e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

Review Of The Legality And Security Aspects Of Electronic Signature Use In Electronic Medical Records At Bakti Pajajaran Regional Public Hospital

Nendy Ardiansyah[1]*, Diansyah[2]
* Medical Records and Health Information Study Program, Politeknik Piksi Ganesha, Indonesia

Abstract

The implementation of electronic signatures in electronic medical records (EMRs) is intended to strengthen authentication, document integrity, accountability, and legal certainty in digital health services. This study reviewed the legality and security of electronic signature use in EMRs at Bakti Pajajaran Regional Public Hospital. A normative-empirical legal design with a descriptive qualitative approach was applied. Primary legal materials and relevant secondary literature were examined, while field data were obtained through in-depth interviews, observation, and documentation from 30 purposively selected informants representing medical records personnel, nurses, midwives, nutritionists, radiographers, information technology staff, and the head of the medical records installation. The study found that all 237 healthcare providers had used electronic signatures in the hospital information environment; however, none of the clinical electronic signatures were certified. The only certified electronic signature was used by the hospital director for administrative documents through the SRIKANDI application. Twenty of 32 reviewed medical record forms had been converted to electronic format, whereas 12 forms, particularly consent-related documents, remained manual. Major barriers included limited storage infrastructure, financing constraints, insufficient periodic socialization, and the absence of a dedicated standard operating procedure. These findings indicate that administrative adoption alone does not ensure adequate legal assurance and information security. The hospital should accelerate certified electronic signature implementation, establish specific governance procedures, strengthen security infrastructure, and provide sustainable organizational and financial support.

Keywords: electronic medical record, electronic signature, legality, security, healthcare provider

Correspondent Author: Nendy Ardiansyah
E-mail: Nendyardiansyah586@gmail.com

Resive : 13 September 2026
Revised : 16 September 2026
Accept : 16 September 2026
Publish : 16 September 2026

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

1. Introduction

The rapid development of information technology has transformed health services by enabling faster, more accurate, and more comprehensive access to clinical and administrative information. In Indonesia, hospitals are responsible for providing comprehensive individual health services, including inpatient, outpatient, and emergency care, as regulated by Law Number 17 of 2023 on Health. These services are supported by medical records as an essential source of clinical evidence, continuity of care, quality assurance, and institutional accountability (Azzahra and Sugiarti, 2025). Minister of Health Regulation Number 24 of 2022 defines medical records as documents containing patient identity, examinations, treatment, procedures, and other services provided to patients. The regulation also directs the transition from paper-based records to electronic medical records (EMRs) and requires healthcare facilities to implement EMRs. This transformation is expected to improve efficiency, accuracy, accessibility, and effectiveness in health information management. Nevertheless, the transition to digital documentation introduces legal and information-security challenges, particularly regarding the confidentiality, authenticity, integrity, and accountability of patient data.

Electronic signatures are an important authentication and verification mechanism in EMRs because they can associate the identity of a healthcare professional with a specific electronic document or clinical action. Indonesian electronic information law recognizes electronic signatures as electronic information attached to or associated with other electronic information and used for verification and authentication. Government Regulation Number 71 of 2019 distinguishes certified and uncertified electronic signatures. Certified electronic signatures are supported by an electronic certificate issued through an officially recognized electronic certification provider, providing stronger assurance of identity, integrity, and legal evidentiary value. In contrast, uncertified signatures may offer more limited guarantees when used for sensitive documents that can become legal evidence (Wati, 2023; Dewi et al., 2024). The need for reliable electronic signatures is particularly important in medical records because healthcare data are sensitive personal data. Security controls such as encryption, authentication, passphrases, access restrictions, and audit mechanisms are required to protect the integrity and confidentiality of electronic health information (Ma'rifat, Suraharta and Jaya, 2024). Prior research also indicates that the implementation of certified electronic signatures in healthcare institutions remains uneven. Azzahra and Sugiarti (2025), for example, reported that certified electronic signatures were available only for selected physicians, while other health professionals continued to use uncertified signatures.

Preliminary observation at Bakti Pajajaran Regional Public Hospital between 18 February and 18 March 2026 showed that electronic signatures had been incorporated into

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

EMR workflows, but certified signatures had not yet been implemented for physicians, nurses, midwives, nutritionists, radiographers, and other clinical users. The hospital director already used a certified electronic signature for administrative documentation through SRIKANDI, whereas clinical EMR signatures remained uncertified. Infrastructure limitations, particularly data-storage capacity, were also identified. This creates an important gap between digital adoption and full legal-security compliance. Accordingly, this study aimed to analyze the legality and security aspects of electronic signature use in EMRs at Bakti Pajajaran Regional Public Hospital, identify implementation barriers, and assess the hospital's readiness to transition toward certified electronic signatures. The findings are expected to provide an evidence-based basis for strengthening internal governance, regulatory compliance, and information-security protection in electronic medical record management.

2. Research Methods

This study used a normative-empirical legal design combined with a descriptive qualitative approach. The normative component examined laws and regulations related to electronic signatures, electronic information, personal data protection, and electronic medical records. The empirical component examined how these requirements were implemented in practice at Bakti Pajajaran Regional Public Hospital. Primary legal materials consisted of relevant statutory provisions, while secondary materials included health-law literature and prior research related to EMRs and electronic signatures. The study was conducted at Bakti Pajajaran Regional Public Hospital, Cibinong, Bogor Regency, West Java, from 18 February to 18 March 2026. The study population comprised 237 healthcare providers who used electronic signatures in the hospital's electronic documentation environment. Purposive sampling was applied because the study sought in-depth information from personnel directly involved in the legality, security, operation, and governance of electronic signatures rather than statistical generalization.

Thirty informants were included: one head of the medical records installation, five medical records officers, five nurses, five midwives, five nutritionists, four radiographers, and five information technology staff members. Data were collected through in-depth interviews using a structured interview guide, direct observation of the electronic signature process, document review, and examination of selected medical record forms. Thirty medical record files were purposively reviewed to identify the distribution of electronic and manual forms across inpatient, outpatient, and emergency units. Data were organized thematically around legal validity, certification status, security safeguards, organizational readiness, infrastructure, and procedural governance.

3. Results and Discussion

a. Electronic Signature Implementation and Certification Status

Electronic signatures had become part of the hospital's electronic documentation process and were used by healthcare providers to support accountability for entries made in the EMR. During account creation, users were required to complete personal

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

identification and sign an integrity pact. This mechanism supported administrative accountability; however, it did not substitute for electronic certification by an officially recognized certification provider. The study found that all 237 healthcare providers had electronic signatures, but none of the clinical signatures were certified. The hospital director was the only person reported to use a certified electronic signature, and its use was limited to administrative documents through SRIKANDI.

Table 1. Electronic Signature Certification Status of Healthcare Providers

Profession	Total Users	Certified ES	Uncertified ES	Certified (%)
Attending physicians	16	0	16	0%
Nurses	120	0	120	0%
Midwives	70	0	70	0%
Nutritionists	15	0	15	0%
Radiographers	15	0	15	0%
Total	237	0	237	0%

The absence of certified signatures among clinical users indicates that the hospital's EMR environment had reached a stage of functional electronic adoption but had not yet achieved full certification-based assurance. Informants identified several implementation barriers, including limited information-technology infrastructure, organizational readiness, financing constraints, and the absence of a specific standard operating procedure (SOP) for certified electronic signatures. These barriers are consistent with the need to align technical implementation with institutional governance rather than treating electronic signatures solely as a software feature.

b. Distribution of Electronic and Manual Medical Record Forms

The hospital had implemented EMRs in inpatient, outpatient, and emergency services; however, documentation remained partially hybrid. Review of 32 forms showed that 20 had been converted to electronic format, while 12 were still maintained manually. Electronic forms predominated in inpatient care, where routine clinical documentation such as medical summaries, integrated patient progress notes, consultation forms, and initial medical assessments had already been digitized.

Table 2. Distribution of Electronic Medical Record Forms

Unit	Electronic Forms (Examples)	Number
Inpatient	Medical summary; patient transfer form; admission and discharge summary; blood transfusion record; ICCU admission/discharge criteria; ward admission/discharge criteria; consultation form; initial inpatient medical assessment; echocardiography; death report; integrated patient progress notes (CPPT)	13
Outpatient	Patient history and summary; PRMRJ; initial nursing assessment; repeat nursing assessment; general follow-up letter	5
Emergency Department	Initial emergency medical assessment; verification form	2

Manual forms were concentrated in documentation requiring patient or family consent, as well as selected medication, transfusion, and intensive-care observation

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

records. This pattern suggests that legal-signature concerns remain one of the practical reasons some high-accountability documents have not yet been fully migrated to the electronic environment.

Table 3. Distribution of Manual Medical Record Forms

Unit	Manual Forms (Examples)	Number
Inpatient	General consent; daily information notes; integrated patient notes; refusal/consent for medical procedures; blood transfusion procedure form; medication administration and monitoring record; ICU/ICCU/HCU/PICU observation card	8
Outpatient	Consent for high-risk treatment; consent for surgery and invasive procedures	2
Emergency Department	Refusal of medical treatment; consent for medical procedures	2

c. Legal Implications of Uncertified Electronic Signatures

Indonesian electronic information law recognizes electronic documents and electronic information as legal evidence, provided that applicable legal requirements are met. In this context, electronic signatures are expected to support verification and authentication. Certified electronic signatures provide stronger assurance because the signatory's identity is linked to an electronic certificate issued by a recognized electronic certification provider. Such certification supports authenticity, document integrity, and non-repudiation, which are particularly important when medical records may be used in medico-legal disputes (Putra and Surata, 2021; Razak, 2025). At Bakti Pajajaran Regional Public Hospital, the legal basis for clinical users' electronic signatures was still largely supported by an integrity pact. Although this arrangement can demonstrate internal accountability, it does not provide the same independent certification mechanism as a certified electronic signature. Informants reported that the hospital had initiated the certification process through the relevant government electronic certification mechanism, but implementation had not yet been completed because of organizational readiness, financing, and infrastructure limitations. These findings are consistent with Azzahra and Sugiarti (2025), who also identified unequal certification coverage among healthcare professionals.

The legal risk is not that every uncertified electronic signature is automatically invalid. Rather, the evidentiary strength, traceability, and certainty of identity may be more open to challenge when the signature lacks certification and robust technical controls. This distinction is important for EMRs because clinical records are not only operational documents but may also become evidence in professional accountability, insurance, audit, or legal proceedings.

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

d. Information Security and Data Protection

Electronic medical records contain sensitive personal information, including identity data, diagnoses, examination results, treatments, and other clinical information. Under Indonesian personal data protection and health legislation, hospitals have responsibilities as data controllers to ensure lawful processing, transparency, accountability, confidentiality, integrity, and availability of patient information. Therefore, electronic signature implementation should be integrated with broader information-security governance rather than evaluated independently. The study indicates that the hospital needs stronger technical and organizational safeguards. Recommended technical measures include encryption, multifactor authentication, role-based access restrictions based on the least-privilege principle, periodic access audits, automatic backups, firewall protection, intrusion-detection mechanisms, and secure internal network governance. Organizational measures include establishing a dedicated SOP, periodic security awareness training, routine evaluation, and clear responsibility for electronic signature administration (Widjaja et al., 2025).

Uncertified electronic signatures may be more vulnerable to identity misuse, document alteration, and disputes regarding authenticity when adequate verification controls are absent. The security concern becomes greater when a digital signature is treated merely as a visual representation of a handwritten signature rather than as a cryptographically supported authentication mechanism. Thus, the transition to certified electronic signatures should be accompanied by stronger identity verification, audit trails, access management, and secure certificate lifecycle management (Dewi et al., 2024).

e. Organizational Readiness, SOPs, and Infrastructure

The hospital had not yet established a dedicated SOP governing electronic signature use in EMRs. Existing policies focused more broadly on EMR management and service governance. The absence of a specific SOP creates variability in operational practice and may complicate orientation for new personnel, incident handling, certificate management, access revocation, and audit procedures. A formal SOP is therefore essential to translate national legal requirements into practical responsibilities at the institutional level.

Infrastructure readiness was also identified as a barrier, particularly the capacity required for electronic data storage and secure system operation. Financing constraints influenced the pace of certification and infrastructure improvement. These findings demonstrate that legal compliance depends on coordinated investment in technology, human resources, governance, and budgeting. The hospital's successful use of certified electronic signatures in SRIKANDI for administrative correspondence provides an

e-ISSN : 2987-0836 DOI : https://doi.org/10.59585/ijhs

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

internal reference point that could be extended to clinical EMR workflows once technical and organizational prerequisites are fulfilled (Adra and Permana, 2023).

f. Risks Associated with Uncertified Electronic Signatures

Three principal risks were identified. First, security risk arises because uncertified signatures may be more vulnerable to unauthorized alteration, identity misuse, or document falsification when strong cryptographic and verification controls are not in place. Second, legal-evidentiary risk may arise when the authenticity or integrity of a sensitive electronic document is challenged. Third, institutional credibility may be affected if patients, auditors, or partner institutions perceive electronic documentation controls as insufficient. These risks do not mean that every uncertified signature is unlawful; rather, they demonstrate why stronger certification, governance, and technical safeguards are necessary for high-accountability clinical documents.

4. Conclusion

Electronic signatures have been implemented in the electronic medical record environment at Bakti Pajajaran Regional Public Hospital, but certified electronic signatures have not yet been applied to the 237 clinical healthcare providers. The only certified electronic signature identified in the study was used by the hospital director for administrative documentation through the SRIKANDI application. The hospital's documentation environment remains hybrid: 20 of 32 reviewed forms were electronic, while 12 forms, particularly consent-related documents, remained manual. The principal barriers to broader certified electronic signature implementation were limited storage and information-technology infrastructure, financing constraints, insufficient periodic socialization, and the absence of a dedicated SOP. These conditions indicate that the hospital has achieved functional digital adoption but has not yet fully established certification-based legal assurance and security governance for clinical electronic signatures. The hospital should prioritize a specific SOP and policy for certified electronic signatures, accelerate registration and certification through an officially recognized electronic certification provider, conduct regular training and socialization, strengthen storage and cybersecurity infrastructure, and ensure sustainable financial support. Future research should examine certified electronic signature implementation after deployment, including audit-trail quality, user acceptance, security performance, and its contribution to legal certainty in electronic medical records.

5. Compliance with Ethical Standards

Acknowledgements

The authors acknowledge the institutional support provided by Bakti Pajajaran Regional Public Hospital and Politeknik Piksi Ganesha during the conduct of this study.

Publish : Association of Indonesian Teachers and Lecturers
International Journal of Health Sciences (IJHS)
Journal Homepage : https://jurnal.agdosi.com/index.php/IJHS/index
Volume 4 | Number 3 | September 2026 |

Disclosure of Conflict of Interest

No conflict of interest was reported in the source manuscript.

Statement of Informed Consent

The source manuscript does not report a formal informed-consent statement or an ethics approval number. These details should be confirmed and completed by the authors before journal submission.

References

Adra, A. and Permana, I. (2023) 'Pemanfaatan Aplikasi Srikandi Bagi Pegawai Di Pusat Pengembangan Sumber Daya Manusia Regional Bukittinggi', Juan: Jurnal Ilmu Administrasi Negara, 11, pp. 1–12.

Ardhia, U. and Ahmad, C. (2023) 'Tanda Tangan Elektronik Dalam Perjanjian Perdata', 4(4), pp. 192–204.

Ayu, J.D. et al. (2024) Metode Penelitian Kualitatif: Teori dan Penerapannya, Vol. 2.

Azzahra, N.S. and Sugiarti, I. (2025) 'Tinjauan Aspek Legalitas Penggunaan Tanda Tangan Elektronik Pada Rekam Medis Elektronik di RS. X Kab. Tasikmalaya', 10(1), pp. 170–177.

Dewi, D.C., Amelia, D., Ratama, F.R., Shidiq, F., Ferdansyah, F. and Anugrah, D. (2024) 'Tanda Tangan Elektronik Sebagai Solusi Hukum Perikatan Dalam Era Digital Di Indonesia', Letterlijk: Jurnal Hukum Perdata, 1(2), pp. 1–13. Available at: https://journal.fhukum.uniku.ac.id/letterlijk/article/view/66.

Dimensy (2025) 'Mengapa Tanda Tangan Elektronik yang Tidak Tersertifikasi Berisiko?', 26 March. Available at: https://dimensy.id/id/about.

Izzah, A.N.E. and Sugandha, W. (2021) 'Penggunaan Tanda Tangan Elektronik Dalam Penyelenggaraan E-Government Guna Mewujudkan Pelayanan Publik Yang Efisien', Journal of Law, Society, and Islamic Civilization, 9(1), p. 1. doi: 10.20961/jolsic.v9i1.52836.

Ma'rifat, R.A., Suraharta, I.M. and Jaya, I.I. (2024) 'Analisis Penggantian Password User ID Dalam Sistem Rekam Medis Elektronik Guna Menjaga Keamanan Data Rekam Medis Di Rumah Sakit', 2, pp. 306–312.

Ministry of Health of the Republic of Indonesia (2022) Regulation of the Minister of Health of the Republic of Indonesia Number 24 of 2022 concerning Medical Records.

Putra, G.F.E. and Surata, I.N. (2021) 'Peranan Dinas Komunikasi, Informatika, Persandian Dan Statistik Kabupaten Buleleng Dalam Menanggulangi Berita Hoaks Berdasarkan Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagaimana Telah Diubah', Kertha Widya, 8(2), pp. 127–153. doi: 10.37637/kw.v8i2.649.

Razak, K. (2025) 'Analisis Yuridis Terhadap Rekam Medis Elektronik Sebagai Alat Bukti Sengketa Medis', Citizen: Jurnal Ilmiah Multidisiplin Indonesia, 5(3), pp. 896–905. doi: 10.53866/jimi.v5i3.854.

Riyadi, S. et al. (2025) 'Implementasi Sistem Informasi Pengelolaan Surat Menggunakan SRIKANDI di Lingkup Pemerintahan Kabupaten Karanganyar', 6, pp. 167–186.

Satria, I. (2023) 'Rekam Medis Elektronik Pada Pelayanan Rumah Sakit Di Indonesia: Aspek Hukum Dan Implementasi', ALADALAH: Jurnal Politik, Sosial, Hukum dan Humaniora, 1(1), pp. 195–205.

Wati, T. (2023) 'Kekuatan Hukum dan Aspek Keamanan Dalam Tanda Tangan Elektronik', Journal Sains Student Research, 1(1), pp. 752–762. doi: 10.61722/jssr.v1i2.394.

Widjaja, G., Yustanti, D.E., Sijabat, H.H. and Dhanudibroto, H. (2025) 'Peran Rumah Sakit Sebagai Pengendali Data Dalam Menjamin Keamanan Data Pribadi Pasien Pada Sistem Kesehatan Digital', JK: Jurnal Kesehatan, 3(2), pp. 159–167.

Yuridis, T., Pidana, T., Tanda, P. and Elektronik, T. (2024) 'Tinjauan Yuridis Tindak Pidana Pemalsuan Tanda Tangan Elektronik dalam Kerangka Hukum Positif Indonesia', 3(1), pp. 94–100.