



KEAMANAN DAN PERLINDUNGAN DATA REKAM MEDIS ELEKTRONIK RAWAT JALAN STUDI KASUS DI RUMAH SAKIT NAILI-DBS KOTA PADANG

SECURITY AND PROTECTION OF OUTPATIENT ELECTRONIC MEDICAL RECORDS CASE STUDY AT NAILI-DBS HOSPITAL, PADANG CITY

Syamsul Kamal^{1*}, Reni Riyanti², Penulis Ketiga³

¹Apikes Iris

²Staf Rekam Medis RS Naili

³Mahasiswa Apikes iris

(syamsulkamal@apikesiris.ac.id, 081378239966)

ABSTRAK

Keamanan dan Perlindungan data di rumah sangat perlu dijaga dan diperhatikan secara khusus dan berkesinambungan, agar data yang ada di rumah sakit tetap terjaga dengan baik, tidak hilang tanpa adanya kebocoran data. Keamanan data merupakan hal yang sangat vital dan penting di rumah sakit, dikarenakan berisi informasi sensitif pasien, riwayat penyakit, hingga kondisi kerahasiaan pasien, jika bocor, bisa menimbulkan stigma sosial, diskriminasi kerja, bahkan bisa pemerasan pada orang yang mengambil keuntungan. Dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi data yang dikirim melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak memiliki wewenang. Transformasi digital dalam pelayanan kesehatan menuntut rumah sakit untuk mengadopsi rekam medis elektronik (RME), termasuk pada unit rawat jalan yang memiliki frekuensi kunjungan pasien tinggi. Penggunaan RME membawa manfaat efisiensi dan akurasi, tetapi juga meningkatkan risiko kebocoran dan penyalahgunaan data kesehatan. Penelitian ini menggunakan pendekatan kualitatif deskriptif dimana untuk menganalisis persepsi tenaga rekam medis, tenaga kesehatan dan staf IT terkait keamanan data RME rawat jalan, hambatan yang dihadapi, serta strategi yang diterapkan dalam pengamanan dan perlindungan data rekam medis elektronik khususnya pada rawat jalan. Hasil penelitian menunjukkan bahwa kelemahan utama terdapat pada kontrol akses, kesadaran pengguna, serta kurangnya kebijakan teknis yang rinci di tingkat rumah sakit. Rekomendasi meliputi penguatan regulasi internal, penerapan otentikasi berlapis, serta edukasi berkelanjutan bagi tenaga kesehatan tentang keamanan data.

Kata kunci: Keamanan; Kebocoran; Perlindungan; RME

ABSTRACT

Data security and protection at home require special and continuous attention to ensure the safety and security of hospital data, preventing data loss and data leaks. Data security is vital and crucial in hospitals, as it contains sensitive patient information, including medical history, and patient confidentiality. Leaks can lead to social stigma, job discrimination, and even extortion. Maintaining the confidentiality of information, especially sensitive information that should only be accessed by authorized parties, is crucial. Furthermore, data sent over public networks is particularly vulnerable to unauthorized access and misuse if not secured. The digital transformation of healthcare requires hospitals to adopt electronic medical records (EMR), including in outpatient units with high patient visits. While the use of EMR offers benefits of efficiency and accuracy, it also increases the risk of health data leakage and



misuse. This study used a descriptive qualitative approach to analyze the perceptions of medical records personnel, healthcare professionals, and IT staff regarding the security of outpatient electronic medical records (ERM) data, the obstacles encountered, and the strategies implemented to secure and protect electronic medical records, particularly in outpatient settings. The results indicate that the main weaknesses lie in access control, user awareness, and the lack of detailed technical policies at the hospital level. Recommendations include strengthening internal regulations, implementing layered authentication, and ongoing education for healthcare professionals.

Keywords: Security; Breach; Protection; EMR

PENDAHULUAN

Dalam era digital yang semakin maju dan berkembang, keamanan dan perlindungan data menjadi isu yang sangat krusial saat ini, karena data merupakan aset berharga bagi individu, perusahaan, dan pemerintah. Penggunaan teknologi digital yang semakin luas, seperti cloud computing, Artificial Intelligence (AI), dan Internet. Meningkatnya ketergantungan pada data serta membuka peluang baru bagi pelaku kejahatan siber untuk mengeksploitasi informasi yang sensitif untuk tujuan menguntungkan seseorang atau sekelompok. Sangat penting untuk melindungi data pribadi pasien yang merupakan aset informasi yang berharga di rumah sakit, karena kebocoran informasi atau kebocoran data dalam sistem dapat menyebabkan kerugian finansial dan menurunkan kepercayaan masyarakat terhadap Instansi Rumah Sakit dan Instansi Pemerintahan.

Rekam Medis adalah dokumen yang berisikan data identitas pasien, pemeriksaan, pengobatan, tindakan, dan pelayanan lain yang telah diberikan kepada pasien. Sedangkan Rekam Medis Elektronik adalah Rekam Medis yang dibuat dengan menggunakan sistem elektronik yang diperuntukkan bagi penyelenggaraan Rekam Medis (Pemerintah 2022) Rekam Medis Elektronik harus memenuhi prinsip keamanan data dan informasi meliputi kerahasiaan, integritas,

dan ketersediaan. Prinsip tersebut dipenuhi baik secara individu maupun kelembagaan karena Rekam Medis dapat digunakan sebagai alat bukti hukum yang sah. (Tahun et al. 2023) Kebocoran data yang semakin sering terjadi menunjukkan perlu tindakan yang lebih serius dalam melindungi informasi digital. Ancaman seperti peretasan, pencurian data, dan penyalahgunaan informasi pribadi dapat menimbulkan dampak serius, baik dalam aspek ekonomi maupun privasi. Oleh karena itu, diperlukan strategi keamanan yang kuat dan kepatuhan terhadap regulasi yang berlaku untuk menjaga keutuhan dan kerahasiaan data.

Rumah sakit Naili DBS dalam hal keamanan datanya, dalam survey pendahuluan didapatkan bahwa RS ini dalam penanganan Keamanan data masih jauh dari harapan yang diinginkan, karena data-data pasien yang ada belum ditangani secara profesional, sehingga data-data masih ada yang bocor yang dapat merugikan pasien tersebut. Dengan adanya penelitian ini diharapkan data pasien dapat diakses dan digunakan oleh orang yang berhak menggunakannya.

Dengan meningkatnya kebutuhan akan perlindungan data, berbagai metode keamanan seperti enkripsi, autentikasi berlapis, serta kepatuhan terhadap peraturan seperti UU Perlindungan Data Pribadi menjadi solusi utama dalam menjaga keamanan informasi. Studi ini bertujuan



untuk mengkaji berbagai strategi keamanan dan tantangan yang dihadapi dalam perlindungan data guna memberikan wawasan yang lebih mendalam mengenai pentingnya menjaga data tetap aman. Data kesehatan, terutama rekam medis pasien bersifat sangat rahasia sehingga rentan terhadap kebocoran. Sebagaimana diatur dalam Pasal 29 Permenkes RI Nomor 24 Tahun 2022 yang membahas tentang rekam medis, keamanan dan perlindungan data meliputi kerahasiaan, integritas, dan ketersediaan yang digunakan sebagai peningkatan penggunaan sistem rekam medis elektronik.(Nadilla Putri Melisa, Wahyu Ratri Sukmaningsih, and Rizka Licia 2024). Menurut penelitian Lissa hamama Kerahasiaan Rekam Medis adalah hal penting

yang memastikan pasien mendapatkan jaminan bahwa data pribadi dan detail kesehatan mereka menjadi sebuah rahasia. Dari hasil wawancara didapatkan informasi bahwa, dalam sistem Rekam Medis Elektronik data tersimpan di server sebagai database. Server disimpan pada ruangan khusus yang dijaga dengan kunci pengaman. Rumah sakit belum mempunyai cadangan data (backup system). Untuk menjaga keamanan dan perlindungan data dari aspek pengguna internal maka setiap pengguna (user) yang diberi hak akses akan di buatkan account/password oleh bagian SIMRS(Lissa Hamama, Maiyestati 2022).

Keamanan informasi harus memenuhi beberapa kriteria-kriteria tertentu diantaranya adalah, 1) Memastikan kerahasiaan, integritas, dan ketersediaan semua informasi kesehatan serta melindungi dalam membuat, menerima, mempertahankan, atau mentransmisikan informasi kesehatan; 2) Melindungi dari ancaman dan bahaya yang diantisipasi secara wajar; 3) Melindungi dari

pengguna atau pengungkapan informasi yang diantisipasi secara wajar berdasarkan perturan privasi; 4) Memastikan kepatuhan tenaga kerja (Ardianto and Nurjanah 2024) Tantangan dalam menjaga keamanan data RME beragam. Salah satu isu utamanya adalah besarnya volume dan keragaman data yang dikumpulkan. Dalam mengumpulkan informasi dari berbagai sumber, termasuk formulir daring, survei, catatan administratif, dan basis data eksternal(Ikawati and Ansyori 2024)

Dari permasalahan diatas maka penulis ingin meneliti terkait keamanan dan perlindungan data dengan konsep pentingnya sistem keamanan data dalam perlindungan Data Rumah Sakit . Penelitian ini bertujuan untuk Menganalisis konsep keamanan dan perlindungan data dalam era Mengidentifikasi ancaman utama yang dapat membahayakan keamanan data, terutama data yang ada di rumah sakit. Mengeksplorasi strategi yang dapat diterapkan untuk meningkatkan keamanan dan perlindungan data, Mengkaji peran regulasi dalam mendukung keamanan data serta menilai efektivitasnya dalam melindungi informasi pengguna. Berdasarkan latar belakang ini, pentingnya fasilitas kesehatan dalam menjaga keamanan data pasien dalam pelaksanaan rekam medis elektronik, serta dampak yang ditimbulkan jika informasi bocor dan beresiko disalahgunakan oleh pihak yang tidak bertanggung jawab dan digunakan oleh kepentingan pribadi atau golongan(Suhariyono, Rusdian Ikawati, and Afifah 2025)

BAHAN DAN METODE

Penelitian ini telah dilaksanakan pada bulan Juni sampai dengan Juli 2025 di RS

Naili DBS Kota Padang, yang ditemani oleh 2 anggota peneliti, dan dilanjutkan dengan pengolahan data di Akademi Perekam dan Informasi Kesehatan IRIS Kota Padang untuk mendapatkan informasi yang valid terkait keamanan dan perlindungan data.

Metode pengumpulan data yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif, dimana metode ini merupakan pendekatan yang menggambarkan, memaparkan, dan mendeskripsikan fenomena atau situasi yang ada secara mendalam dan rinci terkait variabel-variabel yang telah ditetapkan, yang ada di rumah sakit tersebut. Disini penulis juga melakukan wawancara yang mendalam dengan staf rumah sakit terkait keamanan dan perlindungan data dan juga melihat secara langsung keamanan data yang ada di rumah sakit tersebut. terkait komponen ini untuk mendukung tujuan penelitian. Disamping itu penulis juga melakukan

observasi langsung ke objek penelitian dan juga dilakukan telaah dokumen untuk mendapatkan hasil yang maksimal.

Adapun subjek penelitian penulis melakukan wawancara mendalam adalah, 1 orang kepala rekam medis, 1 orang kepala IT, 1 orang kepala Casemix, 1 orang kepala perawat dan satu orang staf rawat jalan. Objek penelitian ini adalah kuesioner dan wawancara dari ka RM, Kepala IT, kepala Casemix, kepala rawat jalan dan Staf rawat jalan.

Untuk Kriteria-kriteria yang diambil dalam penelitian ini adalah kebijakan rumah sakit terkait keamanan dan perlindungan data yaitu belum optimalnya keamanan dan perlindungan data, dan sistem belum dilengkapi *intrusion detection system* (IDS) dan *disaster recovery plan* yang memadai, sehingga masih rentan terhadap serangan siber dan virus

HASIL PENELITIAN

a. Hasil Observasi

Berdasarkan hasil observasi yang peneliti lakukan terkait analisis keamanan dan perlindungan data RME Pasien rawat jalan didapatkan hasil sebagai berikut :

Tabel 1 Hasil observasi RME di RS Naili DBS

No	Variabel yang diamati	Ada	Tidak
1	Jaringan Wireles		✓
2	Jaringan kabel	✓	
3	User /pengguna	✓	
4	Id dan password	✓	

b. Hasil wawancara

Hasil wawancara penulis dengan informan staf rumah sakit terkait penelitian yang dilakukan di ruangan rekam medis, ruangan IT dan ruangan perawat didapatkan beberapa karakteristik informan sebagai berikut :

Tabel 2 Karakteristik informan

No	Informan	Pendidikan	Jenis kelamin	Umur	Jabatan
1	Informan 1	D4	Perempuan	31	Kepala RM
2	Informan 2	S1	Laki-laki	38	Kepala IT
3	Informan 3	S1 Kedokteran	Perempuan	42	Kepala Casemix
4	Informan 4	S1	Perempuan	35	Kepala Rajal
5	Informan 5	D3	Perempuan	30	Staf Rajal

Kepala Rekam Medis(KRM)

P: Bagaimana kebijakan rumah sakit terkait keamanan rekam medis elektronik di rawat jalan?

Krm): Secara kebijakan, setiap tenaga kesehatan memiliki akun pribadi. Namun dalam praktik, saya tahu masih ada staf yang berbagi password karena alasan kecepatan. Ini menjadi tantangan kami dalam implementasi.

P: Apakah ada audit rutin terkait keamanan data?

Krm : Audit dilakukan setahun sekali, tetapi lebih banyak ke aspek administrasi, belum mendalam sampai ke akses user harian.

Kepala Casemix (KC)

P: Apakah ada kendala keamanan saat mengelola data klaim pasien BPJS?

KC : Data klaim dikirim melalui aplikasi bridging. Kendala yang ada biasanya pada keamanan jaringan, kalau internet tidak stabil bisa ada risiko data tidak terkirim sempurna.

P: Apakah ada potensi kebocoran data di bagian ini?

KC: Ada, terutama kalau file klaim diekspor ke Excel dan disimpan di komputer pribadi. Itu rawan kalau tidak terproteksi.

Dokter Rawat Jalan (DRJ)

P: Bagaimana pengalaman dokter dalam menggunakan RME?

DRJ RME membantu mempercepat pencatatan, tapi kadang sistem lambat.

Untuk login, saya hanya pakai username-password, belum ada keamanan tambahan.

P: Apakah menurut dokter ada risiko kebocoran data pasien?

DRJ: Ya, apalagi kalau komputer di ruang praktik tidak dikunci saat ditinggal. Bisa saja orang lain mengakses.

Staf Rawat Jalan (SRJ)

P: Bagaimana pengalaman Ibu saat menggunakan sistem rekam medis elektronik (RME) di unit rawat jalan?

SRJ: Menurut saya, sistem ini memang mempermudah pencatatan pasien. Tapi kadang login terasa merepotkan kalau harus cepat, sehingga beberapa teman memakai akun yang sama biar lebih praktis.

P: Apakah Ibu pernah mendapat sosialisasi atau pelatihan terkait keamanan data pasien?

SRJ: Pernah, tapi hanya sekali waktu awal ada sistem ini. Setelah itu jarang ada pelatihan lagi. Jadi sebagian besar kami belajar sendiri atau bertanya pada staf IT.

P: Bagaimana menurut Ibu tentang risiko kebocoran data pasien?

SRJ: Sejujurnya saya agak khawatir, apalagi kalau ada pasien publik figur. Kalau password bisa dipakai banyak orang, tentu risiko kebocoran lebih besar.

P: Menurut Ibu, apa yang bisa dilakukan agar data pasien lebih aman dari kebocoran?



SRJ Kalau login pakai sidik jari atau kartu ID pribadi lebih bagus. Jadi tidak bisa dipakai bergantian dengan lainnya

Kepala IT (KIT)

P: Bagaimana sistem keamanan data RME rawat jalan yang ada sekarang?

KIT : Sistem menggunakan username dan password. Data di-backup tiap malam, tetapi belum semua data terenkripsi.

PEMBAHASAN

Hasil wawancara dengan Kepala dan staf rekam medis

"Berdasarkan hasil wawancara dengan perawat dan staf IT, ditemukan adanya praktik penggunaan akun bersama pada sistem RME rawat jalan. Namun, dokumen kebijakan rumah sakit yang diperoleh peneliti tidak menjelaskan secara rinci mengenai mekanisme kontrol akses. Ketidakjelasan dokumen internal ini mengindikasikan lemahnya regulasi teknis di tingkat rumah sakit. Untuk itu, analisis selanjutnya menggunakan acuan Permenkes No. 24 Tahun 2022 sebagai standar nasional."

Hasil wawancara menunjukkan bahwa upaya keamanan dan perlindungan data Rekam Medis Elektronik (RME) di rumah sakit belum optimal. Dari sisi kebijakan, kepala rekam medis menyebutkan bahwa aturan akses data sudah ditetapkan, namun implementasi di lapangan masih lemah karena sebagian pegawai menggunakan akun bersama.

Dari sisi tenaga medis, dokter menilai RME sangat membantu pelayanan, tetapi masih ada kekhawatiran data pasien dapat diakses pihak yang tidak berwenang. Perawat mengakui penggunaan akun kolektif untuk

P: Apa kendala terbesar menurut Anda?

KIT: Kendala utamanya disiplin pengguna. Banyak staf yang sharing password. Kami sudah sediakan akun individu, tapi praktik di lapangan berbeda

efisiensi, meskipun sadar hal tersebut berisiko terhadap keamanan data.

Pada bagian sistem informasi dan teknologi, staf IT menjelaskan bahwa sistem RME sudah memiliki perlindungan dasar seperti firewall, antivirus, dan backup data berkala. Namun, sistem belum dilengkapi *intrusion detection system* (IDS) dan *disaster recovery plan* yang memadai, sehingga masih rentan terhadap serangan siber.

Dari sisi **pengelolaan data casemix**, informan menyebutkan bahwa data yang diolah untuk kepentingan klaim juga belum sepenuhnya terlindungi. Proses pertukaran data dengan pihak ketiga sering dilakukan tanpa enkripsi khusus, sehingga menimbulkan risiko kebocoran informasi.

Secara keseluruhan, analisis kualitatif menunjukkan empat faktor utama yang memengaruhi keamanan data RME: **(1) manusia** – kesadaran dan perilaku pengguna masih lemah, **(2) teknologi** – perlindungan dasar ada tetapi belum komprehensif, **(3) kebijakan** – aturan ada namun implementasi tidak konsisten, dan **(4) tata kelola data (termasuk casemix)** – pertukaran data belum dilindungi dengan standar keamanan yang kuat.

Triangulasi Data

Untuk menjaga keabsahan data, dilakukan triangulasi antar-informan. Dari wawancara



dengan kepala rekam medis dan dokter, keduanya sama-sama menekankan pentingnya pembatasan akses, meskipun kepala rekam medis lebih menyoroti masalah kebijakan dan disiplin, sedangkan dokter menekankan aspek kerahasiaan pasien.

Perawat dan kepala rekam medis memberikan informasi yang sejalan mengenai penggunaan akun bersama, yang memperlihatkan adanya kelemahan dari sisi perilaku pengguna.

Sementara itu, staf IT menegaskan bahwa secara teknis sistem memiliki perlindungan dasar, tetapi belum lengkap. Hal ini sesuai dengan kekhawatiran dokter terkait potensi akses oleh pihak yang tidak berwenang.

Dari sisi casemix, kelemahan dalam pengelolaan data klaim memperkuat temuan bahwa perlindungan data belum menyeluruh. Hal ini konsisten dengan penjelasan staf IT bahwa pertukaran data eksternal belum dilindungi enkripsi.

Dengan demikian, triangulasi antar-informan menunjukkan bahwa masalah keamanan RME terjadi secara konsisten pada empat aspek: manusia, teknologi, kebijakan, dan tata kelola data (casemix).

Kesimpulan

Berdasarkan hasil penelitian mengenai keamanan dan perlindungan data rekam medis rawat jalan, dapat disimpulkan bahwa: kebijakan keamanan data telah tersedia, namun implementasinya belum berjalan optimal. Praktik penggunaan akun bersama, password sharing, dan komputer yang tidak terkunci, serta pintu masuk ke komputer server belum memakai kode keamanan, menunjukkan lemahnya disiplin dalam penerapan kebijakan, selanjutnya pada pelatihan keamanan data tidak berkelanjutan, sehingga tingkat kesadaran staf dalam

menjaga kerahasiaan data masih rendah, Sosialisasi terakhir bahkan tercatat lebih dari dua tahun lalu untuk teknologi keamanan masih terbatas, dengan penggunaan username-password standar, backup harian tanpa enkripsi penuh, serta belum adanya mekanisme multi-factor authentication (MFA) dan audit trail yang detail, resiko kebocoran data teridentifikasi nyata, terutama dalam proses ekspor file klaim, penggunaan komputer bersama, serta lemahnya kontrol akses pengguna, selanjutnya, hasil triangulasi metode (wawancara, observasi, dan dokumen) menegaskan adanya kesenjangan antara kebijakan tertulis dan praktik lapangan, sehingga perlindungan data rekam medis rawat jalan masih belum mencapai standar optimal.

Saran

Rumah sakit perlu memperbarui dan menegaskan SOP keamanan data, termasuk pemberian sanksi yang jelas terhadap pelanggaran seperti penggunaan akun bersama atau ketidakdisiplinan dalam logout, selanjutnya, Pelatihan keamanan data perlu dilakukan secara berkala dan menyeluruh, melibatkan seluruh tenaga kesehatan dan staf pendukung. Edukasi harus menekankan pentingnya kerahasiaan, integritas, dan ketersediaan data pasien.berikutnya dala, pengembangan Teknologi Keamanan Rumah sakit perlu menerapkan sistem keamanan modern, seperti MFA, enkripsi data, audit trail, serta pengamanan tambahan pada sistem bridging klaim BPJS, untuk monitoring dan Evaluasi Rutin Audit keamanan harus dilakukan lebih sering, minimal setiap enam bulan, dengan melibatkan tim khusus yang berfokus pada keamanan data rekam medis, berikutnya untuk, Kepala rekam medis, staf IT, dokter,



perawat, dan staf casemix harus dilibatkan secara aktif dalam perumusan, pelaksanaan, serta pengawasan kebijakan keamanan, agar tercipta rasa memiliki dan tanggung jawab bersama terhadap perlindungan data pasien di rumah sakit ini.

DAFTAR PUSTAKA

- Ardianto, Efri Tri, and Lensa Nurjanah. 2024. "Analisis Aspek Keamanan Data Pasien Dalam Implementasi Rekam Medis Elektronik Di Rumah Sakit X." ... *Rekam Medik & Manajemen* ... 3(2):18–30.
- Fauzil, Fauzil, Yusirwan Yusuf, and Adila Kasni Astiena. 2022. "ANALISIS KEPATUHAN DPJP DALAM KELENGKAPAN PENGISIAN REKAM MEDIS DAN FAKTOR-FAKTOR YANG MEMPENGARUHINYA DI RSUD Dr RASIDIN PADANG." *Human Care Journal* 7(2):359. doi: 10.32883/hcj.v7i2.1665.
- Ikawati, Fita Rusdian, and Anis Ansyori. 2024. "A Systematic Review Of RME Data Privacy And Security." 6:107–13.
- Lissa Hamama, Maiyestati, Zarfinal. 2022. "TENTANG REKAM MEDIS DI RSUP M . DJAMIL PADANG Keamanan Dan Perlindungan Data Rekam Medis Elektronik Meliputi : Kerahasiaan , Integritas,ketersediaan." *Jurnal Ilmu Hukum*.
- Nadilla Putri Melisa, Wahyu Ratri Sukmaningsih, and Rizka Licia. 2024. "ANALISIS REKAM MEDIS ELEKTRONIK RAWAT JALAN PADA ASPEK KEAMANAN DATA PASIEN DI RUMAH SAKIT UMUM DAERAH Dr. SOEDIRAN MANGUN SUMARSO WONOGIRI." *Journal Health Information Management Indonesian (JHIMI)* 3(3):160–68. doi: 10.46808/jhimi.v3i3.193.
- Pemerintah, Peraturan. 2022. "Permenkes No 24 Tahun 2022." *PERATURAN MENTERI KESEHATAN REPUBLIK INDONESIA NOMOR 24 TAHUN 2022 TENTANG REKAM MEDIS* (8.5.2017):2003–5.
- Suhariyono, Untung Slamet, Fita Rusdian Ikawati, and Nur Afifah. 2025. "Analisis Aspek Keamanan Informasi Data Pasien Pada Rekam Medis Elektronik Di UPT Puskesmas Karangploso." *Jurnal Manajemen Informasi Kesehatan Indonesia* 13(1):2337–2585.
- Tahun, Nomor, Tentang Rekam, Keamanan Dan, Perlindungan Data, Rekam Medis Elektronik, D. I. Rsup, and M.Djamil Padang. 2023. "(Keamanan Dan Perlindungan Data '."