

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	iv
DAFTAR TABEL	v
DAFTAR KODE	vi
I PENDAHULUAN	1
I.1 Latar Belakang	1
I.2 Rumusan Masalah	3
I.3 Tujuan	3
I.4 Batasan Masalah	3
I.5 Metodologi	4
II STUDI LITERATUR	6
II.1 <i>Break-Glass Protocol</i>	6
II.2 <i>Blockchain</i>	7
II.3 <i>Audit Trail</i>	7
II.4 Penelitian Terkait	8
II.4.1 Interoperabilitas Data Kesehatan dan Standar FHIR	8
II.4.2 Segmentasi Data Sensitif dan <i>Data Segmentation for Privacy (DS4P)</i>	9
II.4.3 Model Kontrol Akses pada Rekam Medis Elektronik: RBAC hingga ABAC	9
II.4.4 Akses Darurat dan Model AC-ABAC	10
II.4.5 <i>Consent Management</i> dan Peran Pasien	10
III ANALISIS MASALAH	11
III.1 Analisis Kondisi Saat Ini	11
III.2 Analisis Kebutuhan	12
III.2.1 Identifikasi Masalah Pengguna	12
III.2.2 Kebutuhan Fungsional	13
III.2.3 Kebutuhan Nonfungsional	14
III.3 Analisis Pemilihan Solusi	14
III.3.1 Alternatif Solusi	14
III.3.2 Analisis Penentuan Solusi	15
IV DESAIN KONSEP SOLUSI	17

IV.1 Model Konseptual Sebelumnya	17
IV.2 Model Konseptual Solusi	18
IV.2.1 Solusi <i>Consent Management System</i>	19
IV.2.2 Solusi Protokol <i>Break-Glass</i> (Akses Darurat)	20
V RENCANA SELANJUTNYA	21

DAFTAR GAMBAR

IV.1	Model konseptual sebelumnya <i>FHIR</i> tanpa <i>Consent Management System</i>	17
IV.2	Model konseptual solusi <i>FHIR</i> dengan <i>Consent Management System</i>	18
IV.3	Model Solusi <i>Consent Management System</i>	19
IV.4	Model Solusi <i>Break-Glass Protocol</i>	20

DAFTAR TABEL

III.1 Kebutuhan Fungsional	13
III.2 Kebutuhan Nonfungsional	14
III.3 Alternatif Solusi	14
III.4 Analisis Penentuan Solusi	15

DAFTAR KODE

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*, sehingga memungkinkan pertukaran data medis secara terstandar dan aman antar sistem yang heterogen (Ayaz dkk. 2021). Standar ini menggabungkan fleksibilitas teknologi web modern dengan model data klinis granular, menjadikannya fondasi utama interoperabilitas semantik pada berbagai sistem kesehatan global (Tabari dkk. 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 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 (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 (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 (Oliveira dkk. 2023). 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 (PA-EHR)* 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. 2025) 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, penerapan SATUSEHAT 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 da-

ta, 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.

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.

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. 2021).

Selain itu, penelitian Tabari dkk. (Tabari dkk. 2024) menunjukkan bahwa penerapan *FHIR* terbukti meningkatkan interoperabilitas semantik dan mempercepat pertukaran data antar sistem medis yang heterogen. Mereka mengidentifikasi dua model implementasi utama, yaitu model data *static* dan *dynamic*, serta menekankan bahwa *FHIR* membantu menghubungkan data dari berbagai sumber seperti rumah sakit, laboratorium, dan sistem riset klinis. Namun, terdapat tantangan utama berupa ketidakonsistenan pemetaan data, keterbatasan interoperabilitas semantik lintas sistem, dan kebutuhan pengelolaan privasi pasien yang lebih ketat. Hal ini menjadi dasar bahwa standar *FHIR* perlu dikombinasikan dengan kebijakan kontrol akses dan segmentasi data yang tepat agar keamanan tetap terjaga.

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 Jr. dan Bandiera-Paiva 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 (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.

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 (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. 2025) 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 <i>FHIR Consent</i> .
FR-2	Pemberian Persetujuan Granular	Pasien dapat menentukan akses berdasarkan jenis data, peran pengguna, dan tujuan penggunaan.
FR-3	<i>Policy Enforcement</i>	Sistem menegakkan kebijakan akses secara otomatis menggunakan <i>security labels DS4P</i> dan atribut pengguna.
FR-4	<i>Break-Glass Access</i>	Tenaga medis dapat melakukan akses darurat dengan autentikasi tambahan dan batas waktu.
FR-5	<i>Audit Trail</i>	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.

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	<i>RBAC Enhanced</i>	Pengembangan sistem berbasis peran dengan tambahan lapisan verifikasi pasien, namun tetap bersifat statis dan kurang adaptif terhadap konteks.
S-2	<i>ABAC Policy Engine</i>	Penerapan kontrol akses berbasis atribut dan integrasi <i>FHIR Consent</i> , mendukung granularitas tinggi pada keputusan akses.
S-3	<i>ABAC dengan DS4P dan Protokol Break-Glass</i>	Integrasi <i>Attribute-Based Access Control</i> untuk kondisi darurat, ditambah pelabelan <i>DS4P</i> serta mekanisme <i>audit</i> 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 <i>RBAC Enhanced</i>	S-2 <i>ABAC Policy Engine</i>	S-3 <i>ABAC + DS4P + Protokol Break-Glass</i>
Privasi Data	3	4	5
Transparansi & Auditabilitas	2	4	5
Kemudahan Implementasi	5	4	3
Kepatuhan terhadap Regulasi (<i>UU PDP 2022</i> , <i>Permenkes 24/2022</i>)	3	4	5
Dukungan <i>FHIR Consent</i>	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.

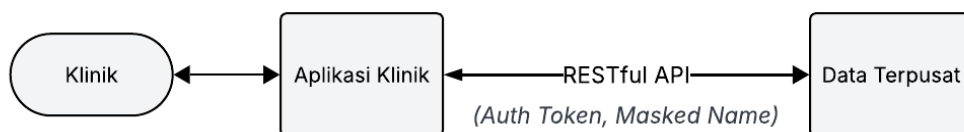
BAB IV

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.



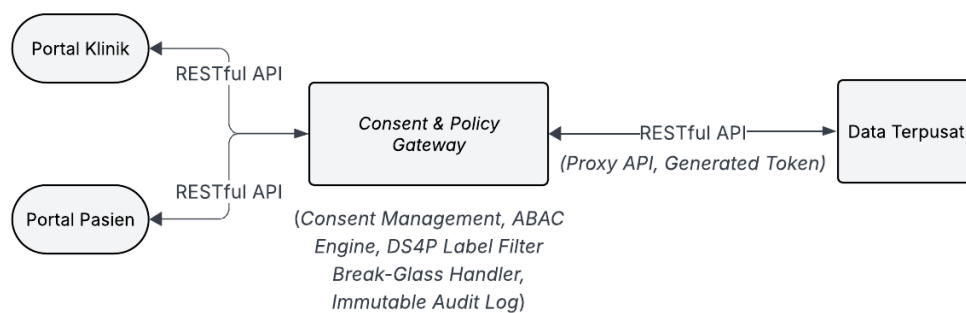
Gambar IV.1 Model konseptual sebelumnya *FHIR* tanpa *Consent Management System*

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*.



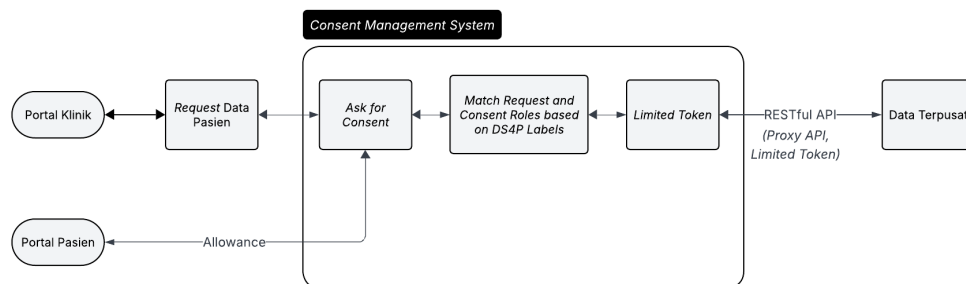
Gambar IV.2 Model konseptual solusi *FHIR* dengan *Consent Management System*

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*.



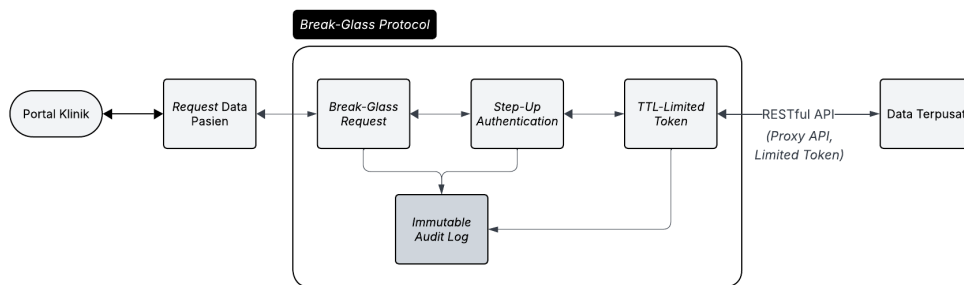
Gambar IV.3 Model Solusi *Consent Management System*

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.



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

BAB V

RENCANA SELANJUTNYA

Jelaskan secara detail langkah-langkah rencana selanjutnya, hal-hal yang diperlukan atau akan disiapkan, dan risiko dan mitigasinya, yang meliputi:

1. Rencana implementasi, termasuk alat dan bahan yang diperlukan, lingkungan, konfigurasi, biaya, dan sebagainya.
2. Desain pengujian dan evaluasi, misalnya metode verifikasi dan validasi.
3. Analisis risiko dan mitigasi, misalnya tindakan selanjutnya jika ada yang tidak berjalan sesuai rencana.

DAFTAR PUSTAKA

- Ayaz, Muhammad, Muhammad Ammad-Uddin, Zaigham Abbas, K. Saad, Daniyal Alhussain, dan P. R. Florina. 2021. "The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities". *JMIR Medical Informatics* 9 (7): e21929. <https://doi.org/10.2196/21929>. <https://doi.org/10.2196/21929>.
- Carvalho Jr., Marcelo A. de, dan Paulo Bandiera-Paiva. 2018. "Health Information System Role-Based Access Control – Current Security Trends and Challenges". *Journal of Healthcare Engineering* 2018 (3): 1–8. <https://doi.org/10.1155/2018/6510249>. <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* 54:101372. <https://doi.org/10.1016/j.imu.2024.101552>. <https://doi.org/10.1016/j.imu.2024.101552>.
- HL7 International. 2025. "FHIR Data Segmentation for Privacy (DS4P) Implementation Guide". Diakses 25 September 2025.
- Kariotis, Theodoros, L. Jennifer, H. Martin, dan W. Patrick. 2025. "Patient Accessible Electronic Health Records and Information Practices in Mental Health Care Contexts: Scoping Review". Accessed 25 September 2025, *International Journal of Medical Informatics* 195:105634. <https://doi.org/10.2196/54973>. <https://doi.org/10.2196/54973>.
- Kementerian Kesehatan Republik Indonesia. 2025. "SATUSEHAT Platform – Keamanan dan Akses Data Pasien". Diakses 25 September 2025.

- Oliveira, Matheus T. de, Yannis Verginadis, Luciana H. A. Reis, Eleni Psarra, Ilias Patiniotakis, dan S. D. Olabarriaga. 2023. “AC-ABAC: Attribute-Based Access Control for Electronic Medical Records during Acute Care”. *Expert Systems with Applications* 213:119271. <https://doi.org/10.1016/j.eswa.2022.119271>. <https://doi.org/10.1016/j.eswa.2022.119271>.
- 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. 2024. “State-of-the-Art Fast Healthcare Interoperability Resources (FHIR)–Based Data Model and Structure Implementations: Systematic Scoping Review”. Accessed 25 September 2025, *JMIR Medical Informatics* 12 (1): e58445. <https://doi.org/10.2196/58445>. <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>.