PENGEMBANGAN *CONSENT MANAGEMENT SYSTEM* DAN *BREAK-GLASS* UNTUK REKAM MEDIS ELEKTRONIK BERBASIS FHIR DAN DS4P

Proposal Tugas Akhir

Oleh

Irfan Musthofa
18222056

PROGRAM STUDI SISTEM DAN TEKNOLOGI INFORMASI
SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG

Desember 2025

LEMBAR PENGESAHAN

PENGEMBANGAN *CONSENT MANAGEMENT SYSTEM* DAN *BREAK-GLASS* UNTUK REKAM MEDIS ELEKTRONIK BERBASIS FHIR DAN DS4P

Proposal Tugas Akhir

Oleh

Irfan Musthofa
18222056

Program Studi Sistem dan Teknologi Informasi
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Proposal Tugas Akhir ini telah disetujui dan disahkan
di Bandung, pada tanggal 5 Desember 2025

Pembimbing

Dr. Ir. Rinaldi, M.T.

NIP. 196512101994021001

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

I.1 Latar Belakang

Perkembangan sistem informasi kesehatan di Indonesia mencapai tonggak penting dengan hadirnya SATUSEHAT, platform nasional berbasis standar *Fast Healthcare Interoperability Resources* (FHIR) yang bertujuan mewujudkan interoperabilitas rekam medis elektronik (RME) lintas fasilitas kesehatan. Dengan FHIR, data pasien direpresentasikan dalam bentuk sumber daya seperti *Patient*, *Observation*, dan *Condition* (Ayaz dkk. August 2021), sehingga memungkinkan pertukaran data medis secara terstandar dan aman antar sistem yang heterogen. Standar ini menggabungkan fleksibilitas teknologi web modern dengan model data klinis granular, menjadikannya fondasi utama interoperabilitas semantik pada berbagai sistem kesehatan global (Tabari dkk. March 2024).

Meskipun demikian, interoperabilitas teknis saja belum cukup tanpa tata kelola akses dan persetujuan pasien yang ketat. Kontrol akses merupakan komponen fundamental dalam perlindungan data pasien karena memastikan hanya pengguna berwenang yang dapat membaca, memodifikasi, atau membagikan informasi medis. Kajian sistematis oleh (Cobrado dkk. 2024) menunjukkan bahwa penelitian akses kontrol pada *Electronic Health Records (EHR)* masih didominasi dengan ide model *Role-Based Access Control (RBAC)* yang bersifat statis, sementara *Attribute-Based Access Control (ABAC)* dinilai lebih fleksibel karena mampu menggabungkan atribut subjek, objek, lingkungan, dan aksi untuk menghasilkan kebijakan akses yang lebih kontekstual. Studi tersebut juga menyoroti bahwa pembahasan mengenai mekanisme *emergency access* dan pengelolaan persetujuan pasien masih terbatas dalam literatur, sehingga diperlukan pendekatan yang lebih komprehensif untuk mendukung skenario klinis yang kompleks.

Model tradisional seperti *Role-Based Access Control (RBAC)* dinilai tidak memadai untuk menangani konteks klinis yang dinamis dan memerlukan keputusan akses berdasarkan kondisi pasien, lokasi, serta urgensi waktu (de Oliveira dkk. 2023). Sebagai solusi, model *Attribute-Based Access Control (ABAC)* dikembangkan untuk memungkinkan kontrol yang lebih spesifik dengan mempertimbangkan atribut pengguna, data, dan lingkungan. Studi oleh (de Oliveira dkk. 2023) memperkenalkan *Acute Care Attribute-Based Access Control* (*AC-ABAC*) yang menerapkan atribut kontekstual secara dinamis pada proses perawatan gawat darurat. Model ini memungkinkan sistem memberikan akses sementara kepada tim medis yang relevan tanpa mengorbankan privasi pasien, serta mencabut izin begitu sesi perawatan berakhir.

Namun, tantangan muncul pada praktik *break-glass access*, yaitu mekanisme pemberian akses darurat ketika nyawa pasien terancam. Pendekatan *break-glass* tradisional yang hanya menonaktifkan kebijakan akses bersifat statis terbukti berisiko disalahgunakan apabila tidak disertai mekanisme audit dan pencatatan forensik yang kuat. Oleh karena itu, diperlukan sistem yang mampu menyeimbangkan kebutuhan klinis dengan akuntabilitas melalui penerapan kontrol akses dinamis, audit yang tidak dapat diubah, dan notifikasi pasien.

Di sisi lain, kemunculan konsep *Patient-Accessible Electronic Health Records* (*PAEHR*) dan *patient portal* memperkuat paradigma perawatan yang berpusat pada pasien, di mana pasien berperan aktif dalam mengontrol siapa yang dapat mengakses data pribadinya dan untuk tujuan apa. Studi tinjauan cakupan oleh (Kariotis dkk. November 2023) menemukan bahwa akses pasien terhadap catatan medisnya meningkatkan transparansi dan kepercayaan terhadap tenaga medis, sekaligus mendorong komunikasi dua arah. Namun, hal ini juga memunculkan kekhawatiran terhadap praktik dokumentasi dan perlindungan informasi sensitif dalam konteks kesehatan mental.

Di Indonesia, berdasarkan (Kementerian Kesehatan Republik Indonesia 2025), penerapan SATUSEHAT Platform masih mengandalkan persetujuan umum dan kontrol akses yang bersifat umum dan kasar, sehingga pasien belum memiliki mekanisme kendali granular atau spesifik terhadap akses data sensitif. Padahal, regulasi nasional seperti Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP) dan Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis mewajibkan penerapan prinsip keamanan, kerahasiaan, keutuhan, serta hak pasien untuk menarik dan menghapus persetujuan.

Tanpa sistem yang mampu menegakkan kebijakan akses berbasis konteks dan melacak aktivitas akses secara transparan, risiko pelanggaran privasi dan sengketa hukum tetap tinggi meskipun platform nasional telah mengadopsi standar interoperabilitas modern.

Berdasarkan permasalahan tersebut, penelitian ini akan merancang dan mengevaluasi prototipe *Consent & Policy Gateway* yang menegakkan kebijakan akses granular menggunakan *FHIR* dan *Data Segmentation for Privacy* (*DS4P*) *Security Labels*. Sistem ini juga akan menyediakan *portal* pasien untuk mengatur pemberian atau pencabutan persetujuan, serta menerapkan protokol *break-glass* dengan audit yang tidak dapat diubah. Pendekatan ini diharapkan dapat memenuhi tuntutan regulasi nasional sekaligus meningkatkan transparansi dan kepercayaan pasien terhadap pengelolaan data rekam medis elektronik di Indonesia.

I.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan sebelumnya, berikut merupakan rumusan masalah tugas akhir ini:

1. Bagaimana merancang mekanisme persetujuan pasien yang bersifat granular dalam sistem rekam medis elektronik berbasis FHIR?
2. Bagaimana merancang kebijakan akses dan pelabelan keamanan untuk melindungi data sensitif pasien sesuai prinsip DS4P?
3. Bagaimana memastikan akses darurat *(break-glass access)* dapat dilakukan secara aman, terkontrol, dan terdokumentasi secara forensik?

I.3 Tujuan

Berdasarkan masalah yang dirumuskan, berikut merupakan tujuan yang ingin dicapai dalam pelaksanaan Tugas Akhir ini:

1. Merancang dan mengimplementasikan prototipe *Consent & Policy Gateway* berbasis standar *FHIR* untuk pengelolaan persetujuan *granular* pasien.
2. Mengintegrasikan dan menguji penerapan *security labels DS4P* guna menegakkan kebijakan akses data medis sensitif.
3. Mengembangkan mekanisme *break-glass* dan *audit trail* yang tidak dapat diubah untuk menjamin akuntabilitas akses darurat.

I.4 Batasan Masalah

Ruang lingkup dari permasalahan Tugas Akhir ini dibatasi agar tidak terjadi penyimpangan bahasan penelitian dan memastikan tujuan tercapai. Berikut merupakan batasan masalah pada pelaksanaan Tugas Akhir ini:

1. Penelitian hanya berfokus pada validasi fungsionalitas perancangan dan implementasi prototipe (*proof of concept*), bukan sistem produksi yang terintegrasi dengan SATUSEHAT atau sistem rumah sakit sebenarnya.
2. Implementasi sistem difokuskan pada lapisan aplikasi website dan *middleware* (*Consent & Policy Gateway*) tanpa mencakup pengembangan sistem rekam medis penuh dari sisi klinis.
3. Simulasi dilakukan menggunakan dataset RME *dummy* berbasis struktur *FHIR Resources* (*Patient*, *Observation*, *Consent*, *AuditEvent*, *Provenance*), bukan data pasien nyata.
4. Portal pasien dan portal klinisi dibangun dalam bentuk antarmuka web sederhana untuk demonstrasi konsep, sehingga desain antarmuka bersifat minimal dan fungsional, bukan fokus utama penelitian.
5. Penelitian tidak mencakup implementasi kriptografi atau enkripsi data medis secara penuh dari awal, melainkan hanya berfokus pada kontrol akses dan pencatatan aktivitas.
6. Evaluasi keamanan difokuskan pada konsistensi penegakkan kebijakan dan integritas audit, bukan pengujian penetrasi atau serangan siber.
7. Pengembangan tidak termasuk aspek skalabilitas.

I.5 Metodologi

Metodologi pelaksanaan Tugas Akhir ini menggunakan *Software Development Life Cycle (SDLC)* dengan tahapan berikut:

1. Perencanaan

   Tahap ini mencakup identifikasi kebutuhan sistem, penentuan ruang lingkup penelitian, serta penyusunan jadwal kerja. Aktivitas meliputi studi literatur terkait FHIR, DS4P, dan mekanisme kontrol akses pada rekam medis elektronik, serta penetapan alat, teknologi, dan batasan implementasi sesuai waktu pengerjaan.

2. Analisis

   Pada tahap ini dilakukan analisis kebutuhan fungsional dan nonfungsional sistem, termasuk identifikasi aktor (pasien, klinisi, administrator), alur persetujuan, aturan kebijakan akses, dan skenario *break-glass*. Analisis juga mencakup pemetaan atribut untuk penegakkan kebijakan berbasis FHIR dan simulasi DS4P *security labels*.

3. Desain

   Tahap desain berfokus pada perancangan arsitektur sistem, *use case diagram* untuk menggambarkan interaksi pengguna dengan sistem, model basis data, serta desain modul utama seperti *Consent Management*, *Policy Engine*, *Break-Glass Handler*, dan *Audit Trail*. Selain itu, dibuat pula desain antarmuka portal pasien dan portal klinisi menggunakan prinsip kemudahan penggunaan serta pemetaan antar komponen *backend* dan *frontend*.

4. Implementasi

   Implementasi dilakukan dengan mengembangkan prototipe *Consent & Policy Gateway* menggunakan tumpukan teknologi yang telah ditentukan. FHIR server diimplementasikan secara mock untuk mensimulasikan pertukaran data antar sistem, sementara *DS4P security labels* diterapkan pada metadata sumber yang relevan.

5. Pengujian

   Tahap ini bertujuan untuk memastikan fungsionalitas sistem berjalan sesuai kebutuhan melalui uji fungsional, uji kasus skenario akses, serta pengujian integritas jejak audit. Evaluasi dilakukan dengan menilai akurasi keputusan akses, keutuhan pencatatan audit, dan waktu respon sistem untuk memastikan prototipe berfungsi sesuai rancangan.

BAB II

STUDI LITERATUR

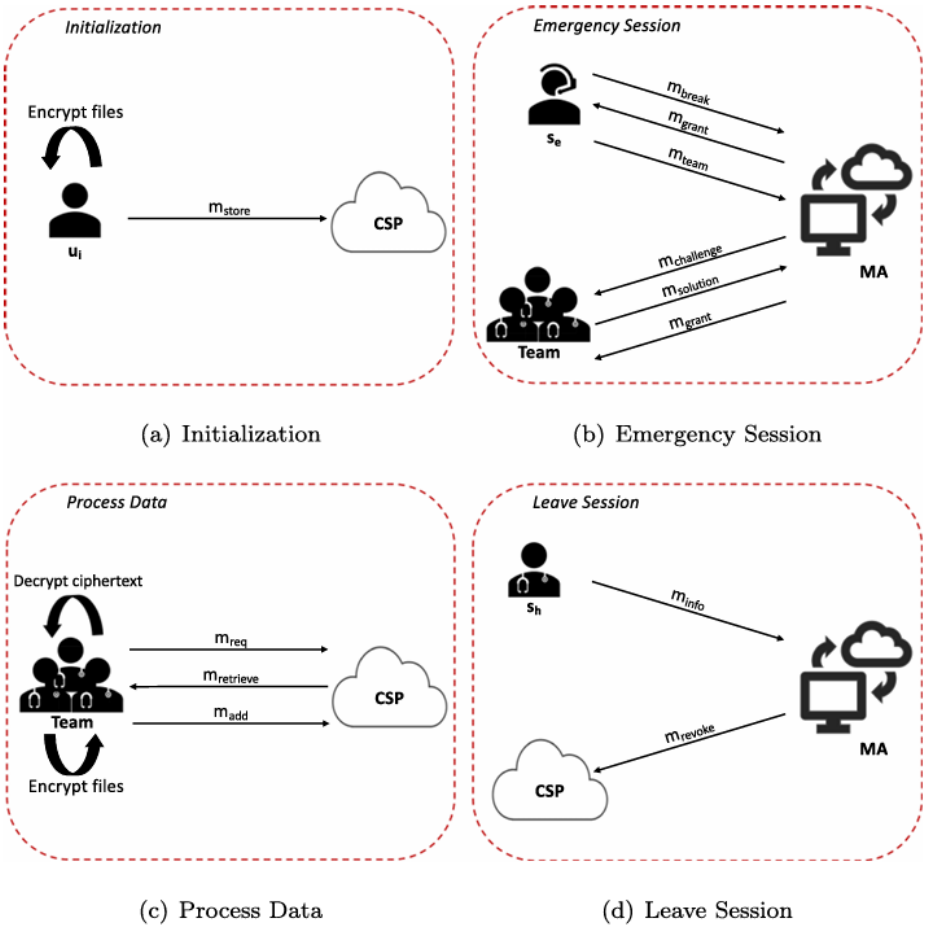
II.1 *Break-Glass Protocol*

Break-glass adalah mekanisme atau protokol pemberian akses darurat terhadap rekam medis ketika pasien tidak dapat memberikan persetujuan eksplisit karena kondisi klinis yang mengancam jiwa. Pada situasi akut seperti stroke, ketersediaan data pasien secara cepat sangat krusial untuk proses triase, diagnosis, dan pemilihan pusat perawatan. Hal ini ditegaskan dalam penelitian (Tuler de Oliveira dkk. March 2020) bahwa akses cepat terhadap data medis pasien merupakan elemen kritis dalam proses penentuan prioritas perawatan, diagnosis awal, dan pemilihan fasilitas kesehatan yang tepat. Dalam kondisi darurat, sistem harus tetap memungkinkan tenaga medis mengakses informasi tersebut meskipun pasien tidak berada dalam kondisi untuk memberikan persetujuan secara langsung.

Permasalahan utama pada mekanisme *break-glass* tradisional adalah sulitnya mencabut kembali akses setelah keadaan darurat selesai. Penelitian tersebut menyatakan bahwa sejumlah pendekatan *break-glass* yang ada belum menyediakan mekanisme pencabutan hak akses yang efektif setelah situasi darurat berakhir, sehingga menimbulkan risiko akses berkepanjangan yang tidak lagi sesuai dengan kebutuhan klinis.

Untuk mengatasi hal tersebut, (Tuler de Oliveira dkk. March 2020) mengusulkan *Red Alert Protocol (RAP)* berbasis *Ciphertext-Policy Attribute-Based Encryption (CP-ABE)* dan *temporary tokens*. Token darurat memungkinkan tenaga medis mengakses data terenkripsi hanya selama periode darurat dan dicabut secara otomatis setelah sesi perawatan berakhir.

Berikut adalah diagram alur *Red Alert Protocol (RAP)* yang diadaptasi dari (Tuler de Oliveira dkk. March 2020):



(a) Initialization (b) Emergency Session

(c) Process Data (d) Leave Session

Gambar II.1 Diagram *Red Alert Protocol (RAP)* (Tuler de Oliveira dkk. March 2020)

Berdasarkan gambar di atas, protokol dimulai dengan fase *Initialization* (a) di mana pasien (u_i) mengenkripsi *Electronic Medical Records* (EMR) mereka dan menyimpannya di *Cloud Service Provider* (CSP) menggunakan pesan m_{store}. Saat situasi kritis terjadi, alur berlanjut ke *Emergency Session* (b). Pada tahap ini, pusat panggilan darurat (s_e) mengirimkan pesan *break-glass* (m_{break}) kepada *Master Authority* (MA) untuk memulai sesi darurat. Secara paralel, tim medis melakukan otentikasi lokasi melalui pertukaran pesan tantangan-respons ($m_{challenge}$ dan $m_{solution}$) untuk membuktikan kehadiran fisik mereka. Setelah validasi berhasil, MA mengirimkan kunci dekripsi dan token akses sementara kepada tim medis melalui pesan m_{grant}.

Setelah mendapatkan akses, protokol memasuki fase *Process Data* (c). Tim medis menggunakan token yang valid untuk meminta (m_{req}) dan mengunduh ($m_{retrieve}$) data pasien terenkripsi dari CSP.

Data tersebut kemudian didekripsi secara lokal menggunakan kunci *Ciphertext-Policy Attribute-Based Encryption* (CP-ABE) darurat, dan tim medis juga dapat menambahkan informasi klinis baru ke dalam sistem melalui pesan m_{add}. Protokol diakhiri dengan fase *Leave Session* (d) ketika perawatan selesai atau pasien dipindahkan. Perwakilan tim (s_h) mengirimkan notifikasi status (m_{info}) ke MA, yang kemudian memicu pengiriman perintah pencabutan (m_{revoke}) ke CSP, sehingga token akses tim tersebut menjadi tidak valid secara instan.

II.2 *Blockchain*

Blockchain adalah teknologi *decentralized ledger* yang menyimpan catatan transaksi dalam bentuk blok yang saling terhubung secara kriptografis. Dalam konteks kesehatan, *blockchain* menawarkan integritas dan ketertelusuran yang kuat untuk pengelolaan data yang sensitif.

(Udayakumar July 2019) mendefinisikan *blockchain* sebagai buku besar digital yang tersebar dan tidak bergantung pada satu otoritas pusat. Catatan di dalamnya bersifat permanen dan tidak dapat diubah setelah divalidasi, serta menggunakan mekanisme kriptografi untuk menjamin proses autentikasi serta otorisasi.

Teknologi konvensional seperti server tunggal dan *database* relasional memiliki risiko besar seperti kegagalan pusat *(single point of failure)*, akses tidak sah, dan ketidakmampuan melacak perubahan. (Sarode, Watanobe, dan Bhalla March 2023) menunjukkan bahwa *audit trail* sering kali disimpan dalam *database* yang dapat dimodifikasi, sehingga keandalannya diragukan karena *database* relasional rentan mengalami perubahan, baik oleh pihak internal maupun eksternal, sehingga mengurangi tingkat kepercayaan terhadap validitas catatan tersebut.

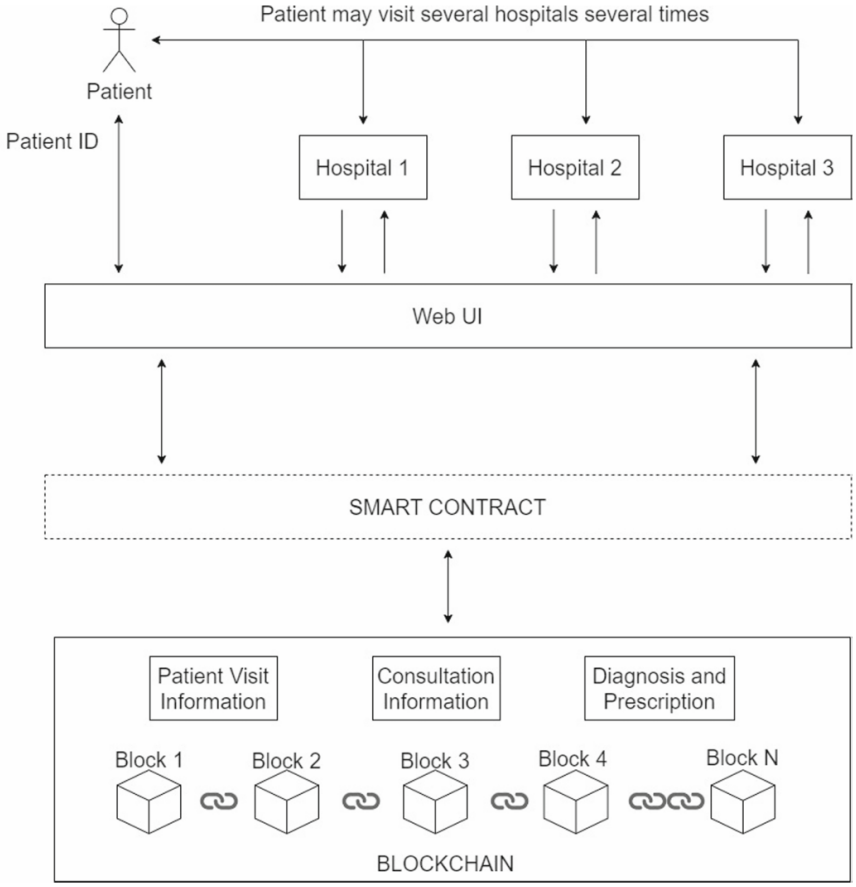
Dalam konteks kesehatan, *blockchain* tidak digunakan untuk menyimpan seluruh rekam medis karena ukuran data yang besar dan pertimbangan privasi. Sebaliknya, yang disimpan biasanya adalah hash, pointer, atau ringkasan metadata yang memastikan integritas dan keaslian data pada sumber utamanya, misalnya server rumah sakit. Dengan cara ini, *blockchain* berfungsi sebagai *proof ledger* terdistribusi.

II.3 *Audit Trail*

Audit trail adalah catatan kronologis mengenai aktivitas dalam sistem, seperti akses, perubahan data, atau tindakan administratif. Dalam sistem rekam medis elektronik (EHR), *audit trail* merupakan mekanisme utama untuk memastikan akuntabilitas, integritas, dan ketertelusuran. (Sarode, Watanobe, dan Bhalla March 2023) menjelaskan bahwa *audit trail* adalah rangkaian catatan yang mendokumentasikan berbagai peristiwa dan perubahan yang terjadi dalam sistem, dan sebagian besar fasilitas layanan kesehatan diwajibkan untuk memelihara catatan tersebut bagi setiap rekam medis elektronik. Menurut (Sarode, Watanobe, dan Bhalla March 2023), *audit trail* yang bergantung pada satu server atau *database* cenderung rentan, karena kegagalan pada satu titik tersebut dapat membuat catatan audit hilang atau dimodifikasi tanpa terdeteksi.

Oleh karena itu, integrasi *audit trail* dengan *blockchain* dianggap sebagai solusi modern. Dengan menyimpan *hash* atau ringkasan aktivitas pada blockchain, *audit trail* menjadi entitas jejak yang tidak bisa diubah, sehingga meningkatkan kepercayaan terhadap catatan tersebut. Selain itu waktu tercatat secara otomatis dan verifikasi dilakukan terdistribusi, memungkinkan ketahanan terhadap kegagalan sistem lokal. Dengan demikian, teori audit trail modern dalam domain kesehatan menekankan perpindahan dari penyimpanan terpusat menuju penyimpanan terdistribusi yang dapat diverifikasi oleh berbagai pihak.

Berikut adalah diagram arsitektur *blockchain* dalam sistem rekam medis elektronik yang diadaptasi dari (Sarode, Watanobe, dan Bhalla March 2023):



Gambar II.2 Diagram arsitektur *blockchain* dalam sistem rekam medis elektronik (Udayakumar July 2019)

Berdasarkan arsitektur sistem yang diusulkan pada Gambar II.2, alur dimulai dengan interaksi pasien ($Patient$) yang mengunjungi berbagai penyedia layanan kesehatan ($Hospital\ 1$, $Hospital\ 2$, $Hospital\ 3$). Seluruh pertukaran data antara entitas ini difasilitasi melalui antarmuka pengguna berbasis web (*Web UI*) yang terintegrasi dengan basis data masing-masing rumah sakit. *Web UI* ini berfungsi sebagai jembatan penghubung menuju lapisan logika bisnis yang dijalankan oleh *Smart Contract*. *Smart Contract* bertugas memvalidasi transaksi dan memastikan integritas data sebelum informasi tersebut dicatat secara permanen, tanpa memerlukan otoritas sentral atau pihak ketiga.

Pada lapisan infrastruktur data, sistem menggunakan teknologi *Blockchain* untuk menyimpan jejak audit (*audit trail*) dari setiap peristiwa medis. Informasi penting seperti detail kunjungan (*Patient Visit Information*), data konsultasi (*Consultation Information*), serta diagnosis dan resep (*Diagnosis and Prescription*) direkam ke dalam blok-blok ($Block\ 1$ hingga $Block\ N$) yang saling terhubung secara kriptografis. Karena sifat *blockchain* yang *immutable* (tidak dapat diubah) dan terdesentralisasi, mekanisme ini menjamin bahwa seluruh riwayat medis pasien tersimpan secara kronologis, transparan, dan aman dari manipulasi data.

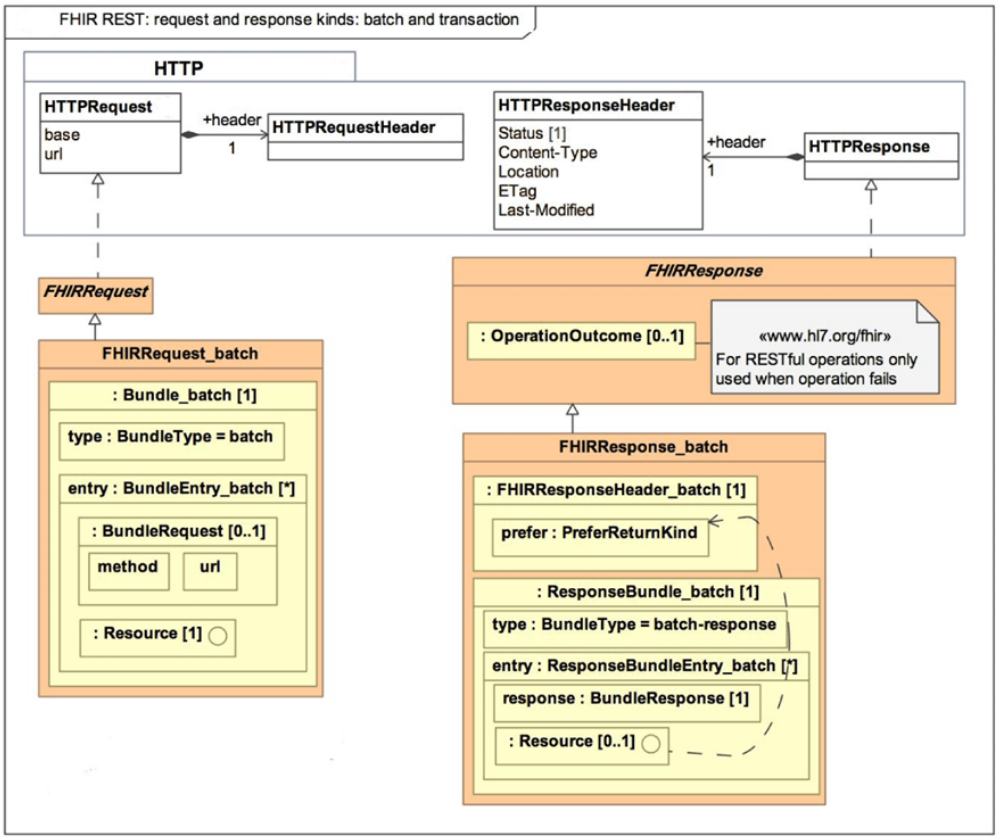
II.4 Penelitian Terkait

II.4.1 Interoperabilitas Data Kesehatan dan Standar FHIR

Interoperabilitas merupakan kemampuan sistem berbeda untuk saling bertukar dan menggunakan informasi dengan cara yang bermakna. Dalam bidang kesehatan, interoperabilitas sangat penting untuk memastikan kesinambungan perawatan dan efisiensi layanan medis. *FHIR* (*Fast Healthcare Interoperability Resources*) dikembangkan oleh *Health Level Seven International (HL7)* sebagai standar terbaru untuk pertukaran data kesehatan elektronik yang fleksibel dan berbasis web. *FHIR* dirancang dengan pendekatan sumber daya modular yang memungkinkan representasi entitas medis seperti *Patient*, *Observation*, *Condition*, dan *Consent* secara terpisah namun terhubung. Setiap sumber daya memiliki *URL* unik dan dapat diakses melalui *RESTful API*, menggunakan format *JSON* atau *XML*, sehingga mendukung integrasi lintas platform dan perangkat (Ayaz dkk. August 2021).

Selain itu, tinjauan literatur sistematis oleh (Ayaz dkk. August 2021) menegaskan bahwa FHIR memegang peranan vital dalam menyelesaikan masalah interoperabilitas data klinis di masa depan, terutama melalui dukungan terhadap teknologi pintar seperti *mobile health apps* dan *wearable devices*. Meskipun demikian, implementasi FHIR masih menghadapi tantangan signifikan, termasuk kompleksitas standar, hambatan adopsi di institusi kesehatan, serta kesulitan teknis dalam pemetaan dan migrasi data dari *legacy systems* ke standar baru ini. Oleh karena itu, keberhasilan penerapan FHIR tidak hanya bergantung pada keunggulan teknisnya, tetapi juga memerlukan strategi penanganan yang tepat terkait keamanan data sensitif dan privasi dalam lingkungan berbasis *cloud*.

Berikut adalah diagram arsitektur secara umum *FHIR* yang diadaptasi dari (Ayaz dkk. August 2021):



Gambar II.3 Diagram arsitektur *FHIR* secara umum (Ayaz dkk. August 2021)

Berdasarkan arsitektur umum yang diilustrasikan pada Gambar 1, standar *Fast Health Interoperability Resources* (FHIR) dirancang di atas protokol web standar, khususnya menggunakan pendekatan *Representational State Transfer* (REST) berbasis HTTP. Diagram tersebut menunjukkan bahwa setiap interaksi dimulai dengan *HTTPRequest* yang mencakup URL dasar untuk identifikasi sumber daya unik, serta *HTTPResponseHeader* yang membawa metadata penting seperti status, tipe konten (*Content-Type*), lokasi, dan stempel waktu modifikasi terakhir (*Last-Modified*).

Struktur permintaan dalam FHIR, yang digambarkan sebagai *FHIRRequest*, memungkinkan pengolahan data secara *batch* atau transaksi melalui mekanisme *Bundle*. Dalam mekanisme ini, sebuah *Bundle_batch* dapat memuat beberapa entri permintaan sekaligus, di mana setiap entri memiliki metode HTTP dan URL spesifik yang mengarah pada *Resource* kesehatan tertentu. Pendekatan modular berbasis sumber daya ini merupakan fitur pembeda utama FHIR dibandingkan standar HL7 versi sebelumnya.

Di sisi respons, *FHIRResponse* dirancang untuk memberikan umpan balik yang terstruktur.Jika terjadi kesalahan atau sekadar memberikan informasi status operasi, sistem dapat mengembalikan *OperationOutcome*. Untuk permintaan yang berhasil, sistem menghasilkan *FHIRResponse_batch* yang berisi *ResponseBundle*, di mana setiap entri respons menyertakan *Resource* yang diminta atau hasil dari operasi yang dilakukan. Hal ini menegaskan bahwa unit dasar transaksi dan pertukaran data dalam arsitektur ini adalah *Resource* itu sendiri, yang berfungsi sebagai konsep diskrit terkecil dalam pertukaran data medis.

II.4.2 Segmentasi Data Sensitif dan *Data Segmentation for Privacy (DS4P)*

Dalam sistem kesehatan modern, tidak semua data pasien memiliki tingkat sensitivitas yang sama. Informasi mengenai *HIV*, kesehatan mental, dan catatan reproduksi, misalnya, memerlukan perlakuan khusus dalam kontrol akses. Untuk itu, *HL7* mengembangkan konsep *Data Segmentation for Privacy (DS4P)*, yaitu mekanisme pelabelan keamanan (*security labeling*) terhadap informasi atau bagian data tertentu dalam *FHIR* agar dapat dibatasi aksesnya sesuai peraturan dan persetujuan pasien.

Panduan resmi (HL7 International 2025) menjelaskan bahwa setiap label keamanan di *DS4P* mengandung metadata tentang tingkat sensitivitas, kategori privasi, atau peraturan yang mengikat suatu data. Label ini kemudian digunakan oleh sistem *policy engine* untuk menegakkan kebijakan akses. Dengan demikian, *DS4P* tidak secara langsung mengenkripsi data, tetapi menghubungkan sumber daya informasi dengan kerangka kerja keamanan yang lebih luas melalui label semantik.

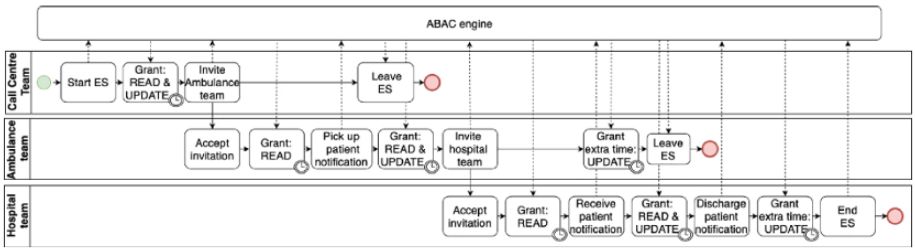
Hal ini relevan bagi penelitian ini karena sistem *Consent & Policy Gateway* yang dirancang akan memanfaatkan prinsip *DS4P* untuk mengatur siapa yang dapat mengakses data sensitif, dengan menambahkan label keamanan dalam metadata *FHIR resource* seperti *meta.security*.

II.4.3 Model Kontrol Akses pada Rekam Medis Elektronik: RBAC hingga ABAC

Kontrol akses adalah fondasi utama keamanan informasi kesehatan. Model *Role-Based Access Control (RBAC)* secara tradisional digunakan dalam sistem informasi kesehatan karena kesederhanaannya. Hak akses diberikan berdasarkan peran pengguna (misalnya dokter, perawat, atau staf admin). Namun, penelitian (Carvalho dan Bandiera-Paiva February 2018) menemukan bahwa *RBAC* memiliki keterbatasan signifikan untuk konteks layanan kesehatan modern yang bersifat dinamis, seperti pengelolaan akses darurat, delegasi izin, dan interoperabilitas lintas *domain*.

Untuk mengatasi keterbatasan tersebut, model *Attribute-Based Access Control (ABAC)* dikembangkan dengan keputusan berbasis atribut subjek, objek, dan konteks lingkungan. Menurut (de Oliveira dkk. 2023), *ABAC* memungkinkan keputusan akses spesifik yang mempertimbangkan situasi waktu nyata, seperti lokasi pengguna atau status darurat pasien. Fleksibilitas inilah yang membuat *ABAC* lebih cocok untuk sistem rekam medis elektronik yang kompleks.

Berikut adalah diagram alur kerja informasi perawatan akut pada *Attribute-Based Access Control (ABAC)* yang diadaptasi dari (de Oliveira dkk. 2023):



Gambar II.4 Diagram alur kerja informasi perawatan akut pada *Attribute-Based Access Control (ABAC)* (de Oliveira dkk. 2023)

Berdasarkan diagram alur kerja informasi perawatan akut, proses dimulai ketika *Call Centre Team* menginisiasi *Emergency Session (ES)*, yang secara otomatis memicu mesin ABAC untuk memberikan hak akses *READ* dan *UPDATE* kepada mereka. Tim ini kemudian mengundang *Ambulance Team* ke dalam sesi. Setelah undangan diterima, *Ambulance Team* awalnya hanya diberikan hak akses *READ*, namun hak ini ditingkatkan menjadi *READ* dan *UPDATE* segera setelah mereka melakukan notifikasi penjemputan pasien *pick up patient*. Mekanisme ini memastikan bahwa hak akses diberikan secara dinamis dan bertahap sesuai dengan keterlibatan aktif tim dalam menangani pasien.

Selanjutnya, alur berlanjut ketika *Ambulance Team* mengundang *Hospital Team*. Tim rumah sakit mendapatkan hak akses *READ* saat menerima undangan untuk persiapan, dan kemudian mendapatkan akses penuh (*READ* dan *UPDATE*) saat pasien tiba dan diterima secara fisik di rumah sakit. Alur kerja ini diakhiri dengan fase pemulangan pasien (*discharge*), di mana sistem memberikan waktu tambahan (*extra time*) bagi tim medis untuk melengkapi data administratif atau klinis sebelum akses benar-benar dicabut dan sesi diakhiri (*End ES*) secara permanen.

II.4.4 Akses Darurat dan Model AC-ABAC

Situasi gawat darurat menuntut sistem yang mampu memberikan akses cepat terhadap data medis tanpa mengorbankan keamanan. Pendekatan konvensional yang dikenal sebagai *break-glass access* memberikan akses darurat tanpa pembatasan granular, namun kerap disalahgunakan karena minimnya *audit* dan kontrol otomatis.

Model *AC-ABAC (Acute-Care Attribute-Based Access Control)* yang dikembangkan oleh (de Oliveira dkk. 2023) memperkenalkan mekanisme dinamis di mana keputusan akses didasarkan pada atribut klinis. Akses darurat diberikan secara sementara dan dicatat sepenuhnya melalui *audit trail* yang tidak dapat diubah, memastikan keseimbangan antara ketersediaan data dan privasi pasien.

II.4.5 *Consent Management* dan Peran Pasien

Konsep *Patient-Accessible Electronic Health Records (PAEHR)* menekankan hak pasien untuk mengakses, memberi, atau mencabut izin atas data kesehatannya. (Kariotis dkk. November 2023) menunjukkan bahwa pemberian akses langsung kepada pasien meningkatkan transparansi dan kepercayaan antara pasien dan penyedia layanan kesehatan.

FHIR menyediakan sarana teknis untuk merekam dan mengatur persetujuan pasien. Namun, penerapan *Consent* dalam banyak studi masih bersifat umum (*coarse-grained*) dan belum mendukung pengaturan granular oleh pasien sendiri. Kondisi ini menjadi celah riset yang dijawab oleh penelitian ini melalui rancangan *Portal Pasien* yang memungkinkan kontrol persetujuan granular berbasis *FHIR*.

BAB III

ANALISIS MASALAH

III.1 Analisis Kondisi Saat Ini

Sistem rekam medis elektronik (RME) di Indonesia saat ini sedang bertransformasi menuju interoperabilitas nasional melalui platform *SATUSEHAT*, yang mengadopsi standar *FHIR (Fast Healthcare Interoperability Resources)*. Meskipun langkah ini memperkuat pertukaran data antar fasilitas kesehatan, penerapan mekanisme privasi dan kontrol akses yang memadai masih terbatas pada tingkat persetujuan umum (*general consent*). Artinya, pasien memberikan persetujuan secara menyeluruh tanpa dapat menentukan data spesifik mana yang dapat diakses oleh tenaga kesehatan tertentu (Ayaz dkk. 2021; Tabari dkk. 2024).

Selain itu, sistem *SATUSEHAT* belum menerapkan segmentasi privasi berbasis *DS4P (Data Segmentation for Privacy)* untuk membedakan tingkat sensitivitas data medis. Kondisi ini berpotensi menimbulkan pelanggaran privasi ketika data sensitif seperti rekam kesehatan mental atau penyakit menular dibagikan secara luas tanpa pembatasan yang proporsional.

Pada sisi keamanan, penerapan kontrol akses di fasilitas kesehatan umumnya masih menggunakan model *RBAC (Role-Based Access Control)* yang bersifat statis dan hierarkis, sehingga sulit menyesuaikan dengan situasi dinamis seperti akses darurat (*emergency access*) atau kerja lintas departemen (de Carvalho Jr. & Bandiera-Paiva 2018). Belum adanya jejak audit (*audit trail*) yang tidak dapat diubah dan kurangnya partisipasi pasien dalam pengelolaan persetujuan memperkuat perlunya pendekatan baru berbasis manajemen persetujuan yang terperinci (*fine-grained consent management*) dan penegakan kebijakan (*policy enforcement*) dinamis.

Menurut dokumentasi resmi (Kementerian Kesehatan Republik Indonesia 2025), keamanan data pasien dijaga melalui kebijakan hak akses yang memastikan hanya

tenaga kesehatan di fasilitas layanan yang memperoleh persetujuan pasien yang dapat mengakses data tersebut. Selain itu, *SATUSEHAT Platform* menerapkan metode pengamanan seperti *masking* dan *encryption* untuk melindungi data selama pemrosesan dan pertukaran. Hal ini menunjukkan bahwa meskipun mekanisme dasar perlindungan data telah diterapkan, aspek pengelolaan persetujuan granular dan segmentasi privasi masih belum didukung secara penuh.

III.2 Analisis Kebutuhan

III.2.1 Identifikasi Masalah Pengguna

Masalah utama yang dihadapi pengguna baik pasien maupun tenaga kesehatan dapat diidentifikasi sebagai berikut:

1. Kurangnya kontrol pasien atas data pribadi.
   Pasien tidak dapat menentukan secara spesifik siapa yang boleh mengakses data tertentu sesuai kebutuhan medis.
2. Ketergantungan pada persetujuan umum (*general consent*).
   Tidak ada mekanisme granular untuk mengelola izin akses berdasarkan tipe data, tujuan, atau waktu.
3. Model kontrol akses yang kaku.
   RBAC tidak mendukung konteks darurat atau multi-atribut seperti lokasi dan kondisi klinis.
4. Ketiadaan audit forensik yang transparan.
   Aktivitas akses data belum dilengkapi jejak audit yang tidak dapat diubah (*immutable audit trail*) untuk memastikan akuntabilitas.
5. Risiko penyalahgunaan *break-glass*.
   Akses darurat dapat dilakukan tanpa pembatasan waktu atau otentikasi tambahan.
6. Belum adanya portal pasien interaktif.
   Sistem belum memberikan sarana bagi pasien untuk memberikan atau mencabut persetujuan secara langsung berbasis *FHIR Consent*.

Untuk mencari solusi atas masalah-masalah tersebut, perlu disusun kebutuhan fungsional dan nonfungsional sistem yang diperlukan. Subbab berikut menjabarkan kebutuhan-kebutuhan tersebut.

III.2.2 Kebutuhan Fungsional

Berikut adalah kebutuhan fungsional yang disajikan dalam bentuk tabel:

Tabel III.1 Kebutuhan Fungsional

Kode	**Kebutuhan Fungsional**	**Deskripsi**
FR-1	Manajemen Persetujuan	Sistem dapat mencatat, menampilkan, dan memperbarui status persetujuan pasien berbasis *FHIR Consent*.
FR-2	Pemberian Persetujuan Granular	Pasien dapat menentukan akses berdasarkan jenis data, peran pengguna, dan tujuan penggunaan.
FR-3	*Policy Enforcement*	Sistem menegakkan kebijakan akses secara otomatis menggunakan *security labels DS4P* dan atribut pengguna.
FR-4	*Break-Glass Access*	Tenaga medis dapat melakukan akses darurat dengan autentikasi tambahan dan batas waktu.
FR-5	*Audit Trail*	Semua aktivitas akses dicatat secara kronologis dan dihash untuk memastikan integritas data audit.
FR-6	Portal Pasien & Klinik	Tersedia antarmuka web untuk pasien dan tenaga medis guna mengelola dan meninjau status akses.

Tabel kebutuhan fungsional di atas dirancang untuk mengatasi tantangan keseimbangan antara interoperabilitas data dan privasi pasien yang kompleks. Kebutuhan FR-1 dan FR-2, yang berfokus pada manajemen persetujuan berbasis standar *Fast Healthcare Interoperability Resources* (FHIR), mengadopsi pendekatan pertukaran data yang fleksibel sebagaimana dijelaskan dalam tinjauan sistematis Ayaz dkk. (Ayaz dkk. August 2021). Lebih lanjut, spesifikasi persetujuan granular (FR-2) merupakan respons langsung terhadap keterbatasan model *Role-Based Access Control* (RBAC) tradisional. Studi (Carvalho dan Bandiera-Paiva February 2018) menegaskan bahwa RBAC murni sering kali terlalu statis untuk menangani dinamika privasi modern, sehingga diperlukan mekanisme yang lebih terperinci seperti yang ditawarkan sistem ini (Carvalho dan Bandiera-Paiva February 2018).

Untuk mekanisme penegakan kebijakan (FR-3) dan penanganan situasi kritis (FR-4), sistem beralih dari kontrol statis menuju model yang adaptif terhadap konteks. Penerapan *Policy Enforcement* menggunakan pendekatan *Attribute-Based Access Control* (ABAC) didasarkan pada temuan de Oliveira dkk., yang menunjukkan bahwa keputusan akses dalam layanan akut memerlukan evaluasi konteks waktu nyata (seperti lokasi dan waktu) yang tidak dapat dipenuhi oleh RBAC (de Oliveira dkk. 2023). Fitur *Break-Glass Access* (FR-4) secara spesifik mengimplementasikan protokol keamanan darurat yang menjamin ketersediaan data kritis saat dibutuhkan, namun tetap membatasi akses tersebut hanya selama durasi insiden, selaras dengan prinsip keamanan *Acute Care* (Tuler de Oliveira dkk. March 2020).

Terakhir, akuntabilitas sistem dijaga melalui mekanisme *Audit Trail* yang berintegritas tinggi (FR-5). Mengingat kerentanan basis data audit tradisional terhadap manipulasi pihak internal maupun eksternal, spesifikasi ini mengadopsi prinsip yang diusulkan oleh Sarode dkk., di mana setiap pencatatan aktivitas harus dilindungi menggunakan fungsi kriptografis (seperti *hash*) untuk memastikan sifat *immutability* data (Sarode, Watanobe, dan Bhalla March 2023). Seluruh fitur keamanan backend ini kemudian dipresentasikan kepada pengguna melalui antarmuka portal (FR-6) untuk transparansi dan kemudahan pengelolaan.

III.2.3 Kebutuhan Nonfungsional

Berikut adalah kebutuhan nonfungsional yang disajikan dalam bentuk tabel:

Tabel III.2 Kebutuhan Nonfungsional

Kode	Kebutuhan Non-fungsional	Deskripsi
NFR-1	Keamanan	Sistem menggunakan autentikasi dan hashing audit untuk menjaga kerahasiaan serta integritas data.
NFR-2	Kinerja	Respon kebijakan akses tidak melebihi 10 detik pada skenario pengujian lokal.
NFR-3	Auditabilitas	Semua keputusan akses dapat dilacak dengan identitas, waktu, dan alasan.

III.3 Analisis Pemilihan Solusi

III.3.1 Alternatif Solusi

Berikut adalah alternatif solusi yang dirancang dalam bentuk tabel:

Tabel III.3 Alternatif Solusi

Kode	Alternatif Solusi	Deskripsi Singkat
S-1	*RBAC Enhanced*	Pengembangan sistem berbasis peran dengan tambahan lapisan verifikasi pasien, namun tetap bersifat statis dan kurang adaptif terhadap konteks.
S-2	*ABAC Policy Engine*	Penerapan kontrol akses berbasis atribut dan integrasi *FHIR Consent*, mendukung granularitas tinggi pada keputusan akses.
S-3	*ABAC* dengan *DS4P* dan Protokol *Break-Glass*	Integrasi *Attribute-Based Access Control* untuk kondisi darurat, ditambah pelabelan *DS4P* serta mekanisme *audit* yang tidak dapat diubah.

Ketiga alternatif ini dievaluasi untuk menentukan solusi yang paling sesuai dengan kebutuhan keamanan, privasi, dan keterlibatan pasien.

III.3.2 Analisis Penentuan Solusi

Untuk menentukan solusi terbaik, ketiga alternatif dinilai berdasarkan beberapa kriteria utama, yaitu: privasi data, transparansi & auditabilitas, kemudahan implementasi, kepatuhan regulasi, dukungan *FHIR Consent*, dukungan akses darurat, dan kesesuaian terhadap masalah penelitian.

Penilaian menggunakan skala 1–5, di mana:

1 = Sangat Buruk, 2 = Buruk, 3 = Cukup, 4 = Baik, 5 = Sangat Baik.

Berikut adalah hasil analisis penentuan solusi dalam bentuk tabel:

Tabel III.4 Analisis Penentuan Solusi

Kriteria Penilaian	**S-1 *RBAC Enhanced***	**S-2 *ABAC Policy Engine***	**S-3 *ABAC* + *DS4P* + Protokol *Break-Glass***
Privasi Data	3	4	5
Transparansi & Auditabilitas	2	4	5
Kemudahan Implementasi	5	4	3
Kepatuhan terhadap Regulasi (*UU PDP 2022*, Permenkes 24/2022)	3	4	5
Dukungan *FHIR Consent*	2	4	5
Dukungan Akses Darurat	1	5	3
Kesesuaian terhadap Permasalahan Penelitian	3	4	5
Total Skor (dari 35)	**19**	**27**	**33**

Berdasarkan hasil evaluasi, solusi S-3 (*ABAC* dengan *DS4P* dan Protokol *Break-Glass*) memperoleh skor tertinggi (33/35) dan dinilai paling sesuai dengan konteks penelitian. Solusi ini tidak hanya menegakkan privasi dan keamanan pasien melalui penerapan *security labels DS4P*, tetapi juga mendukung akses dinamis pada situasi darurat dengan mekanisme *audit* yang tidak dapat diubah. Selain itu, integrasi *FHIR Consent* memberi ruang bagi pasien untuk mengelola persetujuan secara granular, memenuhi prinsip transparansi, akuntabilitas, dan kepatuhan regulasi nasional.

BAB IV

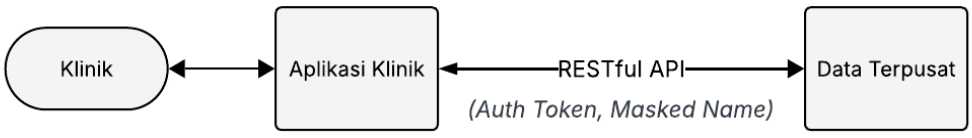
DESAIN KONSEP SOLUSI

IV.1 Model Konseptual Sebelumnya

Model konseptual sistem saat ini menggambarkan alur pertukaran data kesehatan yang hanya memanfaatkan standar *FHIR* sebagai mekanisme interoperabilitas lintas fasilitas kesehatan. Pada kondisi ini, aplikasi klinik mengirimkan permintaan ke sistem basis data terpusat untuk mengambil atau memperbarui data pasien, yang kemudian diteruskan ke sistem rekam medis elektronik (RME) internal rumah sakit dan penyimpanan data. Mekanisme kontrol akses yang digunakan masih bersifat *general consent*, sehingga pasien tidak memiliki kendali granular atas data mana yang dapat diakses.

Di sisi privasi, perlindungan hanya dilakukan melalui *masking* sederhana pada tampilan nama pasien, misalnya "Irf** Mus*****" tanpa segmentasi data sensitif atau kebijakan keamanan berbasis metadata. Tidak terdapat mekanisme penegakan kebijakan (*policy enforcement*), pengelolaan persetujuan granular, maupun audit mendalam sehingga sistem rentan terhadap akses yang tidak tepat.

Berikut adalah diagram alur data pada model konseptual sebelumnya:



Gambar IV.1 Model konseptual sebelumnya tanpa *Consent Management System*

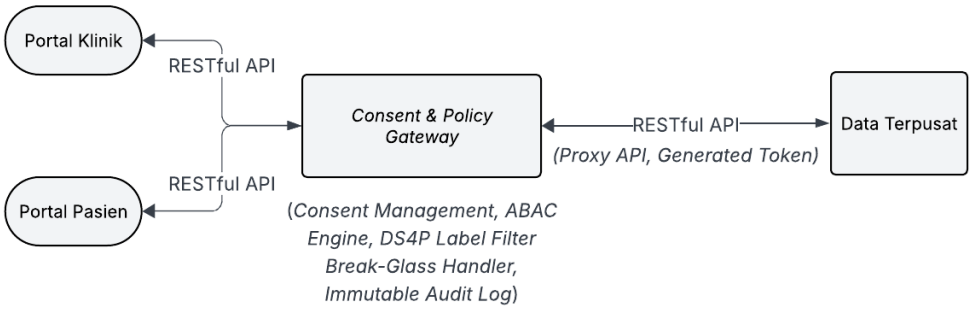
IV.2 Model Konseptual Solusi

Model konseptual solusi yang diusulkan menambahkan lapisan baru bernama *Consent & Policy Gateway* sebagai pengendali akses sebelum permintaan data mencapai server *FHIR*. Lapisan ini terdiri dari beberapa komponen inti yang meliputi *Consent Management*, *Policy Engine* berbasis *ABAC*, *DS4P Security Label Filter*, *Break-Glass Handler*, dan *Immutable Audit Log*.

Pada lapisan antarmuka, disediakan *Portal Pasien* untuk pengelolaan persetujuan granular dan *Portal Klinisi* untuk permintaan akses data. Seluruh permintaan, baik normal maupun darurat, harus melalui *gateway* ini untuk diverifikasi, diberikan keputusan akses, dan dicatat untuk keperluan audit.

Dengan demikian, solusi ini meningkatkan privasi, akuntabilitas, dan kepatuhan regulasi, sekaligus mempertahankan interoperabilitas *FHIR*.

Berikut adalah diagram alur data pada model konseptual solusi yang diusulkan dengan tambahan *Consent & Policy Gateway*:



Gambar IV.2 Model konseptual solusi dengan *Consent Management System*

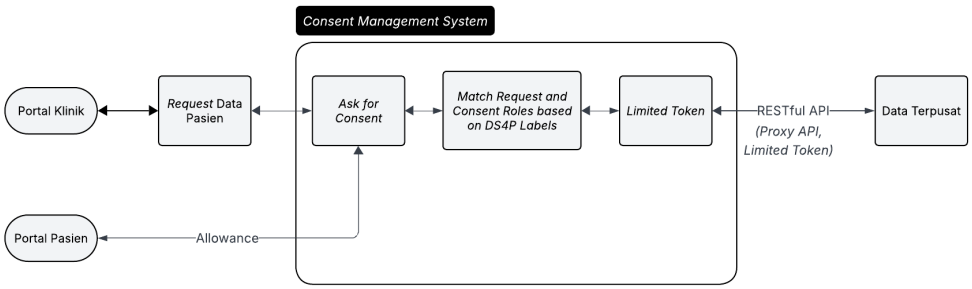
IV.2.1 Solusi *Consent Management System*

Sistem *Consent Management* dirancang untuk memberikan kontrol penuh kepada pasien terhadap siapa yang dapat mengakses data medis mereka, jenis data apa yang boleh diakses, serta untuk tujuan apa. Solusi ini memanfaatkan *FHIR Consent Resource*, di mana setiap persetujuan dicatat secara terstruktur dan dapat diperbarui secara dinamis oleh pasien.

Portal Pasien memungkinkan pasien memberikan persetujuan granular berbasis kategori data, misalnya rekam mental, data sensitif seksual, hasil laboratorium, catatan obat, dan kategori lainnya kepada pengguna di pihak klinis seperti dokter umum, psikiater, perawat, serta konteks penggunaan seperti perawatan aktif, penelitian, atau konsultasi lintas fasilitas.

Consent & Policy Gateway kemudian akan mencocokkan permintaan akses dari klinisi terhadap persetujuan yang tersimpan untuk menentukan apakah akses diperbolehkan atau ditolak. Dengan demikian, sistem ini menggantikan *general consent* dengan *fine-grained consent*, sekaligus mendukung prinsip transparansi dan *patient-centric care*.

Berikut adalah diagram alur solusi *Consent & Policy Gateway*:



Gambar IV.3 Model Solusi *Consent Management System*

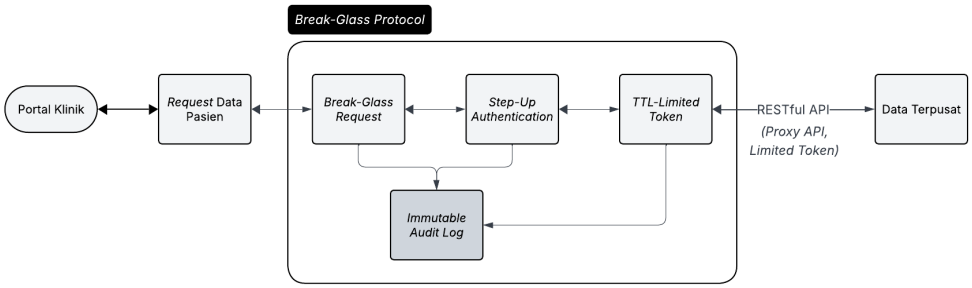
IV.2.2 Solusi Protokol *Break-Glass* (Akses Darurat)

Solusi *Break-Glass* dirancang untuk memberikan akses darurat yang cepat namun tetap akuntabel terhadap data pasien. Tidak seperti sistem tradisional yang hanya membuka seluruh akses, solusi ini menerapkan *ABAC (Attribute-Based Access Control)* untuk mengatur akses berdasarkan atribut kontekstual seperti status darurat, peran medis, hubungan dengan pasien, dan justifikasi klinis.

Ketika suatu permintaan akses ditolak karena tidak terdapat *consent*, sistem akan menampilkan opsi *"Break-Glass"*. Klinisi harus memberikan alasan tertulis, melakukan peningkatan autentikasi (misalnya *OTP*), dan menerima *Break-Glass Token* dengan batas waktu tertentu (*TTL*, misalnya 15 menit). Token ini hanya mengizinkan akses terhadap subset data tertentu dan tetap melalui pemeriksaan *DS4P* untuk mencegah akses ke kategori data yang sangat sensitif tanpa jalur legal yang sesuai.

Seluruh aktivitas selama sesi darurat dicatat ke dalam *immutable audit log* yang membentuk rantai *hash* untuk mendeteksi perubahan. Dengan demikian, mekanisme ini menjaga keseimbangan antara keselamatan pasien dan perlindungan privasi.

Berikut adalah diagram alur solusi *Break-Glass Protocol*:



Gambar IV.4 Model Solusi *Break-Glass Protocol*

BAB V

RENCANA SELANJUTNYA

V.1 Rencana Implementasi

Rencana implementasi Tugas Akhir ini mengikuti tahapan *Software Development Life Cycle (SDLC)* yang telah dijelaskan sebelumnya (perencanaan, analisis, desain, implementasi, dan pengujian), namun diterjemahkan menjadi rencana kerja terstruktur selama kurang lebih 12 minggu. Berikut adalah detail rencana implementasi yang ditampilkan dalam bentuk tabel *Gantt Chart*.

Tabel V.1 Rencana Implementasi Tahap Proposal *Gantt Chart*

Aktivitas	**Sep 2025**				**Okt 2025**				**Nov 2025**				**Des 2025**				**Jan 2026**			
Minggu	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Penentuan Topik dan Dosen Pembimbing																				
Eksplorasi Topik																				
Kajian Literatur Awal																				
Latar Belakang																				
Studi Literatur																				
Pendahuluan																				
Analisis Masalah																				
Desain Solusi																				
Rencana Selanjutnya																				
Pengumpulan Proposal																				
Seminar Proposal																				
Perancangan Arsitektur, Model Data, dan *Flow Policy*																				
Implementasi *Backend*																				

Tabel V.2 Rencana Implementasi Tahap Pengembangan *Gantt Chart*

Aktivitas	**Feb 2025**				**Mar 2025**				**Apr 2025**				**Mei 2025**				**Jun 2025**			
Minggu	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Implementasi Portal Pasien dan Klinik *(Frontend)*																				
Inisialisasi dan Integrasi dengan Server																				
Implementasi *Break-Glass* dan *Immutable Audit Log*																				
Unit Testing dan *System Integration Testing*																				
Penyempurnaan Sistem dan Dokumentasi Teknis																				
Penyusunan Laporan TA																				
Sidang Tugas Akhir																				

V.2 Perangkat Keras yang Digunakan

Implementasi sistem akan dilakukan menggunakan Apple MacBook Pro 16 Inch dengan chip M1 Pro, RAM 16 GB, dan penyimpanan 1 TB sebagai mesin utama pengembangan. Spesifikasi ini cukup untuk menjalankan *environment* pengembangan modern (*Node.js*, *Docker*, *database*, *code editor*) secara bersamaan tanpa *bottleneck* berarti. Berikut adalah daftar spesifikasi perangkat keras yang digunakan dalam bentuk tabel.

Tabel V.3 Perangkat Keras

Komponen	**Spesifikasi**
Model	Apple MacBook Pro 16-inch (M1 Pro)
Prosesor	Apple M1 Pro, 10-core CPU (8 performance cores, 2 efficiency cores), 16-core GPU, *16-core Neural Engine*
GPU	16-core GPU
Neural Engine	*16-core Neural Engine*
Memori	16 GB *unified memory*
Penyimpanan	1 TB SSD
Layar	16.2-inch Liquid Retina XDR, 3456 × 2234 pixel, P3 wide color, True Tone
Sistem Operasi	*macOS* terbaru (misalnya *macOS Sonoma*)
Konektivitas	Wi-Fi 6, Bluetooth 5.0
Port	3× Thunderbolt 4 (USB-C), HDMI, MagSafe 3, headphone jack, SDXC card slot

V.3 Perangkat Lunak dan Teknologi yang Digunakan

Pengembangan sistem akan menggunakan tumpukan teknologi web modern yang mendukung pengembangan cepat, modular, dan mudah diuji. Seluruh kode sumber akan dikelola menggunakan *Git* dengan repositori pada platform seperti *GitHub* atau *GitLab*. *Code editor* utama yang digunakan adalah Visual Studio Code dengan ekstensi pendukung *TypeScript* dan pengembangan *backend*. Berikut adalah daftar perangkat lunak pendukung untuk pengembangan dengan teknologi yang digunakan dalam bentuk tabel.

Tabel V.4 Perangkat Lunak dan Teknologi

Kategori	**Teknologi/Alat**	**Fungsi Utama**
Version Control	*Git* + *GitHub*/*GitLab*	Manajemen versi kode, kolaborasi, dan *backup* proyek
Backend	*Node.js* (*TypeScript*) + *NestJS*	Membangun *Consent & Policy Gateway* (*API*, *policy engine*, *break-glass logic*)
Frontend	*Next.js* (*React*, *TypeScript*) + *Tailwind CSS*	Membangun *Portal Pasien* dan *Portal Klinisi* berbasis web
Database	*PostgreSQL*	Penyimpanan *consent*, *policy*, sesi *break-glass*, dan *audit log*
API Testing	*Postman* / *Insomnia* / *Hoppscotch*	Pengujian *endpoint backend* dan verifikasi *response*
Container (opsional)	*Docker*	Menjalankan *FHIR server* atau *database* dalam *container* terisolasi
Code Editor	Visual Studio Code	Lingkungan utama penulisan dan *debugging* kode

V.4 Rencana Evaluasi

Rencana evaluasi sistem berfokus pada pengujian fungsional berdasarkan kebutuhan fungsional (FR-1 hingga FR-6) serta verifikasi perilaku sistem pada berbagai skenario akses seperti akses normal dengan *consent* yang valid, akses tanpa *consent*, dan akses menggunakan mekanisme *break-glass*. Pengujian dilakukan menggunakan pendekatan *black-box testing*, di mana fokus evaluasi berada pada masukan dan keluaran sistem tanpa mempertimbangkan implementasi internal.

Selain itu, dilakukan pula pengamatan sederhana terhadap kebutuhan nonfungsional, seperti waktu respon dan kelengkapan *audit log*, untuk memastikan bahwa sistem memenuhi ekspektasi minimal terkait performa dan *auditability*. Evaluasi ini memberikan dasar objektif untuk menilai apakah sistem telah berfungsi sesuai rancangan dan mampu mendukung kebutuhan klinis serta privasi pasien secara efektif. Berikut adalah daftar pengujian untuk membuktikan kebutuhan fungsional terpenuhi dalam bentuk tabel.

Tabel V.5 Rencana Pengujian Fungsional

ID	Deskripsi	Langkah Uji	Hasil yang Diharapkan
FR-1	Pengelolaan persetujuan pasien	1) Login sebagai pasien. 2) Membuat *consent* baru. 3) Menampilkan ulang *consent*.	*Consent* tersimpan di basis data, muncul pada daftar, dan detail sesuai input.
FR-2	Persetujuan granular berdasarkan jenis data dan *role*	1) Pasien membuat *consent* untuk dokter umum pada data laboratorium. 2) Dokter umum mencoba akses. 3) Psikiater mencoba akses yang sama.	Dokter umum diizinkan mengakses data laboratorium, sedangkan psikiater ditolak karena tidak sesuai *consent*.
FR-3	Penegakan *policy* dan label DS4P	1) Menandai suatu *FHIR Resource* dengan label DS4P. 2) Klinisi dengan atribut tidak valid mencoba akses. 3) Klinisi dengan atribut valid mencoba akses.	Akses pertama ditolak sesuai *policy*, akses kedua diizinkan sesuai kombinasi *consent* + *policy* + *DS4P*.
FR-4	*Break-Glass Access*	1) Klinisi mencoba mengakses data sensitif tanpa *consent*. 2) Klinisi mengaktifkan *Break-Glass*, mengisi alasan, dan melakukan OTP. 3) Klinisi mengakses data selama masa TTL.	Klinisi menerima *Break-Glass Token* dan dapat mengakses data sensitif dalam TTL, setelah TTL berakhir, akses ditolak.
FR-5	*Immutable Audit Trail*	1) Melakukan operasi akses normal dan *break-glass*. 2) Memeriksa tabel *audit log*. 3) Menjalankan verifikasi *hash-chain*.	Semua event tercatat lengkap dengan waktu, pengguna, dan tindakan; *hash-chain* valid dan tidak menunjukkan manipulasi.
FR-6	Portal Pasien & Portal Klinisi	1) Pasien login dan mengelola *consent*. 2) Klinisi login dan melakukan permintaan akses. 3) Mengamati kemudahan navigasi.	Kedua portal dapat digunakan tanpa error, seluruh fungsi utama berjalan dengan baik, dan antarmuka mudah dipahami.

V.5 Analisis Risiko

Sebagai bagian dari upaya memastikan pelaksanaan Tugas Akhir berjalan secara terukur dan terkendali, dilakukan proses *Risk Assessment* untuk mengidentifikasi risiko-risiko yang berpotensi menghambat penyelesaian proyek, baik dari sisi teknis, manajemen waktu, maupun lingkungan pengembangan. Setiap risiko dinilai berdasarkan besar dampak dan probabilitas terjadinya dengan skala 1–5, serta dirumuskan respons mitigasinya secara ringkas untuk meminimalkan pengaruh negatif terhadap proses implementasi. Berikut adalah daftar analisis risiko dalam bentuk tabel.

Tabel V.6 *Risk Assessment*

Kode	**Deskripsi Risiko**	**Dampak (1–5)**	**Probabilitas (1–5)**	**Risk Response**
R1	Kompleksitas integrasi *FHIR* dan *DS4P* yang berpotensi menyebabkan keterlambatan.	4	3	Fokus pada subset *FHIR Resource*; lakukan *spike* awal dan gunakan arsitektur modular.
R2	Implementasi *policy engine* dan mekanisme *break-glass* terlalu kompleks.	5	3	Lakukan implementasi bertahap, batasi skenario darurat, dan gunakan aturan sederhana terlebih dahulu.
R3	Perubahan kebutuhan dari pembimbing yang dapat menggganggu jadwal implementasi.	5	2	Kunci FR/NFR lebih awal, catat seluruh perubahan melalui *change log*, dan gunakan strategi *Git branching*.
R4	Risiko penggunaan data pasien nyata dalam pengujian.	5	2	Gunakan data dummy sepenuhnya dan lakukan verifikasi ulang terhadap dataset sebelum pengujian.
R6	Kerusakan *development environment* (*Node.js*, dependency, konfigurasi).	3	2	*Lock version*, gunakan *Docker*, dan dokumentasikan proses *setup* serta prosedur *restore*.

Risk Assessment ini berfungsi sebagai panduan untuk menjaga pekerjaan tetap berada dalam jalur yang realistis dan terkontrol. Dengan mengidentifikasi potensi risiko sejak awal dan menyiapkan strategi mitigasi yang spesifik, proses implementasi diharapkan dapat berjalan lebih stabil, minim hambatan, dan menghasilkan prototipe *Consent & Policy Gateway* yang sesuai dengan tujuan Tugas Akhir. Evaluasi risiko ini bersifat adaptif dan dapat diperbarui mengikuti dinamika pekerjaan maupun masukan dari pembimbing.

DAFTAR PUSTAKA

Ayaz, Muhammad, Muhammad Fermi Pasha, Mohammed Alzahrani, Rahmat Budiarto, dan Deris Stiawan. August 2021. "The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities (Preprint)" (). https://doi.org/10.2196/preprints.32869.

Carvalho, Marcelo, dan Paulo Bandiera-Paiva. February 2018. "Health Information System Role-Based Access Control Current Security Trends and Challenges". *Journal of Healthcare Engineering* 2018 (): 1–8. https://doi.org/10.1155/2018/6510249.

Cobrado, Usha Nicole, Suad Sharief, Noven Grace Regahal, Erik Zepka, Minnie Mamauag, dan Lemuel Clark Velasco. 2024. "Access control solutions in electronic health record systems: A systematic review". *Informatics in Medicine Unlocked* 49:101552. ISSN: 2352-9148. https://doi.org/https://doi.org/10.1016/j.imu.2024.101552. https://www.sciencedirect.com/science/article/pii/S2352914824001084.

de Oliveira, Marcela T., Yiannis Verginadis, Lúcio H.A. Reis, Evgenia Psarra, Ioannis Patiniotakis, dan Sílvia D. Olabarriaga. 2023. "AC-ABAC: Attribute-based access control for electronic medical records during acute care". *Expert Systems with Applications* 213:119271. ISSN: 0957-4174. https://doi.org/https://doi.org/10.1016/j.eswa.2022.119271. https://www.sciencedirect.com/science/article/pii/S0957417422022898.

HL7 International. 2025. "FHIR Data Segmentation for Privacy (DS4P) Implementation Guide". Diakses 25 September 2025. https://build.fhir.org/ig/HL7/fhir-security-label-ds4p/.

Kariotis, Timothy, Megan Prictor, Kathleen Gray, dan Shanton Chang. November 2023. “Patient Accessible Electronic Health Records and Information Practices in Mental Healthcare Contexts: A Scoping Review (Preprint)”. *Journal of Medical Internet Research* 27 (). https://doi.org/10.2196/54973.

Kementerian Kesehatan Republik Indonesia. 2025. “SATUSEHAT Platform – Keamanan dan Akses Data Pasien”. Diakses 25 September 2025. https://satusehat.kemkes.go.id/platform.

Sarode, Rashmi, Yutaka Watanobe, dan Subhash Bhalla. March 2023. “A Blockchain-Based Approach for Audit Management of Electronic Health Records”, 86–94. ISBN: 978-3-031-28349-9. https://doi.org/10.1007/978-3-031-28350-5_7.

Tabari, Parinaz, Gennaro Costagliola, Mattia De Rosa, dan Martin Boeker. March 2024. “State-of-the-Art FHIR-based Data Model and Structure Implementations: A Systematic Scoping Review (Preprint)”. *JMIR Medical Informatics* 12 (). https://doi.org/10.2196/58445.

Tuler de Oliveira, Marcela, Alex Bakas, Eugene Frimpong, Adrien Groot, Henk Marquering, Antonis Michalas, dan Silvia Olabarriaga. March 2020. “A break-glass protocol based on ciphertext-policy attribute-based encryption to access medical records in the cloud”. *Annals of Telecommunications* 75 (). https://doi.org/10.1007/s12243-020-00759-2.

Udayakumar, Padmavathi. July 2019. “A Research on impact of Blockchain in Healthcare”. *International Journal of Innovative Technology and Exploring Engineering* 8 (): 8. https://doi.org/10.35940/ijitee.I1007.0789S219.