

DOI: <https://doi.org/10.38035/jemsi.v8i1.10008><https://creativecommons.org/licenses/by/4.0/>

Received: 09 Oktober 2026 | Revised: 12 Oktober 2026 | Accepted: 23 Oktober 2026

Rancangan Pengembangan Keamanan Rekam Medis Pada Hospital Information System (HIS) Di Rumah Sakit Awal Bros

Feronica Dewi Pratiwi¹, Sali Setiatin², Candra Mecca Sufyana³

¹Manajemen Informasi Kesehatan, Politeknik Piksi Ganseha Bandung, Indonesia, lppm.piksi.ganeshha.bandung@gmail.com

²Manajemen Informasi Kesehatan, Politeknik Piksi Ganseha Bandung, Indonesia, salisetiatin@gmail.com

³Manajemen Informasi Kesehatan, Politeknik Piksi Ganseha Bandung, Indonesia, candra.mecca@piksi.ac.id

Corresponding Author: candra86mecca@gmail.com³

Abstract: *The development of Hospital Information Systems (HIS) improves the efficiency of medical record management but also increases the need to protect confidential health information. Security systems that still rely on basic authentication, access control, and user discipline require strengthening through more integrated security mechanisms. This study aimed to analyze security requirements and develop a prototype design for medical record security in HIS through the integration of authentication mechanisms, access control, session security, activity logging, and security monitoring. The study employed a Research and Development (R&D) method using the Waterfall model, which comprised requirements analysis, system design, prototype development, and testing. Data were collected through observation, document analysis, and system requirements analysis based on six security aspects: confidentiality, integrity, authentication, availability, access control. The prototype was developed as a MedSecure Hospital website and tested using black-box testing on authentication, access management, MFA & Session, Audit Trail, Security Monitoring, system administration, and logout functions. The results showed that the main functions of the prototype operated according to the design. The study concludes that MedSecure Hospital can serve as an initial model for developing integrated and layered medical record security. These findings provide a basis for further development and integration of HIS security systems in hospital operational environments.*

Keyword: *Hospital Information System, Medical Record Security, MedSecure Hospital, Waterfall, Black-Box Testing.*

Abstrak: Perkembangan *Hospital Information System* (HIS) meningkatkan efisiensi pengelolaan rekam medis, tetapi juga meningkatkan kebutuhan terhadap perlindungan informasi kesehatan yang bersifat rahasia. Sistem keamanan yang masih bergantung pada autentikasi dasar, pengendalian akses, dan kedisiplinan pengguna memerlukan penguatan melalui mekanisme keamanan yang lebih terintegrasi. Penelitian ini bertujuan menganalisis kebutuhan keamanan dan mengembangkan rancangan prototipe keamanan rekam medis pada HIS melalui integrasi mekanisme autentikasi, pengendalian akses, keamanan sesi, pencatatan

aktivitas, dan pemantauan keamanan. Penelitian menggunakan metode *Research and Development* (R&D) dengan model *Waterfall* yang meliputi analisis kebutuhan, perancangan, pengembangan prototipe, dan pengujian. Data dikumpulkan melalui observasi, studi dokumentasi, dan analisis kebutuhan sistem dengan mengacu pada enam aspek keamanan, yaitu *confidentiality*, *integrity*, *authentication*, *availability*, *access control*. Prototipe dikembangkan dalam bentuk *website MedSecure Hospital* dan diuji menggunakan metode *black-box testing* terhadap fungsi autentikasi, pengelolaan akses, *MFA & Sesi*, *Jejak Audit*, *Monitoring Keamanan*, administrasi sistem, dan *logout*. Hasil pengujian menunjukkan bahwa fungsi utama prototipe berjalan sesuai dengan rancangan. Penelitian menyimpulkan bahwa *MedSecure Hospital* dapat menjadi model awal pengembangan keamanan rekam medis yang terintegrasi dan berlapis. Hasil ini berimplikasi sebagai dasar pengembangan dan integrasi sistem keamanan HIS pada lingkungan operasional rumah sakit.

Kata Kunci: *Hospital Information System*, Keamanan Rekam Medis, *Medsecure Hospital*, *Waterfall*, *Black-Box Testing*.

PENDAHULUAN

Perkembangan teknologi informasi dalam pelayanan kesehatan telah mendorong perubahan pengelolaan rekam medis dari sistem manual menuju Rekam Medis Elektronik (RME) (Isnaeni & Widiyanto, 2025; Patilima et al., 2026). Penerapan RME bertujuan untuk meningkatkan efisiensi pelayanan, keakuratan data, kemudahan akses informasi pasien, serta integrasi pelayanan antarunit (Puspita & Wisnuwardhana, 2026). Penggunaan sistem elektronik memungkinkan pengelolaan data rekam medis menjadi lebih cepat dan terstruktur dibandingkan dengan sistem konvensional (Budiman et al., 2025). Hospital Information System (HIS) menjadi salah satu sistem yang mendukung integrasi pengelolaan informasi rumah sakit, termasuk data rekam medis pasien (Hilmy et al., 2026). Perubahan tersebut memberikan manfaat dalam pengelolaan informasi kesehatan, tetapi sekaligus meningkatkan kebutuhan terhadap sistem keamanan yang mampu melindungi data pasien (Arapa, 2026; Rangkuti et al., 2026).

Rekam medis mengandung informasi yang bersifat rahasia, meliputi identitas pasien, riwayat penyakit, hasil pemeriksaan, diagnosis, serta tindakan medis (Santoso et al., 2025; Sari et al., 2022). Perlindungan terhadap informasi tersebut diperlukan untuk mencegah kebocoran data, penyalahgunaan akses, maupun penggunaan data tanpa kewenangan yang dapat menimbulkan dampak etika, hukum, dan kepercayaan pasien terhadap rumah sakit (Fauziah et al., 2026; Indra et al., 2024). Rekam medis harus dijaga kerahasiaannya dan hanya dapat diakses oleh pihak yang berwenang sesuai dengan ketentuan yang berlaku sebagaimana diatur dalam Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis. Keamanan HIS mencakup enam aspek utama, yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), autentikasi (*authentication*), ketersediaan (*availability*), kontrol akses (*access control*), dan nir-sangkal (*non-repudiation*) (Rosalinda et al., 2021). Dalam penerapannya, keamanan sistem masih dapat menghadapi permasalahan seperti penggunaan username dan password yang tidak diperbarui secara berkala serta belum memadainya Standard Operating Procedure (SOP) terkait keamanan data (Nugroho et al., 2023).

Permasalahan keamanan rekam medis tidak hanya berkaitan dengan teknologi, tetapi juga dengan perilaku pengguna dalam menjalankan prosedur keamanan HIS. Kelalaian petugas dalam menjaga kerahasiaan akses, penggunaan akun bersama, serta perbedaan pemahaman tenaga kesehatan mengenai perlindungan data pasien masih menjadi permasalahan dalam penerapan RME (Pramesti et al., 2024). Studi di Klinik Mata Dr. Hasri Ainun Habibie menunjukkan bahwa dokter penanggung jawab membutuhkan waktu adaptasi dalam menggunakan sistem RME dan alur pelayanan perlu disesuaikan secara bertahap dengan sistem

yang diterapkan (Yunengsih & Oktaviani, 2024). Keamanan data medis juga berhubungan langsung dengan perlindungan privasi pasien yang merupakan bagian penting dalam penyelenggaraan pelayanan kesehatan (Sofia et al., 2022). Kesenjangan antara kebutuhan keamanan HIS yang seharusnya mampu melindungi rekam medis secara menyeluruh dengan kondisi penerapan pada aspek teknis, prosedural, dan pengguna menunjukkan perlunya pengembangan sistem keamanan yang lebih sesuai dengan kebutuhan operasional rumah sakit.

Penelitian terdahulu telah membahas keamanan rekam medis elektronik melalui berbagai aspek, termasuk kerahasiaan, integritas, autentikasi, ketersediaan, kontrol akses, dan nir sangkal serta mengidentifikasi permasalahan pengelolaan kredensial dan SOP keamanan data (Nugroho et al., 2023). Penelitian lainnya menunjukkan bahwa kesadaran dan perilaku sumber daya manusia menjadi bagian penting dalam menjaga keamanan data pasien (Pramesti et al., 2024) sedangkan perlindungan privasi menjadi aspek yang tidak dapat dipisahkan dari pengelolaan data medis (Sofia et al., 2022). Kajian tersebut menunjukkan bahwa keamanan rekam medis perlu dipandang sebagai kesatuan antara mekanisme teknis sistem, prosedur pengelolaan, dan perilaku pengguna. Penelitian ini mengembangkan sistem keamanan rekam medis melalui perancangan dan pengembangan prototipe yang mengintegrasikan kebutuhan perlindungan data, pengelolaan akses, dan mekanisme keamanan dalam HIS. Pengembangan tersebut diarahkan untuk menghasilkan prototipe sistem keamanan yang dapat digunakan sebagai dasar penguatan pengelolaan rekam medis elektronik di Rumah Sakit Awal Bros Batam.

Penelitian ini bertujuan untuk mengembangkan sistem keamanan rekam medis pada Hospital Information System (HIS) di Rumah Sakit Awal Bros Batam. Pengembangan dilakukan dengan mengidentifikasi kebutuhan keamanan dan kesenjangan penerapan keamanan rekam medis pada aspek teknis, prosedural, dan pengguna. Hasil identifikasi tersebut digunakan sebagai dasar dalam merancang dan mengembangkan prototipe sistem keamanan rekam medis yang sesuai dengan kebutuhan pengelolaan HIS. Prototipe yang dikembangkan selanjutnya digunakan untuk menunjukkan penerapan mekanisme keamanan dalam pengelolaan data dan akses rekam medis. Hasil penelitian diharapkan dapat menghasilkan prototipe dan rekomendasi pengembangan yang mendukung peningkatan perlindungan data pasien serta penguatan keamanan pengelolaan rekam medis elektronik di rumah sakit.

METODE

Metode penelitian berisi jenis penelitian, objek penelitian, populasi, Sampel, waktu dan tempat penelitian, instrumen, alat analisis, serta hal-hal lain yang berkaitan dengan cara penelitian. Bagian ini dapat dibagi menjadi beberapa paragraf atau sub bab, tetapi tidak perlu mencantumkan penomoran.

Penelitian ini menggunakan metode Research and Development (R&D) yang bertujuan menghasilkan suatu produk berupa rancangan dan prototipe pengembangan keamanan rekam medis pada Hospital Information System (HIS) di Rumah Sakit Awal Bros Batam. Produk yang dihasilkan dalam penelitian ini berupa prototipe aplikasi berbasis web yang diberi nama MedSecure Hospital. Prototipe tersebut digunakan untuk merepresentasikan mekanisme keamanan yang dirancang berdasarkan kebutuhan keamanan rekam medis pada HIS. Penelitian ini tidak sampai pada tahap implementasi prototipe ke dalam HIS operasional Rumah Sakit Awal Bros Batam.

Dalam pelaksanaan R&D, model pengembangan perangkat lunak yang digunakan adalah Waterfall. Waterfall digunakan sebagai model pengembangan karena tahapan penelitian dilakukan secara berurutan, mulai dari analisis kebutuhan, perancangan sistem, pengembangan prototipe, hingga pengujian. Setiap tahapan menghasilkan keluaran yang menjadi dasar bagi tahapan berikutnya, sehingga alur pengembangan dapat ditelusuri secara sistematis. Tahapan

Waterfall dalam penelitian ini terdiri atas analisis kebutuhan, perancangan sistem, pengembangan prototipe, dan pengujian.

Penelitian dilakukan pada konteks pengelolaan keamanan rekam medis pada HIS di Rumah Sakit Awal Bros Batam pada tahun 2026. Subjek penelitian adalah sistem keamanan dan kebutuhan pengelolaan rekam medis pada HIS, sedangkan objek penelitian adalah rancangan pengembangan keamanan rekam medis yang diwujudkan dalam bentuk prototipe MedSecure Hospital. Pengembangan rancangan mengacu pada enam aspek keamanan informasi, yaitu confidentiality, integrity, authentication, availability, access control, dan non-repudiation. Keenam aspek tersebut digunakan sebagai dasar dalam mengidentifikasi kebutuhan keamanan dan menentukan fitur yang dikembangkan pada prototipe.

A. Tahapan Penelitian

Pelaksanaan penelitian dilakukan mengikuti tahapan R&D dengan model Waterfall sebagai berikut.

1. Analisis Kebutuhan (Requirements Analysis)

Tahap pertama dilakukan untuk mengidentifikasi kondisi keamanan rekam medis pada HIS yang sedang berjalan serta menentukan kebutuhan pengembangan sistem. Pengumpulan informasi dilakukan melalui observasi dan studi dokumentasi. Observasi digunakan untuk memperoleh gambaran mengenai tampilan, alur akses, modul, serta mekanisme keamanan yang terdapat pada HIS. Studi dokumentasi digunakan untuk memperoleh informasi mengenai alur pengelolaan rekam medis, ketentuan keamanan, dan kebutuhan perlindungan data rekam medis. Hasil observasi dan studi dokumentasi selanjutnya dianalisis berdasarkan enam aspek keamanan, yaitu confidentiality, integrity, authentication, availability, access control, dan non-repudiation. Analisis dilakukan dengan membandingkan kondisi keamanan yang tersedia pada sistem dengan kebutuhan penguatan keamanan. Tahap ini menghasilkan daftar kebutuhan fungsional keamanan yang menjadi dasar dalam perancangan prototipe. Kebutuhan yang teridentifikasi antara lain penguatan autentikasi melalui MFA, pengelolaan sesi dan auto-logout, pengelolaan hak akses berdasarkan peran, pencatatan aktivitas melalui audit trail, monitoring keamanan, pengelolaan pengguna, pencadangan database, serta pengaturan sistem.

2. Perancangan Sistem (System Design)

Berdasarkan kebutuhan yang telah diperoleh pada tahap analisis, dilakukan perancangan sistem keamanan MedSecure Hospital. Tahap ini menghasilkan rancangan struktur sistem, alur proses, struktur menu, hak akses pengguna, rancangan antarmuka, serta mekanisme keamanan yang akan diterapkan pada prototipe. Perancangan alur data digambarkan menggunakan Data Flow Diagram (DFD) untuk menunjukkan hubungan antara pengguna, administrator, proses sistem, dan penyimpanan data. DFD Level 0 digunakan untuk menggambarkan sistem secara umum, sedangkan DFD Level 1 digunakan untuk menguraikan proses utama menjadi autentikasi dan sesi, pengelolaan hak akses, pelayanan rekam medis, jejak audit dan monitoring, serta administrasi sistem. Selain DFD, rancangan sistem juga direpresentasikan melalui rancangan alur penggunaan sistem dan komponen fungsional yang terdapat pada prototipe. Fitur keamanan yang dirancang meliputi Permintaan Akses, Hak Akses Otomatis, MFA & Sesi, Jejak Audit, dan Monitoring Keamanan. Sementara itu, fitur administrasi sistem meliputi Data Pengguna, Laporan, Backup Database, dan Pengaturan Sistem.

3. Pengembangan Prototipe (Prototype Development)

Tahap pengembangan merupakan proses menerjemahkan hasil analisis kebutuhan dan rancangan sistem menjadi prototipe berbasis web yang diberi nama MedSecure Hospital. Pengembangan dilakukan berdasarkan rancangan yang telah ditetapkan pada tahap sebelumnya. Prototipe dikembangkan dengan mengintegrasikan fungsi pelayanan rumah sakit dan mekanisme keamanan. Modul pelayanan yang direpresentasikan

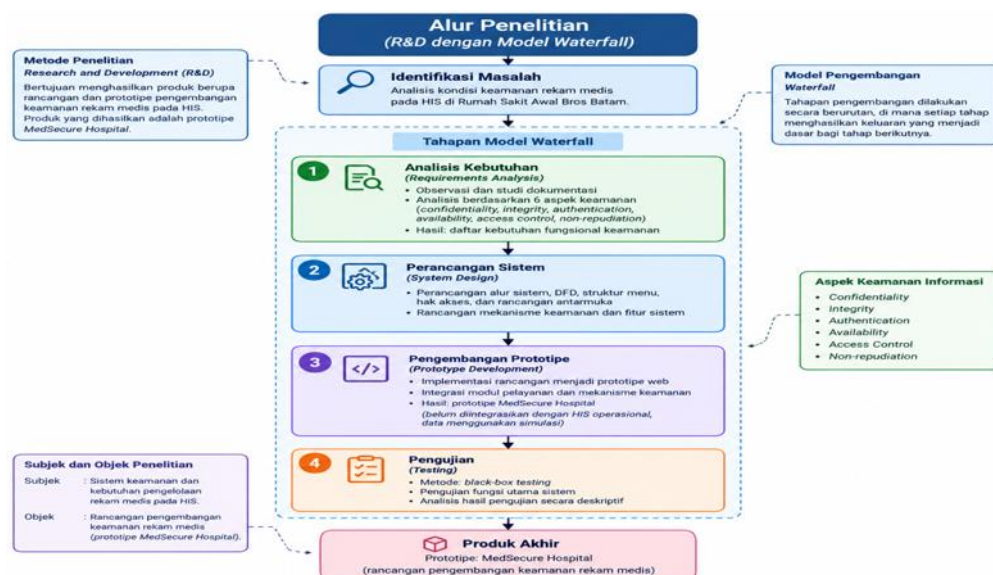
meliputi Pendaftaran, Kasir, Dokter, Perawat, Rekam Medis, Apoteker, dan Direktur. Mekanisme keamanan meliputi autentikasi pengguna, pengelolaan hak akses, MFA dan sesi, audit trail, monitoring keamanan, serta fungsi administrasi sistem. Pada tahap ini, rancangan DFD, alur sistem, struktur menu, dan kebutuhan keamanan diterjemahkan menjadi tampilan serta fungsi pada prototipe. Setiap fungsi dikembangkan sesuai kebutuhan yang telah ditetapkan pada tahap analisis sehingga terdapat keterkaitan antara kebutuhan, rancangan, dan produk prototipe. Prototipe yang dihasilkan merupakan representasi rancangan pengembangan keamanan dan belum diintegrasikan dengan HIS yang digunakan dalam operasional Rumah Sakit Awal Bros Batam. Data yang digunakan dalam prototipe bersifat simulasi dan tidak menggunakan data pasien sebenarnya.

4. Pengujian (Testing)

Tahap terakhir dilakukan untuk mengetahui kesesuaian fungsi prototipe dengan kebutuhan dan rancangan yang telah ditentukan. Pengujian menggunakan metode black-box testing, yaitu pengujian berdasarkan masukan dan keluaran fungsi tanpa melakukan pemeriksaan terhadap kode program secara langsung. Pengujian dilakukan terhadap fungsi utama prototipe, meliputi login, dashboard, Permintaan Akses, Hak Akses Otomatis, MFA & Sesi, Jejak Audit, Monitoring Keamanan, Data Pengguna, Laporan, Backup Database, Pengaturan Sistem, akses modul pelayanan rumah sakit, dan logout. Setiap fungsi diuji menggunakan skenario yang telah ditentukan dengan memberikan input tertentu dan mengamati output yang dihasilkan oleh sistem. Hasil pengujian dicatat berdasarkan kesesuaian antara hasil aktual dengan hasil yang diharapkan. Apabila fungsi menghasilkan keluaran sesuai dengan skenario pengujian, fungsi dinyatakan berhasil. Hasil pengujian kemudian dianalisis secara deskriptif untuk mengetahui apakah fungsi prototipe telah berjalan sesuai rancangan.

B. Alur Penelitian

Secara keseluruhan, alur penelitian dilakukan secara berurutan sesuai dengan tampilan gambar berikut:



Gambar 1. Alur Penelitian dan Pengembangan Prototipe Keamanan Rekam Medis

Dengan alur tersebut, R&D berfungsi sebagai metode penelitian untuk menghasilkan produk, sedangkan Waterfall berfungsi sebagai model pengembangan yang mengatur urutan proses pengembangan produk. Hasil akhir penelitian berupa prototipe

MedSecure Hospital sebagai rancangan awal pengembangan keamanan rekam medis yang dapat menjadi dasar untuk pengembangan dan pengujian lebih lanjut sebelum diterapkan pada HIS operasional Rumah Sakit Awal Bros Batam.

HASIL DAN PEMBAHASAN

Hasil

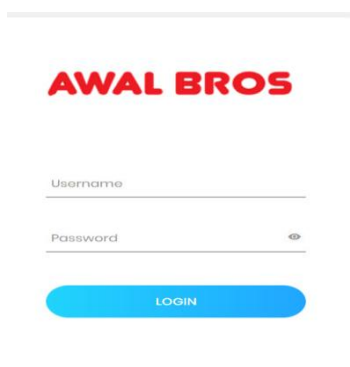
Kondisi Existing *Hospital Information System* (HIS) di Rumah Sakit Awal Bros Batam

Hospital Information System (HIS) yang digunakan di Rumah Sakit Awal Bros Batam merupakan sistem informasi terintegrasi yang mendukung pengelolaan pelayanan pasien, administrasi, dan data klinis. Akses sistem dilakukan melalui halaman *login* menggunakan *username* dan *password* sehingga pengguna perlu melakukan autentikasi sebelum mengakses modul yang tersedia. Sistem menyediakan berbagai modul yang mendukung kebutuhan operasional rumah sakit, antara lain *Electronic Medical Record* (EMR), Master Data, SATU SEHAT, Inventory, Transaksi, Keuangan, Operasi, Medical Record, Utility, dan BPJS.

Modul *Electronic Medical Record* (EMR) digunakan untuk mengelola berbagai informasi pasien, meliputi identitas pasien, nomor rekam medis, tanggal lahir, jenis kelamin, penjamin, poli tujuan, dan dokter yang menangani pasien. HIS juga menyediakan fitur pencatatan alergi yang memuat jenis alergi, nama alergen, serta catatan tambahan mengenai reaksi alergi. Informasi tersebut menjadi bagian penting dalam dokumentasi rekam medis karena dapat digunakan sebagai informasi pendukung dalam proses pelayanan dan pengambilan keputusan klinis.

HIS juga memiliki fitur skrining *Emerging Disease* yang digunakan untuk mendokumentasikan kondisi dan faktor risiko penyakit infeksi. Informasi yang tersedia mencakup riwayat perjalanan, riwayat kontak dengan kasus penyakit menular, gejala klinis, serta tindak lanjut yang diperlukan. Ketersediaan fitur tersebut menunjukkan bahwa HIS tidak hanya digunakan untuk pencatatan data rekam medis, tetapi juga mendukung pengelolaan informasi klinis dan kebutuhan pelayanan lainnya.

Gambaran antarmuka HIS menunjukkan beberapa tampilan utama yang digunakan dalam pengelolaan data dan informasi rekam medis pasien. Tampilan yang diamati meliputi halaman *login*, *dashboard Medical Record*, menu skrining *Emerging Disease*, menu pencatatan alergi, dan menu *Medical Record*. Halaman *login* digunakan sebagai akses awal bagi pengguna, sedangkan tampilan *Medical Record* memuat berbagai informasi yang berkaitan dengan data dan dokumentasi rekam medis pasien. Menu skrining *Emerging Disease* dan pencatatan alergi digunakan untuk mendukung pengelolaan informasi klinis tertentu yang menjadi bagian dari data pasien. Tampilan tersebut menjadi dasar untuk mengidentifikasi struktur sistem, jenis informasi yang dikelola, fitur yang tersedia, serta mekanisme akses pada sistem *existing*. Berikut disajikan Tampilan Awal pada Gambar berikut.



Gambar 2. Tampilan *Login* HIS di Rumah Sakit Awal Bros Batam



Gambar 3. Tampilan *Dashboard Medical Record*

[illegible]

Gambar 4. Tampilan Menu Skrining *Emerging Disease*

Tambah Alergi

Jenis Alergi

:

...

Alergen

:

Isi Alergen

Catatan

:

Isi Catatan Alergen

 Simpan

 Tutup

Gambar 5. Tampilan Menu Alergi, Jenis Alergi, Alergen, dan Catatan

RS AWAL BROS

PROFESIONAL RAPI IBADAH MENDENGKARKAN ASERTIF



[Home](#)
[EMR](#)
[EMR RJ](#)
[EMR RI](#)
[Sistem](#)
[Master](#)
[SATU SEHAT](#)
[Inventory](#)
[Transaksi](#)
[Keuangan](#)
[Inquiry](#)
[Operasi](#)
[Medical Record](#)
[Utility](#)
[QUERY](#)
[BPJS](#)
[Logout](#)

Pemeriksaan Berkas

Laporan Medical Record V2

Diagnosa Pasien Per-Poli V2

Surat Keterangan Lahir V2

Surat Keterangan Dokter V2

Lap Medrec Internal V2

Laporan Medrec Eksternal V2

Pencatatan Berkas Keluar

Laporan Kematian V2

Jml Pasien RI /Penjamin V2

Jml Pasien per dokter setiap bulan

Rokap Pasien Rirsuangan

Jml Pasien RJ /Penjamin V2

Laporan Keluar Masuk Pasien V2

Medrec Inactive v2

Laporan Detail Pendaftaran Pasien

Gambar 6. Tampilan Menu *Medical Record*

1. Hasil Analisis Keamanan Rekam Medis pada HIS

Analisis keamanan dilakukan dengan membandingkan kondisi sistem *existing* dengan enam aspek keamanan informasi yang menjadi dasar pengembangan, yaitu *confidentiality*, *integrity*, *authentication*, *availability*, dan *access control*. Analisis digunakan untuk mengetahui mekanisme keamanan yang telah tersedia serta kebutuhan penguatan yang dapat diterjemahkan ke dalam rancangan prototipe. Berikut disajikan analisis keamanan rekaman medis HIS pada Tabel 1.

Tabel 1. Analisis rekaman medis HIS

No.	Aspek Keamanan	Kondisi Existing	Kebutuhan Pengembangan
1	<i>Confidentiality</i>	Akses data dilakukan melalui akun pengguna dan pembatasan hak akses	Penguatan perlindungan data dan pencegahan akses oleh pihak yang tidak berwenang
2	<i>Integrity</i>	Data yang telah difinalisasi memiliki mekanisme pembatasan perubahan	Penguatan pengendalian perubahan dan pencatatan aktivitas perubahan data

3	<i>Authentication</i>	Menggunakan <i>username</i> dan <i>password</i> setelah beberapa kegagalan login	serta OTP beberapa kali	Penguatan mekanisme MFA	otentikasi melalui mekanisme
4	<i>Availability</i>	Tersedia <i>backup</i> dan infrastruktur pendukung system	mekanisme	Penguatan pemulihan dan kesinambungan akses	mekanisme
5	<i>Access control</i>	Hak akses disesuaikan dengan peran pengguna		Penguatan berdasarkan kebutuhan pengguna	pembatasan akses dan kewenangan

Berdasarkan Tabel 1, hasil analisis menunjukkan bahwa HIS telah memiliki sejumlah mekanisme keamanan dasar untuk melindungi rekam medis. Mekanisme tersebut mencakup autentikasi pengguna, pembatasan hak akses, pencatatan aktivitas, perlindungan jaringan, serta mekanisme pencadangan data. Kondisi tersebut menunjukkan bahwa pengembangan yang dibutuhkan tidak diarahkan untuk menggantikan sistem yang telah tersedia, tetapi untuk memperkuat mekanisme keamanan pada bagian yang masih memiliki celah.

Hasil identifikasi menunjukkan beberapa kebutuhan pengembangan yang menjadi dasar penyusunan prototipe. Pada aspek autentikasi, sistem masih menggunakan *username* dan *password* sebagai mekanisme utama, sedangkan *OTP* digunakan setelah terjadi beberapa kali kegagalan *login*. Mekanisme tersebut belum dapat dikategorikan sebagai *Multifactor Authentication* (MFA) apabila *OTP* belum digunakan sebagai faktor autentikasi kedua dalam proses *login* normal. Penguatan autentikasi menjadi salah satu kebutuhan yang perlu direpresentasikan dalam rancangan pengembangan.

Pada pengelolaan sesi pengguna, fitur *auto logout* telah tersedia, tetapi durasi sesi masih perlu dievaluasi agar sesuai dengan kebutuhan keamanan dan aktivitas pengguna. Sesi yang tetap terbuka dalam waktu yang relatif panjang dapat meningkatkan risiko akses oleh pihak lain ketika perangkat ditinggalkan tanpa melakukan *logout*. Rancangan pengembangan karena itu diarahkan pada pengelolaan sesi yang lebih aman melalui pengaturan batas waktu tidak aktif.

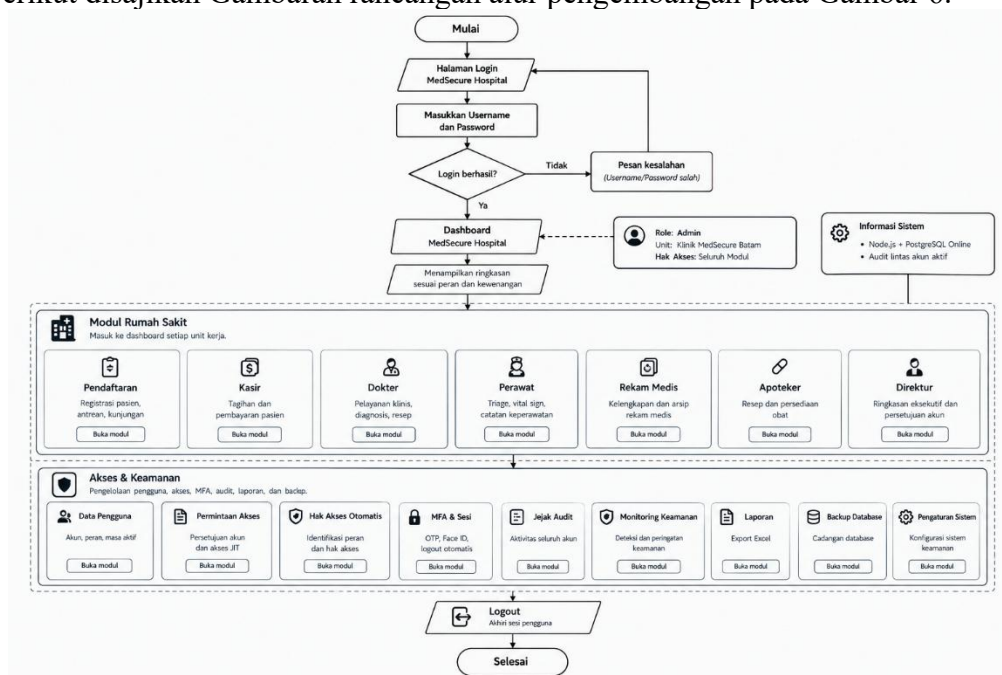
Pada aspek *non-repudiation*, HIS telah menyediakan *audit trail* untuk mencatat aktivitas pengguna. Mekanisme tersebut dapat digunakan untuk menelusuri aktivitas dalam sistem, tetapi pemantauan *log* perlu diperkuat agar tidak hanya dilakukan ketika terdapat kejadian yang mencurigakan. Pengembangan diarahkan pada penyediaan mekanisme pemantauan aktivitas yang lebih terstruktur sehingga aktivitas pengguna dapat ditelusuri dan dievaluasi secara lebih mudah.

Aspek pengguna juga menjadi bagian dari kebutuhan pengembangan keamanan. Penggunaan akun bersama dan kebiasaan tidak melakukan *logout* dapat mengurangi efektivitas mekanisme autentikasi dan pengendalian akses yang telah tersedia. Kondisi tersebut menunjukkan bahwa keamanan sistem perlu didukung oleh mekanisme teknis yang dapat mengurangi ketergantungan terhadap kedisiplinan pengguna. Hasil identifikasi kebutuhan tersebut selanjutnya digunakan sebagai dasar dalam menentukan fitur pada prototipe keamanan rekam medis.

2. Rancangan Pengembangan Keamanan Rekam Medis

Hasil analisis kebutuhan digunakan untuk menyusun rancangan pengembangan keamanan rekam medis dalam bentuk prototipe aplikasi berbasis web. Prototipe dikembangkan sebagai representasi rancangan keamanan yang dapat menggambarkan

penerapan fitur keamanan pada pengelolaan data rekam medis. Prototipe yang dikembangkan diberi nama *MedSecure Hospital* dan digunakan sebagai produk rancangan dalam penelitian. Rancangan sistem terdiri atas beberapa komponen utama, yaitu autentikasi pengguna, pengelolaan hak akses, pengelolaan data rekam medis, pengelolaan sesi pengguna, serta pencatatan aktivitas sistem. Setiap komponen dirancang berdasarkan kebutuhan keamanan yang telah diidentifikasi pada sistem existing. Struktur tersebut memungkinkan aspek keamanan tidak hanya dijelaskan secara konseptual, tetapi juga direpresentasikan dalam bentuk antarmuka dan alur fungsi pada aplikasi. Rancangan autentikasi diarahkan untuk memperkuat proses verifikasi pengguna melalui pengelolaan kredensial dan mekanisme autentikasi tambahan. Rancangan pengelolaan hak akses digunakan untuk membatasi akses terhadap informasi berdasarkan peran pengguna. Pengelolaan sesi digunakan untuk mengatur kondisi login dan logout pengguna, sedangkan pencatatan aktivitas digunakan untuk menyediakan jejak aktivitas yang dapat ditelusuri. Berikut disajikan Gambaran rancangan alur pengembangan pada Gambar 6.



Gambar 7. Rancangan Alur Pengembangan Keamanan Rekam Medis

Gambar 6 menunjukkan alur penggunaan prototipe *MedSecure Hospital* yang dimulai dari halaman login dan proses autentikasi pengguna. Setelah login berhasil, pengguna diarahkan ke dashboard yang menampilkan ringkasan sistem serta akses terhadap modul pelayanan rumah sakit dan fitur administrasi dan keamanan. Modul pelayanan meliputi Pendaftaran, Kasir, Dokter, Perawat, Rekam Medis, Apoteker, dan Direktur. Fitur administrasi dan keamanan meliputi Data Pengguna, Permintaan Akses, Hak Akses Otomatis, MFA & Sesi, Jejak Audit, Monitoring Keamanan, Laporan, *Backup Database*, dan Pengaturan Sistem. Akses terhadap setiap modul disesuaikan dengan peran dan kewenangan pengguna, kemudian proses penggunaan sistem diakhiri melalui *logout*.

Selain itu Data Flow Diagram (DFD) disusun sebagai rancangan konseptual untuk menggambarkan aliran data dan proses keamanan pada HIS. DFD Level 0 menggambarkan interaksi antara pengguna layanan, administrator, dan sistem dalam proses autentikasi, permintaan akses, pengelolaan rekam medis, serta pemantauan keamanan. Selanjutnya, DFD Level 1 menguraikan proses menjadi autentikasi dan sesi, pengelolaan hak akses, pelayanan rekam medis, jejak audit dan monitoring, serta administrasi sistem. Rancangan tersebut dilengkapi dengan penyimpanan data pengguna dan hak akses, data rekam medis, jejak audit, serta data backup dan konfigurasi. DFD digunakan untuk memperjelas

rancangan aliran data sebagai dasar pengembangan keamanan RME dan bukan sebagai gambaran implementasi sistem yang telah dikembangkan. berikut tampilan DFD disajikan dalam bentuk Gambar berikut.

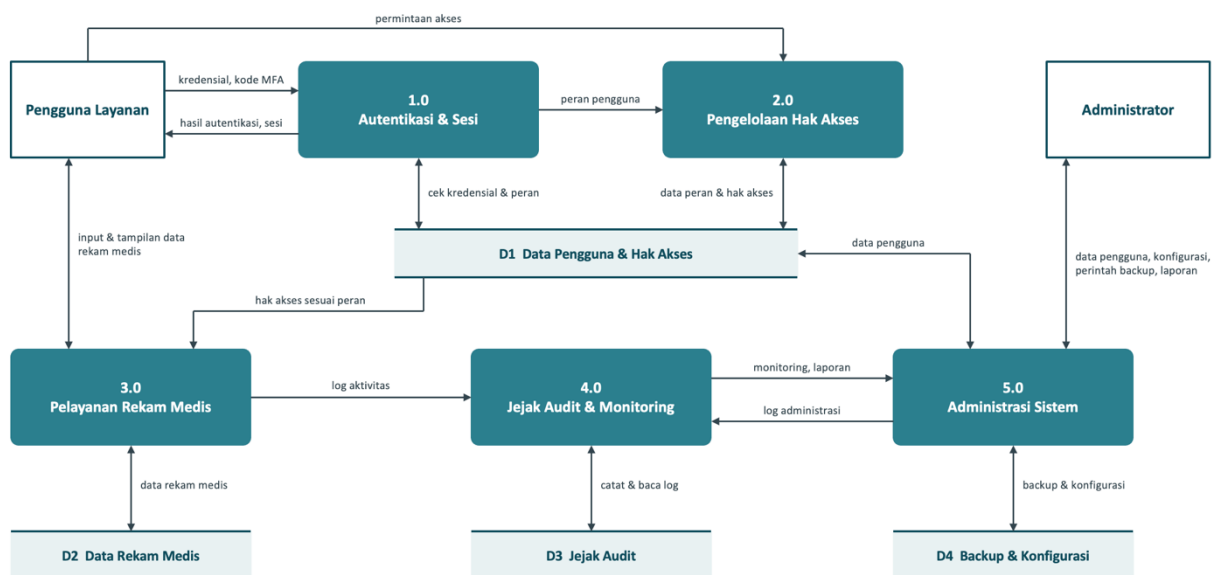
DFD Level 0 (Diagram Konteks) – MedSecure Hospital



Notasi: kotak = entitas eksternal, oval/kotak berwarna = proses, garis ganda = penyimpanan data, panah = aliran data

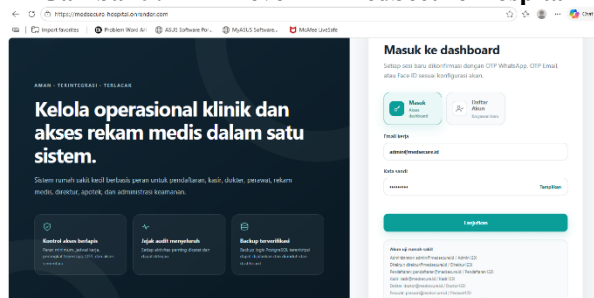
Gambar 8. DFD Level 0 (Diagram Konteks) – MedSecure Hospital

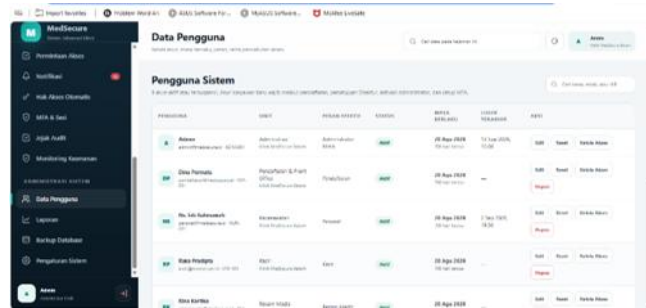
DFD Level 1 – MedSecure Hospital



Proses 1.0, 2.0, 3.0, dan 5.0 juga mengirim log aktivitas ke Proses 4.0 (tidak digambar agar diagram tetap terbaca).

Gambar 9. DFD Level 1 – MedSecure Hospital





Gambar 10. Tampilan Halaman MedSecure Hospital

Pengujian dilakukan terhadap fungsi utama prototipe *MedSecure Hospital* menggunakan metode *black-box testing*. Pengujian difokuskan pada kesesuaian antara masukan pengguna, proses pada sistem, dan keluaran yang dihasilkan. Pengujian mencakup fungsi autentikasi, pengelolaan akses, keamanan sesi, pencatatan aktivitas, monitoring, serta administrasi sistem untuk memastikan setiap fitur berjalan sesuai dengan rancangan. Berikut disajikan pengujian fungsional aplikasi pada Tabel 2.

Tabel 2. Hasil Pengujian Fungsional Prototipe MedSecure Hospital

No.	Fitur yang Diuji	Skenario yang Skenario	Hasil yang Diharapkan	Hasil yang Hasil Pengujian
1	Login	Memasukkan username dan password yang benar	Pengguna berhasil masuk ke dashboard sesuai peran	✓
2	Login	Memasukkan username atau password yang salah	Sistem menolak akses dan menampilkan pesan kesalahan	✓
3	Dashboard	Mengakses dashboard setelah login	Sistem menampilkan ringkasan sistem dan modul sesuai kewenangan pengguna	✓
4	Permintaan Akses	Membuka menu Permintaan Akses	Sistem menampilkan dan memproses permintaan akses sesuai kewenangan	✓
5	Hak Akses Otomatis	Mengakses pengaturan hak akses berdasarkan peran	Sistem memberikan akses sesuai peran dan kewenangan pengguna	✓
6	MFA & Sesi	Mengakses pengaturan MFA dan sesi pengguna	Sistem menyediakan mekanisme autentikasi tambahan dan pengelolaan sesi	✓
7	Jejak Audit	Pengguna melakukan aktivitas pada sistem	Aktivitas pengguna tercatat dan dapat ditelusuri melalui jejak audit	✓
8	Monitoring Keamanan	Membuka menu Monitoring Keamanan	Sistem menampilkan informasi kejadian atau aktivitas keamanan	✓
9	Data Pengguna	Membuka dan mengelola data akun pengguna	Sistem menampilkan data pengguna, peran, status, dan masa berlaku akun	✓
10	Laporan	Mengakses menu Laporan dan melakukan ekspor data	Sistem menampilkan laporan dan menyediakan fungsi ekspor	✓
11	Backup Database	Mengakses menu Backup Database	Sistem menyediakan fungsi pengelolaan pencadangan database	✓
12	Pengaturan Sistem	Membuka menu Pengaturan Sistem	Sistem menampilkan fungsi konfigurasi sistem sesuai hak akses administrator	✓

13	Modul Sakit	Rumah	Mengakses modul sesuai kewenangan pengguna	Sistem membuka modul pelayanan sesuai hak akses pengguna	✓
----	----------------	-------	---	--	---

Berdasarkan Tabel 2, hasil pengujian menunjukkan bahwa fungsi utama pada prototipe *MedSecure Hospital* dapat berjalan sesuai dengan rancangan. Proses login mampu melakukan autentikasi pengguna dan mengarahkan pengguna ke dashboard sesuai peran dan kewenangannya. Fitur Permintaan Akses, Hak Akses Otomatis, serta MFA dan Sesi merepresentasikan mekanisme pengendalian akses dan keamanan sesi pengguna. Fitur Jejak Audit dan Monitoring Keamanan mendukung pencatatan serta pemantauan aktivitas sistem, sedangkan Data Pengguna, Laporan, *Backup Database*, dan Pengaturan Sistem mendukung fungsi administrasi keamanan. Modul pelayanan rumah sakit juga dapat diakses melalui dashboard sesuai dengan kewenangan pengguna. Fungsi logout berjalan untuk mengakhiri sesi pengguna setelah penggunaan sistem.

PEMBAHASAN

Hasil penelitian menunjukkan bahwa pengembangan prototipe *MedSecure Hospital* dapat menjadi pendekatan untuk memperkuat aspek keamanan dalam pengelolaan rekam medis pada sistem informasi rumah sakit. Temuan utama penelitian tidak hanya terletak pada tersedianya prototipe berbasis web, tetapi pada pengintegrasian beberapa mekanisme keamanan ke dalam satu lingkungan sistem, yaitu autentikasi pengguna, pengelolaan hak akses, *MFA & Sesi*, *Jejak Audit*, *Monitoring Keamanan*, serta administrasi pengguna dan sistem. Struktur tersebut menunjukkan bahwa keamanan rekam medis perlu dipandang sebagai mekanisme yang bersifat berlapis, bukan hanya sebagai proses login menggunakan *username* dan *password*. Dalam penelitian ini, pengembangan rancangan keamanan didasarkan pada lima kriteria, yaitu *confidentiality*, *integrity*, *authentication*, *availability*, dan *access control*.

Hasil analisis terhadap sistem yang berjalan menunjukkan bahwa sistem informasi rumah sakit telah menyediakan mekanisme dasar berupa autentikasi pengguna, pengaturan akses, pencatatan aktivitas, perlindungan jaringan, dan pencadangan data. Meskipun demikian, masih terdapat kebutuhan untuk memperkuat perlindungan data, pengendalian perubahan data, autentikasi, ketersediaan dan pemulihan data, serta pengendalian akses. Kelima kebutuhan tersebut menjadi dasar dalam penyusunan rancangan pengembangan keamanan pada prototipe *MedSecure Hospital*. Penelitian sebelumnya menunjukkan bahwa tantangan keamanan pada data kesehatan muncul karena melibatkan banyak aktor, komponen teknologi, serta prosedur organisasi sehingga perlindungan data membutuhkan kombinasi antara mekanisme teknis dan pengelolaan akses yang sistematis (Suyahman, 2026).

A. Confidentiality

Aspek *confidentiality* berkaitan dengan perlindungan informasi rekam medis agar hanya dapat diakses oleh pengguna yang memiliki kewenangan. Berdasarkan hasil analisis, sistem yang berjalan telah menerapkan akun pengguna dan pembatasan akses terhadap data. Namun, masih diperlukan penguatan perlindungan data untuk mencegah akses oleh pihak yang tidak berwenang. Oleh karena itu, rancangan *MedSecure Hospital* mengakomodasi pengelolaan hak akses pengguna berdasarkan peran dan kewenangan sehingga informasi rekam medis dapat diberikan kepada pengguna sesuai dengan kebutuhan aksesnya. Penguatan tersebut mendukung upaya menjaga kerahasiaan informasi rekam medis dalam lingkungan sistem informasi rumah sakit.

B. Integrity

Aspek *integrity* berkaitan dengan menjaga keutuhan dan keakuratan data rekam medis agar tidak mengalami perubahan yang tidak sesuai dengan kewenangan. Hasil analisis menunjukkan bahwa data yang telah difinalisasi memiliki pembatasan terhadap perubahan.

Namun, diperlukan penguatan terhadap pengendalian perubahan dan pencatatan aktivitas pengguna. Dalam rancangan MedSecure Hospital, kebutuhan tersebut didukung melalui fitur Jejak Audit yang mencatat aktivitas pengguna dalam sistem. Pencatatan aktivitas tersebut memungkinkan aktivitas dan perubahan data ditelusuri berdasarkan pengguna dan tindakan yang dilakukan, sehingga mendukung pemeliharaan integritas informasi rekam medis.

C. Authentication

Aspek authentication berkaitan dengan proses verifikasi identitas pengguna sebelum memperoleh akses ke sistem. Berdasarkan hasil analisis, sistem yang berjalan telah menggunakan username dan password serta OTP setelah terjadi beberapa kali kegagalan login. Meskipun demikian, diperlukan penguatan mekanisme autentikasi untuk meningkatkan perlindungan terhadap akun pengguna. Rancangan MedSecure Hospital mengakomodasi kebutuhan tersebut melalui fitur MFA & Sesi. Fitur tersebut memberikan mekanisme autentikasi tambahan dan pengelolaan sesi pengguna sebagai bentuk penguatan terhadap proses verifikasi identitas dan keamanan akses pengguna.

D. Availability

Aspek availability berkaitan dengan ketersediaan sistem dan informasi rekam medis ketika dibutuhkan oleh pengguna yang berwenang. Hasil analisis menunjukkan bahwa sistem yang berjalan telah didukung oleh mekanisme pencadangan data dan infrastruktur pendukung. Namun, masih diperlukan penguatan terhadap pemulihan data dan kesinambungan akses apabila terjadi gangguan atau kehilangan data. Dalam rancangan MedSecure Hospital, kebutuhan tersebut didukung melalui fitur Backup Database. Mekanisme pencadangan tersebut menjadi bagian dari rancangan untuk mendukung ketersediaan informasi dan pemulihan data apabila terjadi gangguan pada sistem.

E. Access Control

Aspek access control berkaitan dengan pengaturan hak akses pengguna berdasarkan peran dan kewenangannya. Hasil analisis menunjukkan bahwa hak akses pada sistem yang berjalan telah disesuaikan dengan role pengguna. Namun, masih diperlukan penguatan pembatasan akses berdasarkan kebutuhan dan kewenangan pengguna. Pengembangan fitur Permintaan Akses dan Hak Akses Otomatis pada prototipe MedSecure Hospital memberikan penekanan bahwa pengguna tidak seharusnya memperoleh akses yang sama terhadap seluruh informasi rumah sakit. Hak akses perlu disesuaikan dengan peran dan kewenangan pengguna sehingga dapat mengurangi risiko akses yang tidak sesuai dengan kebutuhan dan kewenangan.

Selain kelima kriteria tersebut, prototipe MedSecure Hospital dilengkapi dengan fitur Jejak Audit dan Monitoring Keamanan untuk mendukung pemantauan aktivitas pengguna. Jejak Audit berfungsi mencatat aktivitas yang dilakukan pengguna sehingga aktivitas dalam sistem dapat ditelusuri apabila diperlukan. Sementara itu, Monitoring Keamanan mendukung pemantauan kejadian dan aktivitas keamanan dalam sistem. Kedua fitur tersebut diposisikan sebagai mekanisme pendukung dalam penerapan lima kriteria keamanan, terutama dalam mendukung pengendalian perubahan data, pengawasan aktivitas pengguna, dan pengendalian akses, bukan sebagai kriteria keamanan tambahan.

Pengembangan Backup Database, Data Pengguna, Laporan, dan Pengaturan Sistem melengkapi aspek keamanan dari sisi administrasi sistem. Keberadaan backup terutama berkaitan dengan keberlangsungan dan ketersediaan informasi apabila terjadi gangguan atau kehilangan data. Integrasi fungsi administrasi tersebut dengan fitur keamanan menunjukkan bahwa pengamanan rekam medis tidak hanya berkaitan dengan perlindungan

ketika data sedang diakses, tetapi juga mencakup pengelolaan akun, konfigurasi sistem, pemantauan, pelaporan, dan pemulihan data.

Dari perspektif pengembangan perangkat lunak, penggunaan model Waterfall memberikan alur pengembangan yang sistematis melalui analisis kebutuhan, perancangan, pengembangan, dan pengujian. Pendekatan tersebut sesuai dengan karakter penelitian yang berorientasi pada pengembangan prototipe berdasarkan kebutuhan keamanan yang telah diidentifikasi. Hasil pengujian black-box menunjukkan bahwa fungsi utama prototipe dapat berjalan sesuai dengan skenario yang dirancang. Keberhasilan fungsi login, dashboard, pengelolaan akses, MFA & Sesi, Jejak Audit, Monitoring Keamanan, administrasi pengguna, backup, modul pelayanan rumah sakit, dan logout menunjukkan bahwa rancangan yang dikembangkan telah dapat diterjemahkan ke dalam fungsi sistem yang dapat diuji secara fungsional.

Kontribusi penelitian ini terletak pada penyatuan kebutuhan keamanan rekam medis dengan struktur operasional rumah sakit dalam bentuk prototipe MedSecure Hospital. Prototipe tidak hanya menampilkan fitur keamanan secara terpisah, tetapi menempatkannya berdampingan dengan modul pelayanan seperti Pendaftaran, Kasir, Dokter, Perawat, Rekam Medis, Apoteker, dan Direktur. Struktur tersebut memberikan gambaran bahwa keamanan perlu melekat pada alur penggunaan sistem informasi rumah sakit, karena akses terhadap informasi kesehatan terjadi melalui berbagai peran dan aktivitas pelayanan. Implikasi penelitian bagi bidang sistem informasi kesehatan adalah tersedianya rancangan awal yang dapat digunakan sebagai acuan dalam pengembangan sistem keamanan rekam medis yang lebih terstruktur. Prototipe dapat menjadi dasar pengembangan lebih lanjut menuju sistem yang terintegrasi dengan infrastruktur rumah sakit, khususnya dalam penerapan autentikasi berlapis, pengendalian hak akses berdasarkan peran, pengelolaan sesi, pencatatan aktivitas, pemantauan kejadian keamanan, serta mekanisme pencadangan.

Penelitian ini memiliki beberapa keterbatasan. Prototipe MedSecure Hospital masih merupakan representasi rancangan dan belum diintegrasikan dengan HIS yang digunakan dalam operasional Rumah Sakit Awal Bros Batam. Data yang digunakan dalam prototipe juga bersifat simulasi sehingga hasil pengujian belum menggambarkan kondisi sistem ketika berhadapan dengan data pasien sebenarnya dan beban pengguna pada lingkungan rumah sakit. Pengujian yang dilakukan berfokus pada fungsi sistem melalui black-box testing sehingga belum mencakup penetration testing, pengujian kerentanan, pengujian performa, maupun pengujian keamanan infrastruktur secara langsung. Keterbatasan tersebut penting diperhatikan karena keamanan sistem kesehatan dipengaruhi tidak hanya oleh fungsi aplikasi, tetapi juga oleh infrastruktur, konfigurasi, pengguna, prosedur organisasi, dan lingkungan operasional.

Berdasarkan keterbatasan tersebut, penelitian selanjutnya direkomendasikan untuk melakukan integrasi prototipe dengan HIS pada lingkungan uji yang terkendali, menggunakan data yang telah dianonimkan, serta melakukan pengujian keamanan secara lebih komprehensif. Pengujian dapat diperluas melalui vulnerability assessment, penetration testing, pengujian performa, evaluasi keamanan sesi, serta pengujian skenario akses tidak sah. Pengembangan berikutnya juga dapat memperkuat mekanisme audit trail, menerapkan pengendalian akses yang lebih granular, serta mengevaluasi penggunaan MFA dalam kondisi operasional yang sebenarnya.

KESIMPULAN DAN SARAN

Kesimpulan

Penelitian ini menghasilkan prototipe MedSecure Hospital sebagai rancangan pengembangan keamanan rekam medis pada Hospital Information System (HIS) di Rumah Sakit Awal Bros Batam. Rancangan dikembangkan berdasarkan hasil analisis terhadap lima

kriteria keamanan, yaitu confidentiality, integrity, authentication, availability, dan access control. Kelima kriteria tersebut menjadi dasar dalam mengidentifikasi kebutuhan perbaikan keamanan pada sistem yang berjalan dan menerjemahkannya ke dalam rancangan fitur keamanan pada prototipe.

Hasil rancangan menunjukkan bahwa aspek confidentiality didukung melalui pengelolaan hak akses pengguna sesuai dengan peran dan kewenangan. Aspek integrity didukung melalui pengendalian perubahan data dan fitur Jejak Audit untuk mencatat aktivitas pengguna. Aspek authentication diperkuat melalui penerapan MFA dan pengelolaan sesi pengguna. Aspek availability didukung melalui mekanisme Backup Database untuk membantu ketersediaan dan pemulihan data. Sementara itu, aspek access control diwujudkan melalui fitur Permintaan Akses dan Hak Akses Otomatis yang menyesuaikan pemberian akses dengan kebutuhan dan kewenangan pengguna.

Hasil pengujian black-box menunjukkan bahwa fungsi utama pada prototipe, meliputi login, dashboard, pengelolaan akses, MFA & Sesi, Jejak Audit, Monitoring Keamanan, administrasi pengguna, backup, modul pelayanan rumah sakit, dan logout dapat berjalan sesuai dengan skenario pengujian yang dirancang. Dengan demikian, prototipe MedSecure Hospital dapat menjadi rancangan awal yang memberikan gambaran fungsional mengenai penguatan keamanan rekam medis pada HIS.

Prototipe yang dihasilkan masih berupa rancangan dan belum diintegrasikan dengan HIS operasional Rumah Sakit Awal Bros Batam. Oleh karena itu, hasil penelitian dapat digunakan sebagai dasar untuk pengembangan dan pengujian lebih lanjut pada lingkungan rumah sakit, khususnya melalui integrasi dengan HIS, penggunaan data yang telah dianonimkan, serta pengujian keamanan yang lebih komprehensif sebelum diterapkan pada lingkungan operasional.

Saran

Bagi Manajemen dan Unit Information Technology RS Awal Bros Batam\

1. Mengembangkan fitur Multifactor Authentication (MFA), auto-logout, dan pengelolaan hak akses sebagai penguatan keamanan HIS.
2. Melakukan pemantauan audit trail dan kejadian keamanan secara berkala serta memperbarui SOP terkait kerahasiaan dan penggunaan akun.
3. Melakukan pengujian keamanan lebih lanjut sebelum rancangan diintegrasikan ke HIS operasional.

Bagi Petugas Rekam Medis dan Tenaga Kesehatan

1. Menjaga kerahasiaan akun, menghindari penggunaan akun bersama, dan selalu melakukan logout setelah menggunakan HIS.
2. Meningkatkan kepatuhan terhadap SOP dan pelatihan keamanan informasi dalam pengelolaan rekam medis.

Bagi Peneliti Selanjutnya

1. Mengembangkan dan mengintegrasikan prototipe dengan HIS serta melakukan pengujian keamanan dan kinerja yang lebih komprehensif.
2. Mengkaji penerapan pada rumah sakit lain dan mengeksplorasi teknologi keamanan lanjutan, seperti blockchain, untuk memperkuat audit trail dan akuntabilitas akses data.

REFERENSI

- Arapa, A. (2026). *Keamanan Dan Perlindungan Data Rekam Medis*. AMU Press.
- Atin, S., Irmayanti, H., Heryandi, A., Nursikuwagus, A., Ishaq, U. M., & Darmayadi, A. (2026). Model Blockchain Pada Rekam Medis Terdistribusi: Tinjauan Ontologi dan Epistemologi Terhadap Integritas Data. *Komputa: Jurnal Ilmiah Komputer dan Informatika*, 15(1). <https://doi.org/10.34010/komputa.v15i1.18639>

- Budiman, A., Isa, M., & Soekiswati, S. (2025). Analisis risiko dan tindakan pencegahan kebocoran data rekam medis elektronik pasien di RS P Surakarta. *Jurnal Kesehatan*, 7(3), 2118–2127.
- Fauziah, Y. A., Susanto, D. A., & Utama, Y. P. (2026). Perlindungan Hukum Data Kesehatan Pasien di Era Digital: Legal Protection of Patient's Health Data in The Digital Era. *Jurnal Hukum dan Etika Kesehatan*, 6(1), 1–19. <https://doi.org/10.30649/jhek.v6i1.270>
- Hilmy, M. R., Putranto, R. D., Mahadewi, E. P., Setiawan, I., & Shameela, A. (2026). Analisis Integrasi Sistem Informasi Rumah Sakit dan Elektronik Rekam Medik Sebagai Respon Terhadap Permenkes Nomor 24 Tahun 2022. *Journal of Syntax Literate*, 11(1), 55.
- Indra, I., Dewi, T. N., & Wibowo, D. B. (2024). Perlindungan kerahasiaan data pasien vs kewajiban membuka akses rekam medis elektronik. *Soepa Jurnal Hukum Kesehatan*, 10(1), 97–117. <https://doi.org/10.24167/sjkh.v10i1.11542>
- Isnaeni, D. R., & Widiyanto, W. W. (2025). Evaluasi Kesiapan Implementasi Rekam Medis Elektronik Dengan Metode DOQ-IT. *Infokes: Jurnal Ilmiah Rekam Medis Dan Informatika Kesehatan*, 15(2), 122–128. <https://doi.org/10.47701/sz6pxf23>
- Nugroho, R. H., Siswatibudi, H., Permata, K., & Yogyakarta, I. (2023). Evaluasi aspek keamanan dan kerahasiaan rekam medis elektronik di Rumah Sakit Panti Nugroho. *Jurnal Permata Indonesia*, 14(2), 72–81. <https://doi.org/10.59737/jpi.v14i2.265>
- Nur Adiya, A. Z. D., Anggraeni, D. L., & Ilham Albana. (2024). Analisa Perbandingan Penggunaan Metodologi Pengembangan Perangkat Lunak (Waterfall, Prototype, Iterative, Spiral, Rapid Application Development (RAD)). *Merkurius : Jurnal Riset Sistem Informasi dan Teknik Informatika*, 2(4), 122–134. <https://doi.org/10.61132/mercurius.v2i4.148>
- Patilima, S. M., Ismail, G. A., & Antu, M. I. A. (2026). Implementasi Digitalisasi Rekam Medis dalam Menunjang Pelaksanaan Pelayanan Kesehatan di RSUD Bolaang Mongondow Utara. *Indonesian Journal of Innovation Multidisipliner Research*, 4(3), 7239–7261. <https://doi.org/10.69693/ijim.v4i3.1772>
- Pramesti, D. P. A., Ayuningtyas, D., & Verdi, R. (2024). Keamanan dan kerahasiaan data medis pasien dalam implementasi rekam medis elektronik: Tinjauan sistematis. *Prepotif: Jurnal Kesehatan Masyarakat*, 8(3), 7691–7702. <https://doi.org/10.31004/prepotif.v8i3.38445>
- Puspita, M., & Wisnuwardhana, I. A. (2026). Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) dan Rekam Medis Elektronik (RME) terhadap Kualitas Pelayanan Rawat Jalan: Literature Review. *JEMARI: Journal of Health and Medical Record Indonesia*, 3(1), 7–12. <https://doi.org/10.32660/jemari.v3i1.1055>
- Rangkuti, D. S. R., Tarigan, A. M., & Sembiring, R. M. (2026). Sosialisasi Keamanan Data Identitas untuk Pelayanan Kesehatan. *Jurnal Pengabdian Kepada Masyarakat Indonesia (JUPIKMAS)*, 1(3), 392–398.
- Rosalinda, R., Setiatin, S. S., & Susanto, A. S. (2021). Evaluasi penerapan rekam medis elektronik rawat jalan di Rumah Sakit Umum X Bandung tahun 2021. *Cerdika: Jurnal Ilmiah Indonesia*, 1(8), 1045–1056. <https://doi.org/10.36418/cerdika.v1i8.135>
- Santoso, A. D., Wulandari, I., Indonesia, I., Wicaksana, F. A., & Ramadhan, M. U. C. (2025). Legal Analysis of Patient Rights to Access and Confidentiality of Medical Records from the Perspective of Positive Law and Islamic Law. *Equality : Journal of Law and Justice*, 2(1), 27–41. <https://doi.org/10.69836/equality-jlj.v2i1.245>
- Sari, R. S., Desnita, Y., & Apriliani, M. (2022). Identifikasi Pengetahuan dan Pemahaman Profesional Perekam Medis terhadap Kompetensi Perekam Medis. *Jurnal Inovasi Penelitian*, 2(8), 2639–2646. <https://doi.org/10.47492/jip.v2i8.1139>
- Sofia, S., Ardianto, E. T., Muna, N., & Sabran, S. (2022). Analisis aspek keamanan informasi data pasien pada penerapan RME di fasilitas kesehatan. *Jurnal Rekam Medik & Manajemen Informasi Kesehatan*, 1(2), 94–103.

- Sonia, D., Putra, D. H., & Nurmalasari, M. (2026). Blockchain untuk Keamanan Data Kesehatan dalam Rekam Medis Elektronik. *J-REMI: Jurnal Rekam Medik dan Informasi Kesehatan*, 7(3), 209–218.
- Suyahman, S. (2026). Manajemen dan Kebijakan Keamanan Informasi. PT Solusi Administrasi Hukum. <https://journal.sah.co.id/index.php/publisher/article/view/50>
- Yunengsih, Y., & Oktaviani, V. (2024). Tingkat kesiapan implementasi rekam medis elektronik: Studi kasus pada Klinik Mata Dr. Hasri Ainun Habibie. *INNOVATIVE: Journal of Social Science Research*, 4(3), 16706–16716.