.²²

In addressing the challenge of cybercrime hacking against Hospital Management Information Systems (HMIS), healthcare institutions need to adopt an approach that goes beyond technical solutions and includes the development of policies and protocols that strengthen their defenses. It is essential to implement policies that include regular risk assessments, the development of incident response procedures, and the execution of cybersecurity awareness training for all employees. Additionally, intersectoral cooperation, both nationally and internationally, is crucial for sharing information about the latest threats and effective mitigation strategies. Compliance with existing regulations also plays a key role in ensuring that security measures align with industry standards and legal requirements. By adopting a comprehensive and proactive approach, hospitals can enhance their resilience to cyber threats, protect patient data from theft or damage, and maintain the integrity and reliability of their

²² M. Syuib and Maisarah Maisarah, 'Tindak Pidana Pencurian Jaringan Wifi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik', *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 6.1 (2021), 51
<<https://doi.org/10.22373/justisia.v6i1.10611>>.

information systems. This approach not only safeguards critical information assets but also helps maintain patient trust and ensures the continuity of hospital operations in the face of potential cyber threats.

4. Conclusion

In the context of legal research on cybercrime, particularly hacking against Hospital Management Information Systems (HMIS), there is a need for specific identification of security vulnerabilities that are not only technical but also organizational and regulatory. There is an urgent need to integrate national legal frameworks with more dynamic and adaptive international cybersecurity standards. This is crucial as hackers not only enhance their technical capabilities but also employ increasingly sophisticated and cross-jurisdictional tactics. This research reveals that the current legal framework, while adequate in some aspects, still requires adjustments to effectively address and prevent cybercrime in the healthcare sector. Specifically, the Electronic Information and Transactions Law (UU ITE) needs to be continuously updated to cover new aspects of cybercrime, including the use of AI and machine learning by criminals to access and manipulate data automatically.

Based on these discussions, the author conveyed concrete recommendations as strategic steps to improve cybersecurity in the health sector. First, the Revision and Adaptation of the ITE Law is needed to adapt to the latest technological developments and practices in cybersecurity. The addition of provisions specifically regulating data security in the health sector is very important, including provisions on the use of artificial intelligence and machine learning to predict and prevent cyberattacks. This will allow for the initial protection of the system as well as its data and backups. Second, the Integration of International Standards must be carried out by adopting standards such as ISO/IEC 27001 on information security management systems. The adoption of these international standards will increase global confidence and ensure that security practices in Indonesia are on par with best practices in the world.

Furthermore, enhancing human resource capacity requires significant investment in training personnel in the healthcare sector, particularly in cybersecurity. Certification programs and continuous training for IT technicians in hospitals should be mandatory, with a focus on realistic hacking scenario simulations. Additionally, public-private sector collaboration should be strengthened by involving government, private sector, and academic institutions in developing cybersecurity solutions, including the establishment of a national cybersecurity response center focused on the healthcare sector. Finally, regular audits and monitoring should be mandatory for all healthcare facilities, with cybersecurity audits conducted by independent external auditors covering risk assessments and system penetration testing. Implementing these recommendations is expected to reduce the risks and impacts of cybercrime on

HMIS, enhance public trust in the integrity of health systems, and ensure optimal protection of health data through thorough and ongoing legal analysis of existing and forthcoming regulations.

References

- Arisandy, Yogi Oktafian, 'Penegakan Hukum Terhadap Cyber Crime Hacker', *Indonesian Journal of Criminal Law and Criminology (IJCLC)*, 1.3 (2021), 162–69 <<https://doi.org/10.18196/ijclc.v1i3.11264>>
- Aryo, Ahmad, and Hatarto Pakpahan, 'Tindak Pidana Turut Serta Mengakses Komputer Dan/Atau Sistem Elektronik Dengan Modus Skimming', *Bhirawa Law Journal*, 2.2 (2021), 122–29 <<https://doi.org/10.26905/blj.v2i2.6822>>
- Dachban, Yohnly Boelian, Redyanto Sidi, and Yasmirah Mandasari Saragih, 'Tinjauan Yuridis Kesiapan Rumah Sakit Dan Tanggungjawab Rumah Sakit Pasca Peraturan Menteri Kesehatan Nomor: 24/2022 Tentang Rekam Medis Dan Kesiapan Rumah Sakit', *Jurnal Ners*, 7.1 (2023), 232–39 <<https://doi.org/10.31004/jn.v7i1.13001>>
- Djajaputra, Gunawan, Endang Pandamdari, and Endyk M. Asror, 'Analisis Hak Atas Tanah Dalam Sengketa Kepemilikan Tanah Beserta Penyelesaiannya', *Synotic Law: Jurnal Ilmu Hukum*, 1.1 (2022), 45–56 <<https://doi.org/10.56110/sl.v1i1.4>>
- Ghaly, Abiyyu, and Maria Silvya E. Wangga, 'Analisis Tindak Pidana Pencabulan Atau Memasuki Rumah Tanpa Izin Menurut Kuhp (Putusan Nomor 137/PID.B/2020/PN RKB)', *Reformasi Hukum Trisakti*, 5.4 (2023), 1154–63 <<https://doi.org/10.25105/refor.v5i4.18552>>
- Hairan, Hairan, and Rahmat Datau, 'Kebijakan Formulasi Hukum Pidana Terhadap Tindak Pidana Pertanahan Di Indonesia', *Gorontalo Law Review*, 3.1 (2020), 17 <<https://doi.org/10.32662/golrev.v3i1.907>>
- Irwansyah, *Penelitian Hukum; Pilihan Metode Dan Praktik Penulisan Arikel* (Yogyakarta: Mitra Buana Media, 2020)
- Jalali, Mohammad S, and Jessica P Kaiser, 'Cybersecurity in Hospitals: A Systematic, Organizational Perspective', *Journal of Medical Internet Research*, 20.5 (2018), e10059 <<https://doi.org/10.2196/10059>>
- Kumorowani, Riyan Putri, and Dety Mulyanti, 'Analisis Penerapan Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan Pendekatan HOT FIT: Systematic Literature Review', *DIAGNOSA: Jurnal Ilmu Kesehatan Dan Keperawatan*, 1.2 (2023), 25–33 <<https://doi.org/10.59581/diagnosa-widyakarya.v1i2.174>>
- Muhaimin, *Metode Penelitian Hukum* (Mataram: Mataram University Perss, 2020)
- Pane, Musa Darwin, and Sahat Maruli tua Situmeang, 'Penegakan Hukum Cyber Crime Dalam Upaya Penanggulangan Tindak Pidana Teknologi Informasi', *Jurnal Loyalitas Sosial: Journal of Community Service in Humanities and Social Sciences*, 3.2 (2021), 93 <<https://doi.org/10.32493/JLS.v3i2.p93-105>>
- Pansariadi, Rafi Septia Budianto, and Noenik Soekorini, 'Tindak Pidana Cyber Crime Dan Penegakan Hukumnya', *Binamulia Hukum*, 12.2 (2023), 287–98 <<https://doi.org/10.37893/jbh.v12i2.605>>

- Purwati, Ani, *Metode Penelitian Hukum: Teori Dan Praktek* (Surabaya: CV. Jakad Media Publishing, 2020)
- Putra, Budi Kristian Bivanda, 'Kebijakan Aplikasi Tindak Pidana Siber (Cyber Crime) Di Indonesia', *Pamulang Law Review*, 1.1 (2019), 1
<<https://doi.org/10.32493/palrev.v1i1.2842>>
- Rusli, Sienny, 'Implementasi Sistem Informasi Manajemen Rumah Sakit Dalam Pengolahan Data Rumah Sakit', *JKM (Jurnal Kesehatan Masyarakat) Cendekia Utama*, 10.2 (2022), 158 <<https://doi.org/10.31596/jkm.v10i2.1036>>
- Saputra, Muhamad Ganda, Nihayatul Munaa, Yuni Anggraini, Faizatul Ummah, Nahardian Vica Rahmawati, Ari Kusdiyana, and others, 'Evaluasi Implementasi Sistem Informasi Manajemen Rumah Sakit Dengan Metode HOT-Fit Di RSU Muhammadiyah Babat', *J-REMI : Jurnal Rekam Medik Dan Informasi Kesehatan*, 4.4 (2023), 248–56 <<https://doi.org/10.25047/j-remi.v4i4.4047>>
- Sari, Indah, 'Mengenal Hacking Sebagai Salah Satu Kejahatan Di Dunia Maya', *Jurnal Sistem Informasi Universitas Suryadarma*, 10.2 (2014)
<<https://doi.org/10.35968/jsi.v10i2.1086>>
- Singgi, I Gusti Ayu Suanti Karnadi, I Gusti Bagus Suryawan, and I Nyoman Gede Sugiarta, 'Penegakan Hukum Terhadap Tindak Pidana Peretasan Sebagai Bentuk Kejahatan Mayantara (Cyber Crime)', *Jurnal Konstruksi Hukum*, 1.2 (2020), 334–39 <<https://doi.org/10.22225/jkh.2.1.2553.334-339>>
- Siregar, Rospita Adelina, 'Penerapan Permenkes Nomor 24 Tahun 2022 Tentang Rekam Medis Terhadap Efektivitas Pelayanan Kesehatan', *Jurnal Ilmu Hukum Kyadiren*, 5.2 (2024)
- Sudiarti, Tati, Soedarto Soepangat, and Teguh Wiyono, 'Analisis Implementasi Sistem Informasi Manajemen Rumah Sakit Di Instalasi Rawat Jalan Klinik Paru Rumah Sakit Paru Cirebon', *Jurnal Manajemen Kesehatan Yayasan RS.Dr. Soetomo*, 5.1 (2019), 57 <<https://doi.org/10.29241/jmk.v5i1.138>>
- Syuib, M., and Maisarah Maisarah, 'Tindak Pidana Pencurian Jaringan Wifi Menurut Pasal 30 Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik', *Jurnal Justisia : Jurnal Ilmu Hukum, Perundang-Undangan Dan Pranata Sosial*, 6.1 (2021), 51 <<https://doi.org/10.22373/justisia.v6i1.10611>>
- Tangel, Pricillia T., Aaltje E. Manampiring, and Nova H. Kapantow, 'Penerapan Sistem Informasi Manajemen Rumah Sakit Di RSUD Dr. Sam Ratulangi Tondano', *E-CliniC*, 12.2 (2023), 121–33 <<https://doi.org/10.35790/ecl.v12i2.52755>>
- Wilar, Youce Albertus, Kristia Yulian, and Akhmad Amiruddin Natsir, 'Analisis Keamanan Sistem Manajemen Informasi Rumah Sakit Umum Daerah Nabire', *MAHESA : Malahayati Health Student Journal*, 3.10 (2023), 3365–74
<<https://doi.org/10.33024/mahesa.v3i10.11246>>
- Wirajaya, Karma Maha, and I Nyoman Adikarya Nugraha, 'Evaluasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) Dengan Metode HOT-Fit Di Rumah Sakit Daerah Mangusada', *Jurnal Manajemen Kesehatan Yayasan RS.Dr. Soetomo*, 8.1 (2022), 124 <<https://doi.org/10.29241/jmk.v8i1.934>>