Jurnal Kesehatan Qamarul Huda
Vol. 13, No.2, Desember 2025, hlm. 179-185

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

Tinjauan Keamanan Data Rekam Medis Elektronik Pasien di RSUD Patut Patuh Patju Gerung Lombok Barat

Alin Putri Septiana[1*)], Muhamad Siladani Fatuhu[2)], Ni Komang Wijiani Yanti[3)], Fuji Khairan[4)]
Email: alinseptiana8@gmail.com

[1,2, 3)] D3 Rekam Medis Informasi Kesehatan, Fakultas Kesehatan, Universitas Nahdlatul Ulama NTB
[4)] S1 Kebidanan, Fakultas Kesehatan Universitas Qamarul Huda Badaruddin Bagu

ABSTRAK

Digitalisasi layanan kesehatan di Indonesia menimbulkan perhatian besar terhadap keamanan data rekam medis elektronik (RME). Kebocoran data pasien dapat berdampak pada kerugian material maupun non-material serta menurunkan kepercayaan publik. Studi pendahuluan di RSUD Patut Patuh Patju Gerung menemukan kendala berupa sistem error, data ganda, diagnosa tidak lengkap, serta Standar Prosedur Operasional (SPO) yang belum diperbarui. Penelitian ini bertujuan meninjau keamanan data RME dengan fokus pada sistem keamanan, kompetensi petugas, dan implementasi SPO. Metode penelitian menggunakan pendekatan deskriptif kualitatif dengan studi kasus pada lima responden (empat petugas rekam medis dan satu petugas IT) melalui wawancara mendalam dan observasi check list. Hasil penelitian menunjukkan bahwa RSUD telah menerapkan autentikasi (username, password, auto-logout), backup harian, serta memiliki petugas kompeten melalui pelatihan. Namun, masih terdapat kendala berupa sistem error, data ganda, dan akses pasca kunjungan yang belum dibatasi. Penelitian ini menyimpulkan bahwa meskipun sistem keamanan sudah diterapkan, evaluasi rutin, pembaruan SPO, serta pelatihan berkelanjutan tetap diperlukan agar keamanan data pasien terjamin sesuai regulasi terbaru. Temuan ini diharapkan menjadi rekomendasi praktis bagi manajemen rumah sakit dalam meningkatkan perlindungan data pasien di era digital.

Kata kunci: Keamanan Data; Rekam Medis Elektronik; Rumah Sakit

ABSTRACT

The digitalization of healthcare services in Indonesia has raised significant concern regarding the security of Electronic Medical Record (EMR) data. Patient data breaches can result in both material and non-material losses, as well as erode public trust. A preliminary study at RSUD Patut Patuh Patju Gerung identified several issues, including system errors, duplicate data, incomplete diagnoses, and Standard Operating Procedures (SOPs) that have not been updated. This study aims to assess EMR data security by focusing on security systems, staff competence, and SOP implementation. The research method employed a descriptive qualitative approach involving a case study of five respondents (four medical record staff and one IT staff) through in-depth interviews and checklist observations. The results indicate that the hospital has implemented authentication measures (usernames, passwords, auto-logout) and daily backups, and possesses competent staff through training. However, obstacles remain, such as system errors, duplicate data, and unrestricted post-visit access. The study concludes that although security systems have been implemented, routine evaluations, SOP updates, and continuous training are still necessary to ensure patient data security in compliance with the latest regulations. These findings are expected to serve as practical recommendations for hospital management to enhance patient data protection in the digital era.

Keywords: *Data Security, Electronic Medical Record, Hospital.*

1. LATAR BELAKANG

Fasilitas pelayanan kesehatan memiliki peran penting dalam meningkatkan derajat kesehatan masyarakat. Rumah sakit, sebagai salah satu fasilitas kesehatan, memiliki fungsi strategis dalam penyediaan pelayanan rawat inap, rawat jalan, serta gawat darurat. Berdasarkan Peraturan Pemerintah Republik Indonesia Nomor 47 Tahun 2016, fasilitas kesehatan merupakan sarana yang menyelenggarakan upaya promotif, preventif,

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

kuratif, dan rehabilitatif yang dilakukan pemerintah maupun masyarakat. Untuk mendukung mutu pelayanan, rumah sakit membutuhkan sistem administrasi kesehatan yang tertib, salah satunya melalui penerapan Rekam Medis Elektronik (RME).

RME adalah dokumen digital yang memuat identitas pasien, hasil pemeriksaan, pengobatan, tindakan, dan pelayanan kesehatan lainnya (Permenkes No. 24 Tahun 2022). Definisi ini sejalan dengan pendapat Handiwidjojo (2015) yang menyatakan bahwa rekam medis elektronik merupakan sistem informasi kesehatan yang dirancang untuk menyimpan data pasien secara digital.

Penggunaan RME diharapkan mampu meningkatkan efisiensi, akurasi pencatatan, serta mengurangi risiko kesalahan pada sistem manual. Namun, implementasinya tidak terlepas dari tantangan, terutama pada aspek keamanan dan kerahasiaan data pasien. Ancaman tidak hanya berasal dari sistem teknologi, tetapi juga dari kelalaian sumber daya manusia sebagai operator. Hal ini sejalan dengan Meilia, Christianto, dan Librianty (2019) yang menyatakan bahwa penggunaan rekam medis elektronik selain memberi manfaat efisiensi juga menimbulkan dilema etik terkait kerahasiaan informasi pasien.

Beberapa kasus kebocoran data kesehatan di Indonesia membuktikan lemahnya perlindungan informasi. Tahun 2021 terjadi kebocoran 279 juta data BPJS Kesehatan yang diperdagangkan secara ilegal, serta 230 ribu data pasien COVID-19 dari aplikasi eHAC. Pada tahun 2022, sebanyak 6 juta data pasien dari server Kementerian Kesehatan terpublikasi, dan pada tahun 2023 terjadi kebocoran 19,5 juta data BPJS Ketenagakerjaan. Rentetan kasus ini menunjukkan bahwa data kesehatan merupakan target utama kejahatan siber, sehingga penerapan keamanan RME menjadi isu strategis (Aviat, 2022). Hal ini juga sejalan dengan Hendriyanto (2021) yang menegaskan bahwa akses ilegal terhadap informasi kesehatan merupakan bentuk pelanggaran hukum yang perlu mendapatkan sanksi tegas. Badan Siber dan Sandi Negara (BSSN, 2022) juga menekankan bahwa lemahnya manajemen keamanan informasi sering kali lebih berbahaya dibanding kelemahan sistem teknologi itu sendiri. Kasus kebocoran 19,5 juta data BPJS Ketenagakerjaan yang diberitakan media nasional (CNN Indonesia, 2023) semakin memperlihatkan urgensi perlindungan data pasien.

Studi pendahuluan di RSUD Patut Patuh Patju Gerung mengungkap beberapa permasalahan, seperti error sistem, data ganda, diagnosa pasien yang tidak lengkap, serta Standar Prosedur Operasional (SPO) yang belum diperbarui. Kondisi ini menimbulkan kerentanan terhadap keamanan data pasien. Oleh karena itu, penelitian ini bertujuan untuk meninjau keamanan RME dengan menitikberatkan pada sistem keamanan, kompetensi petugas, dan implementasi SPO penyimpanan dokumen, sekaligus memberikan masukan praktis bagi manajemen rumah sakit dalam memperkuat kebijakan perlindungan data pasien sesuai regulasi nasional, termasuk UU Perlindungan Data Pribadi Tahun 2022.

2. METODE PENELITIAN

Penelitian ini menggunakan metode deskriptif kualitatif dengan pendekatan studi kasus. Lokasi penelitian adalah Instalasi Rekam Medis RSUD Patut Patuh Patju Gerung, Kabupaten Lombok Barat, pada Juni 2025. Populasi penelitian adalah 34 petugas rekam medis, dengan sampel sebanyak 5 orang (4 petugas rekam medis dan 1 petugas IT) yang dipilih melalui purposive sampling. Kriteria inklusi adalah pengalaman minimal satu tahun menggunakan RME, pernah mengikuti pelatihan, serta terlibat dalam penyimpanan dokumen. Kriteria eksklusi adalah petugas yang sedang cuti atau tidak memiliki akses ke sistem RME. Instrumen penelitian meliputi pedoman wawancara dan check list observasi. Data dikumpulkan melalui wawancara mendalam dan observasi langsung. Analisis data dilakukan dengan analisis kualitatif melalui reduksi, penyajian, dan penarikan kesimpulan sesuai model Miles dan Huberman.

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

3. HASIL DAN PEMBAHASAN

3.1. Sistem Keamanan Rekam Medis Elektronik di RSUD Patut Patuh Patju

RSUD Patut Patuh Patju Gerung telah menerapkan autentikasi personal (username, password), fitur logout otomatis, dan backup harian. Namun, hasil wawancara menunjukkan masih terdapat kendala teknis. Beberapa petugas menyampaikan sering terjadi sistem error yang menghambat proses input data: Beberapa responden juga menekankan adanya data ganda yang harus diperiksa ulang, serta akses data pasien pasca kunjungan yang seharusnya dibatasi tetapi masih dapat dilakukan.

> "*Kami sudah menerapkan autentikasi dengan username dan password untuk pengguna ditambah fitur logout otomatis setelah komputer tidak digunakan selama 30 menit*" (Informan 1).

> "*Kadang sistem mengalami error, jadi kami terlambat input data pasien*." (Informan 2)

> "*Masih ada data ganda di sistem, sehingga harus dicek ulang*." (Informan 3)

> "*Akses data pasien setelah kunjungan masih bisa dibuka, padahal seharusnya dibatasi.*" (Informan 4).

Hasil wawancara menunjukkan proses backup data juga dilakukan secara rutin setiap hari ke server cadangan. Mekanisme backup ini menjadi upaya preventif untuk menjaga ketersediaan data apabila terjadi kerusakan perangkat, gangguan teknis, atau serangan siber. Sistem backup otomatis tersebut membantu rumah sakit mengurangi risiko kehilangan data pasien, sekaligus memastikan kelancaran pelayanan medis.

> "*Backup data dilakukan setiap hari dan disimpan di server cadangan*" (Informan 5).

Selain itu, terdapat pula kendala teknis berupa keterlambatan sinkronisasi data ketika jaringan rumah sakit terganggu. Hal ini berpotensi menghambat kelancaran pelayanan pasien dan menurunkan akurasi rekam medis. Peneliti juga menemukan bahwa pengelolaan akses data riwayat pasien setelah kunjungan selesai masih perlu ditingkatkan. Keterbukaan akses yang tidak sepenuhnya terkendali dapat membuka celah terjadinya kebocoran atau penyalahgunaan informasi medis pasien.

Temuan ini menunjukkan bahwa fondasi keamanan sistem sudah ada, tetapi masih terdapat celah. Mukhtar Harun (2018) menyebutkan bahwa lima prinsip utama keamanan data adalah privacy, integrity, authenticity, availability, dan access control. Pada penelitian ini, aspek availability relatif terjaga karena adanya backup harian, tetapi aspek privacy dan access control masih lemah.

Alexsius et al. (2024) menegaskan bahwa ancaman keamanan informasi dapat berasal dari faktor internal, seperti kelalaian petugas atau salah input, maupun eksternal seperti serangan siber. Hal ini sejalan dengan kondisi di RSUD Patut Patuh Patju Gerung yang masih menghadapi error sistem dan potensi kebocoran data akibat lemahnya pembatasan akses.

Menurut Handiwidjojo (2015), penerapan RME tidak hanya soal teknologi, melainkan juga kesiapan manajemen rumah sakit dalam mengendalikan risiko. Sistem yang tidak di audit secara rutin akan menghasilkan error berulang dan mengurangi kualitas data medis.

Dengan demikian, sistem keamanan RME di RSUD Patut Patuh Patju Gerung sudah berjalan cukup baik melalui penerapan autentikasi, logout otomatis, dan backup harian. Namun, evaluasi lanjutan tetap diperlukan untuk memperkuat sistem, khususnya dalam penanganan gangguan jaringan dan pengaturan hak akses data secara lebih ketat.

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

3.2. Kompetensi Petugas Rekam Medis dalam Mengoperasikan Rekam Medis Elektronik di RSUD Patut Patuh Patju Gerung

Sebagian besar petugas rekam medis memiliki latar belakang pendidikan yang relevan (D3 Rekam Medis) dan telah mengikuti pelatihan dasar penggunaan RME. Namun, hanya sebagian kecil yang pernah mendapatkan pelatihan lanjutan sehingga masih ditemukan kesalahan input maupun diagnosa yang tidak lengkap.

"*Pelatihan rutin tetap diperlukan karena sistem terus berkembang untuk memahami fitur-fitur baru*." (Informan 1)

"*Saat menginput diagnosa pasien, kadang hasilnya tidak lengkap*." (Informan 2)

Pelatihan yang diberikan mencakup pemahaman tentang cara menggunakan aplikasi rekam medis, prosedur input data pasien, hingga aspek menjaga kerahasiaan informasi medis. Dengan adanya pelatihan ini, petugas mampu menjalankan tugas pencatatan data pasien secara elektronik dengan baik dan sesuai ketentuan.

Peneliti juga menemukan bahwa pelatihan yang diberikan masih terbatas pada tahap awal implementasi. Dalam praktiknya, perkembangan teknologi informasi berlangsung cepat, sehingga banyak fitur sistem yang diperbarui secara berkala. Kondisi ini menuntut adanya pelatihan berkelanjutan agar petugas tidak hanya memahami sistem dasar, tetapi juga mampu menyesuaikan diri dengan pembaruan yang ada. Tanpa adanya pelatihan lanjutan, risiko kesalahan input, kelalaian, atau ketidakmampuan memanfaatkan fitur sistem secara optimal dapat terjadi.

Selain itu, faktor kesadaran individu juga memengaruhi kinerja petugas dalam menjaga keamanan data. Meski sudah memiliki kompetensi teknis, keberhasilan implementasi RME sangat bergantung pada kedisiplinan petugas dalam menjaga kerahasiaan akun, tidak membagikan password, serta memastikan prosedur keamanan dipatuhi. Oleh karena itu, selain pelatihan teknis, diperlukan pula pembinaan terkait etika dan tanggung jawab dalam pengelolaan data pasien.

Menurut Technology Acceptance Model (TAM) (Santi & Erdani, 2021), penerimaan teknologi dipengaruhi oleh perceived ease of use dan perceived usefulness. Tanpa pelatihan berkelanjutan, petugas akan kesulitan memahami fitur baru, sehingga kualitas input data menurun. Selain itu, Human Error Theory menjelaskan bahwa kesalahan manusia seperti lupa logout, salah input, atau membagikan password dapat menjadi penyebab kebocoran data (Rusdianan et al., 2024). Oleh karena itu, pelatihan berkelanjutan dan pembinaan kedisiplinan kerja menjadi langkah penting untuk memperkuat kompetensi petugas.

Dengan demikian, dapat disimpulkan bahwa petugas rekam medis di RSUD Patut Patuh Patju Gerung memiliki kemampuan dasar yang baik dalam mengelola RME, tetapi masih membutuhkan peningkatan kapasitas secara berkelanjutan. Upaya pelatihan rutin dan pembinaan disiplin kerja menjadi langkah penting untuk menjaga konsistensi kualitas pengelolaan RME.

3.3. SPO Penyimpanan Rekam Medis Elektronik di RSUD Patut Patuh Patju Gerung

Seluruh responden menyatakan bahwa RSUD telah memiliki SPO terkait penyimpanan RME, termasuk backup, pemulihan data, dan retensi minimal 25 tahun. Namun, beberapa responden menyoroti bahwa pengawasan implementasi masih lemah dan belum ada prosedur teknis pembaruan sistem secara rutin.

"*SPO digunakan sebagai pedoman, tapi pengawasan pelaksanaannya masih kurang*." (Informan 2)

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

> "*Belum ada prosedur teknis yang mengatur pembaruan sistem secara rutin*." (Informan 5).

Hasil observasi juga menunjukkan bahwa SPO tertulis masih bersifat umum dan belum merinci pembagian tugas antar-unit, langkah-langkah teknis menghadapi gangguan sistem, serta mekanisme audit internal untuk mengevaluasi keamanan data.

SPO ini memuat aturan tentang mekanisme penyimpanan data pasien, termasuk proses backup, pemulihan data melalui Disaster Recovery Plan (DRP), serta pengaturan masa retensi rekam medis minimal 25 tahun sebagaimana diatur dalam Permenkes No. 24 Tahun 2022.

Selain itu, SPO yang ada masih jarang dievaluasi dan diperbarui secara berkala. Perkembangan teknologi informasi yang sangat cepat menuntut adanya pembaharuan regulasi internal agar tetap relevan dengan kondisi terkini. Tanpa pembaruan, ada risiko SPO menjadi tidak sesuai dengan kebutuhan, sehingga efektivitasnya dalam menjaga keamanan data dapat berkurang.

RSUD Patut Patuh Patju Gerung telah memiliki SPO yang mengatur backup, pemulihan bencana (DRP), dan retensi minimal 25 tahun sesuai Permenkes No. 24 Tahun 2022. Namun, kelemahan ditemukan pada pengawasan implementasi dan belum adanya pembaruan rutin. Kondisi ini konsisten dengan Asih et al. (2024) yang menyatakan bahwa SPO yang tidak diperbarui hanya menjadi dokumen administratif yang kurang efektif.

Selain itu, aspek hukum juga mempertegas kewajiban menjaga kerahasiaan data pasien. UU No. 29 Tahun 2004 tentang Praktik Kedokteran dan UU No. 36 Tahun 2009 tentang Kesehatan mewajibkan fasilitas kesehatan menjaga rahasia kedokteran. Lebih lanjut, UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi menegaskan bahwa data kesehatan termasuk kategori data pribadi sensitif. Meilia et al. (2019) juga menambahkan bahwa penggunaan RME selain membawa manfaat efisiensi, juga menimbulkan dilema etik terkait kerahasiaan pasien. Dengan demikian, pembaruan SPO yang konsisten dengan regulasi serta pengawasan implementasi menjadi keharusan untuk menjamin perlindungan data pasien.

Hasil penelitian menunjukkan bahwa keamanan RME di RSUD Patut Patuh Patju Gerung dipengaruhi oleh tiga faktor utama: sistem teknologi, kompetensi SDM, dan regulasi internal. Sistem yang baik akan sia-sia tanpa SDM kompeten, begitu pula SPO yang lengkap tidak berguna tanpa implementasi yang konsisten. Sofia et al. (2022) menegaskan bahwa pengelolaan keamanan RME harus melibatkan kombinasi teknologi, regulasi hukum, dan kesiapan pengguna. Penelitian ini mendukung teori tersebut dengan menunjukkan bahwa kelemahan pada salah satu faktor langsung berdampak pada efektivitas keseluruhan sistem.

4. KESIMPULAN

Penelitian ini menyimpulkan bahwa sistem keamanan rekam medis elektronik di RSUD Patut Patuh Patju Gerung sudah memiliki fondasi berupa autentikasi pengguna, auto-logout, dan backup harian, namun masih terdapat kelemahan pada aspek privasi dan kontrol akses karena data pasien tetap bisa diakses setelah kunjungan berakhir. Kompetensi petugas rekam medis cukup baik didukung latar pendidikan dan pelatihan dasar, tetapi masih ditemukan kesalahan input dan diagnosa tidak lengkap akibat kurangnya pelatihan lanjutan dan pengawasan disiplin. Standar Prosedur Operasional (SPO) penyimpanan rekam medis sudah tersedia sesuai regulasi, namun belum diperbarui secara berkala dan belum diawasi implementasinya dengan baik. Dengan demikian, perlindungan data pasien hanya dapat terwujud apabila sistem teknologi diperkuat, kompetensi SDM ditingkatkan, dan

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

SPO dijalankan secara konsisten sesuai regulasi dan perkembangan teknologi. Sehubungan dengan hal tersebut, disarankan agar rumah sakit memperkuat sistem keamanan dengan enkripsi, meningkatkan kemampuan petugas melalui pelatihan berkelanjutan serta pembinaan etika kerja, dan melakukan pembaruan SPO secara konsisten disertai audit internal. Dengan langkah tersebut, perlindungan data pasien akan lebih terjamin dan kepercayaan masyarakat terhadap pelayanan rumah sakit dapat meningkat.

5. UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Universitas Nahdlatul Ulama Nusa Tenggara Barat atas dukungan akademik, serta manajemen dan staf RSUD Patut Patuh Patju Gerung yang telah memberikan izin dan fasilitas penelitian.

DAFTAR PUSTAKA

Asih, H., Indrayadi., & Soraya. (2024). *Evaluasi keamanan data pasien pada rekam medis elektronik dengan systematic literature review*. FIFO, 16(12). [DOI:https://doi.org/10.22441/fifo.2024.v1612.001]

Alexsius, A., Prasetyo, Y., & Sari, M. (2024). *Ancaman keamanan data pada implementasi rekam medis elektronik di rumah sakit*. Jurnal Sistem Informasi Kesehatan, *12*(1), 45–56. http://openjournal.masda.ac.id/index.php/MRHI

Aviat. (2022). *Kebocoran data eHAC dan implikasinya terhadap sistem kesehatan di Indonesia*. Jurnal Keamanan Siber, 4(3), 76–85.

Badan Siber dan Sandi Negara. (2022). *Laporan tahunan keamanan siber nasional 2022*. Badan Siber dan Sandi Negara Republik Indonesia. https://bssn.go.id

CNN Indonesia. (2023). *Kebocoran 19,5 juta data BPJS Ketenagakerjaan di forum hacker*. CNN Indonesia. https://www.cnnindonesia.com

Handiwidjojo, W. (2015). *Rekam medis elektronik*. Jurnal Eksplorasi Karya Sistem Informasi dan Sains, 2(1).

Hendriyanto, K. (2021). *Juridical analysis of illegal information access*. SOEPRA Jurnal Hukum Kesehatan, 7(1), 27–35. [DOI:https://doi.org/10.24167/shk.v7i1.2689]

Kementerian Kesehatan RI. (2016). *Peraturan Pemerintah Republik Indonesia Nomor 47 Tahun 2016 tentang fasilitas pelayanan kesehatan*. https://peraturan.bpk.go.id/Details/5768/pp-no-47-tahun-2016

Meilia, P. D., Christianto, G. M., & Librianty, N. (2019). *Buah simalakama rekam medis elektronik*: *Manfaat versus dilema etik*. Jurnal Etika Kedokteran Indonesia, 3(2).[DOI: https://doi.org/10.26880/jeki.v3i2.37]

Mukhtar, H. (2018). *Prinsip-prinsip keamanan data dalam sistem informasi kesehatan*. Jurnal Informasi Kesehatan, *6*(2), 101–110.

Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. (2022). Kementerian Kesehatan Republik Indonesia. https://yankes.kemkes.go.id/unduhan/fileunduhan_1662611251_882318.pdf

Peraturan Pemerintah Republik Indonesia Nomor 47 Tahun 2016 tentang Fasilitas Pelayanan *Kesehatan*. (2016). Lembaran Negara Republik Indonesia Tahun 2016 Nomor 222. https://peraturan.bpk.go.id/Details/5768/pp-no-47-tahun-2016

Rusdianan, I., Utama, T., Ravi, A., & Sucipto. (2024). *Tinjauan keamanan dan kerahasiaan rekam medis elektronik*. EduRMIK, 3(2). http://openjournal.masda.ac.id/index.php/MRHI/index

Santi, R., & Erdani, Y. (2021). *Technology Acceptance Model dalam penggunaan sistem informasi kesehatan di rumah sakit*. Jurnal Manajemen Informasi Kesehatan Indonesia, *9*(1), 33–42. https://doi.org/10.33560/jmiki.v9i1.487

Sofia, R., Wijaya, A., & Lestari, D. (2022). *Analisis aspek keamanan informasi pasien pada penerapan RME di fasilitas kesehatan*. Jurnal Rekam Medik dan

DOI: 10.37824/jkqh.v13i1.2025
p-ISSN : 2354-9777
e-ISSN : 2614-8420

Informasi Kesehatan, 1(2). [DOI:https://doi.org/10.47134/rammik.v1i1.29]

Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 *tentang Praktik Kedokteran*. (2004). Lembaran Negara Republik Indonesia Tahun 2004 Nomor 116.

Undang-Undang Republik Indonesia Nomor 29 Tahun 2004 *tentang Praktik Kedokteran*. (2004). Lembaran Negara Republik Indonesia Tahun 2004 Nomor 116. https://peraturan.bpk.go.id/Details/43738/uu-no-29-tahun-2004

Undang-Undang Republik Indonesia Nomor 36 Tahun 2009 *tentang Kesehatan*. (2009). Lembaran Negara Republik Indonesia Tahun 2009 Nomor 144. https://peraturan.bpk.go.id/Details/162321/uu-no-36-tahun-2009

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 *tentang Perlindungan Data Pribadi.* (2022). Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196. https://peraturan.bpk.go.id/Details/190241/uu-no-27-tahun-2022