

**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
<Bulan> 2025**

**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

Telah disetujui dan disahkan sebagai Proposal Tugas Akhir
di Bandung, pada tanggal <tanggal>

Pembimbing,

Dr. Ir. Rinaldi Munir, M. T.
NIP 19651210 199402 1 001

DAFTAR ISI

| | |
|--|------------|
| DAFTAR ISI..... | iii |
| DAFTAR LAMPIRAN | v |
| DAFTAR GAMBAR..... | vi |
| DAFTAR TABEL | vii |
| BAB I PENDAHULUAN..... | 1 |
| I.1 Latar Belakang..... | 1 |
| I.2 Rumusan Masalah..... | 3 |
| I.3 Tujuan | 4 |
| I.4 Batasan Masalah | 4 |
| I.5 Metodologi..... | 5 |
| BAB II STUDI LITERATUR | 7 |
| II.1 Interoperabilitas Data Kesehatan dan Standar FHIR | 7 |
| II.2 Segmentasi Data Sensitif dan Data Segmentation for Privacy (DS4P) | 8 |
| II.3 Model Kontrol Akses pada Rekam Medis Elektronik: RBAC hingga ABAC | 8 |
| II.4 Akses Darurat dan Model AC-ABAC | 9 |
| II.5 <i>Consent Management</i> dan Peran Pasien | 9 |
| BAB III ANALISIS MASALAH | 10 |
| III.1 Analisis Kondisi Saat Ini | 10 |

| | | |
|---|-------------------------------------|-----------|
| III.2 | Analisis Kebutuhan | 11 |
| III.2.1 | Identifikasi Masalah Pengguna | 11 |
| III.2.2 | Kebutuhan Fungsional | 12 |
| III.2.3 | Kebutuhan Nonfungsional | 13 |
| III.3 | Analisis Pemilihan Solusi..... | 13 |
| III.3.1 | Alternatif Solusi..... | 13 |
| III.3.2 | Analisis Penentuan Solusi..... | 14 |
| BAB IV DESAIN KONSEP SOLUSI..... | | 16 |
| BAB V RENCANA SELANJUTNYA | | 20 |
| DAFTAR PUSTAKA | | 29 |
| LAMPIRAN A JUDUL LAMPIRAN | | 31 |

DAFTAR LAMPIRAN

Lampiran A. Contoh Judul Lampiran.....Error! Bookmark not defined.

A.1 Contoh Judul Anak Lampiran.....31

DAFTAR GAMBAR

Gambar II.1 Tahapan konstruksi koleksi retorik kalimat**Error! Bookmark not defined.**

DAFTAR TABEL

Tabel II.1 Pengelompokan nomor *Tag MARC-21 Error! Bookmark not defined.*

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 dapat direpresentasikan dalam bentuk sumber daya seperti pasien, observasi, dan kondisi, 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 di 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 menjadi komponen fundamental dalam perlindungan data pasien karena memastikan hanya pengguna berwenang yang dapat membaca, memodifikasi, atau membagikan informasi medis. Namun, penelitian sistematis menunjukkan bahwa sebagian besar sistem rekam medis elektronik (RME) masih menghadapi kendala dalam aspek otorisasi, akuntabilitas, dan akses darurat, serta minim dukungan terhadap mekanisme manajemen persetujuan pasien yang efektif (Cobrado dkk. 2024). Model tradisional seperti *Role-Based Access Control* (RBAC) dinilai tidak memadai untuk menangani konteks klinis dinamis yang memerlukan keputusan akses berdasarkan kondisi pasien, lokasi, dan 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 (de 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* (PAEHR) dan *patient portal* memperkuat paradigma perawatan yang berpusan 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 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 menegakkan 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 kripto 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 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 penggeraan.

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 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. (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 ketidakkonsistenan 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.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 (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.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 de 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 Tall dkk. (2023), ABAC memungkinkan keputusan akses spesifik yang mempertimbangkan situasi waktunya, seperti lokasi pengguna atau status darurat pasien. Fleksibilitas inilah yang membuat ABAC lebih cocok untuk sistem rekam medis elektronik yang kompleks.

II.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.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 yang 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.

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 menjelaskan kebutuhan-kebutuhan tersebut.

III.2.2 Kebutuhan Fungsional

Berikut adalah kebutuhan fungsional yang disajikan dalam bentuk tabel:

Tabel III.2.2 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 fungsional yang disajikan dalam bentuk tabel:

Tabel III.2.3 Kebutuhan Fungsional

| Kode | Kebutuhan Non-Fungsional | Deskripsi |
|--------------|--------------------------|--|
| NFR-1 | Keamanan | Sistem menggunakan autentikasi dan <i>hashing audit</i> 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.3.1 Kebutuhan Fungsional

| Kode | Alternatif Solusi | Deskripsi Singkat |
|------------|----------------------------------|--|
| S-1 | <i>RBAC Enhanced</i> | Pengembangan sistem berbasis peran dengan tambahan lapisan verifikasi pasien, namun masih bersifat statis. |
| S-2 | <i>ABAC Policy Engine</i> | Penerapan kontrol akses berbasis atribut dan integrasi FHIR Consent, mendukung granularitas tinggi. |

| | | |
|------------|--|---|
| S-3 | ABAC dengan DS4P dan Protokol <i>Break-Glasss</i> | Integrasi <i>Attribute-Based Access Control</i> kontekstual untuk kondisi darurat serta pelabelan DS4P dan audit yang tak 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.3.1 Analisis Penentuan Solusi

| Kriteria Penilaian | S-1 RBAC Enhanced | S-2 ABAC Policy Engine | S-3 ABAC dengan DS4P dan Protokol <i>Break-Glasss</i> |
|------------------------------|-------------------|------------------------|---|
| 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 | 3 | 5 |
| 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-Glasss*) 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.

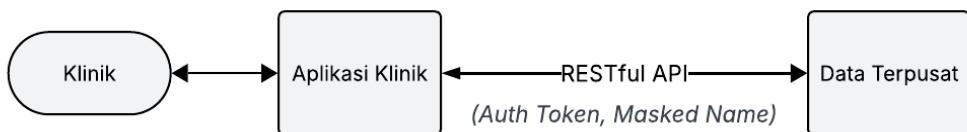
BAB IV

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 (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.

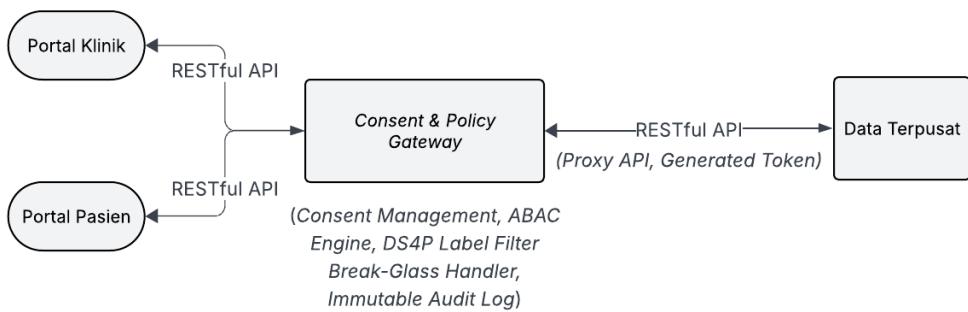
Di sisi privasi, perlindungan hanya dilakukan melalui *masking* sederhana pada tampilan nama pasien, misalnya “Irf** Mus****,” tanpa segmentasi data sensitif atau kebijakan keamanan berbasis metadata. Tidak terdapat mekanisme penegakan kebijakan (*policy enforcement*), pengelolaan persetujuan granular,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



Gambar IV.1.1 *Flow Diagram* Konseptual Sebelumnya

IV.2 Model Konseptual Solusi

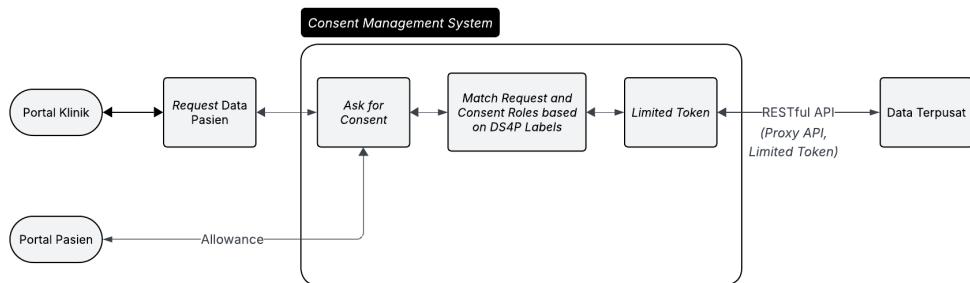
Model konseptual solusi yang diusulkan menambahkan lapisan baru bernama *Consent & Policy Gateway* sebagai pengendali akses sebelum permintaan data mencapai server FHIR. Lapisan ini terdiri dari beberapa komponen inti yang berisi *Consent Management, Policy Engine* berbasis ABAC, DS4P *Security Label 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, diberi keputusan akses, dan dicatat untuk audit. Dengan demikian, solusi ini meningkatkan privasi, akuntabilitas, dan kepatuhan regulasi, sekaligus mempertahankan interoperabilitas FHIR.



Gambar IV.2.1 *Flow Diagram* Konseptual Solusi

IV.2.1 Solusi *Consent Management System*

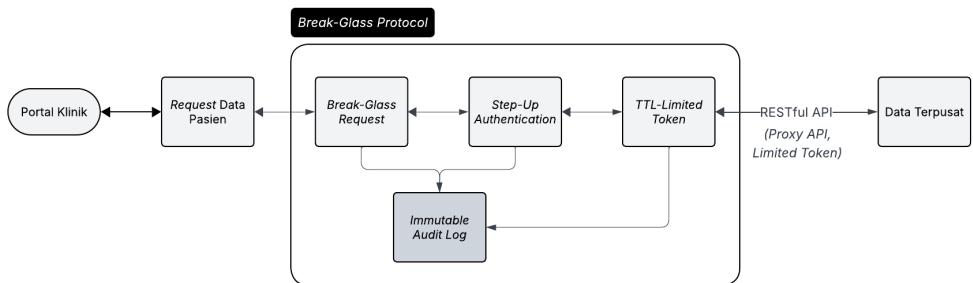
Sistem *Consent Management* dirancang untuk memberikan kontrol penuh kepada pasien terhadap siapa yang dapat mengakses data medis mereka, jenis data apa yang boleh diakses, serta untuk tujuan apa. Solusi ini memanfaatkan FHIR *Consent Resource*, di mana setiap persetujuan dicatat secara terstruktur dan 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 lainnya ke pengguna di pihak klinis seperti dokter umum, psikiater, perawat, serta konteks penggunaan perawatan aktif, penelitian, konsultasi lintas fasilitas. *Gateway* akan mencocokkan permintaan klinisi terhadap persetujuan yang tersimpan untuk menentukan apakah akses diperbolehkan. Sistem ini menggantikan *general consent* dengan *fine-grained consent*, mendukung prinsip transparansi dan *patient-centric care*.



Gambar IV.2.2 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 semua 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 ada consent, sistem menampilkan opsi "*Break-Glass*". Klinisi harus memberikan alasan tertulis, melakukan peningkatan autentikasi (misalnya OTP), dan menerima *Break-Glass Token* berbatas waktu (TTL, misalnya 15 menit). Token ini hanya mengizinkan subset data tertentu dan selalu melewati pemeriksaan DS4P untuk mencegah akses ke kategori data super sensitif tanpa jalur hukum tertentu. Semua aktivitas selama sesi darurat dicatat ke *immutable audit log* yang membentuk rantai *hash* untuk mendeteksi perubahan. Dengan demikian, mekanisme ini menjaga keseimbangan antara keselamatan pasien dan perlindungan privasi.



Gambar IV.2.3 Solusi Protokol *Break-Glass*

BAB V

RENCANA SELANJUTNYA

V.1 Rencana Implementasi

Rencana implementasi Tugas Akhir ini mengikuti tahapan (*Software Development Life Cycle*) SDLC yang sudah dijelaskan sebelumnya (perencanaan, analisis, desain, implementasi, dan pengujian), tetapi 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

| Aktivitas | Sep 2025 | | | Okt 2025 | | | | Nov 2025 | | | | Des 2025 | | | | Jan 2025 | | | |
|---------------------------------------|----------|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|----------|---|---|---|
| Penentuan Topik dan Dosen Pembimbing | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| Tahap Penggeraan Proposal Tugas Akhir | | | | | | | | | | | | | | | | | | | |
| Eksplorasi Topik dan Pemetaan Masalah | | | | | | | | | | | | | | | | | | | |
| Kajian Literatur Awal | | | | | | | | | | | | | | | | | | | |
| Latar Belakang dan Rumusan Masalah | | | | | | | | | | | | | | | | | | | |
| Studi Literatur | | | | | | | | | | | | | | | | | | | |

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.

Tabel V.2 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) |
| 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, jack audio, 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 di platform seperti GitHub atau GitLab. Code editor utama yang digunakan adalah Visual Studio Code dengan ekstensi pendukung TypeScript dan pengembangan backend.

Tabel V.3 Perangkat Lunak dan Teknologi

| Kategori | Teknologi / Alat | Fungsi Utama |
|-----------------------------|--|--|
| <i>Version Control</i> | Git + GitHub/GitLab | Manajemen versi kode, kolaborasi, dan backup proyek |
| <i>Backend</i> | Node.js + NestJS (TypeScript) | Membangun Consent & Policy Gateway (API, policy engine, break-glass logic) |
| <i>Frontend</i> | Next.js (React, TypeScript) + Tailwind CSS | Membangun Portal Pasien & Portal Klinisi berbasis web |
| <i>Database</i> | PostgreSQL | Penyimpanan consent, policy, sesi break-glass, dan audit log |
| <i>API Testing</i> | Postman / Insomnia / Hoppscotch | Pengujian endpoint backend dan verifikasi response |
| <i>Container (opsional)</i> | Docker | Menjalankan FHIR server atau DB dalam container terisolasi |
| <i>Code Editor</i> | 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 s.d. FR-6) dan 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 dengan pendekatan *black-box testing*, di mana fokusnya adalah pada *input* dan *output* dari sistem, bukan implementasi internal. Selain itu, dilakukan pula pengamatan sederhana terhadap kebutuhan nonfungisional misalnya waktu respon dan kelengkapan audit log untuk memastikan sistem memenuhi ekspektasi dasar performa dan auditabilitas.

Tabel V.4 Tabel Pengujian

| ID FR | Deskripsi Pengujian | Langkah Uji | Hasil yang Diharapkan |
|-------|--|---|---|
| FR-1 | Pengelolaan persetujuan pasien | 1) Login sebagai pasien di Portal Pasien. 2) Membuat consent baru (pilih jenis data dan role). 3) Menyimpan dan menampilkan ulang daftar consent. | Consent baru tersimpan di basis data, muncul di daftar consent, dan detailnya sesuai input pasien. |
| FR-2 | Persetujuan granular berdasarkan jenis data/role | 1) Pasien membuat consent hanya untuk dokter umum mengakses data laboratorium. 2) Klinisi (dokter umum) mencoba akses data lab. 3) Klinisi lain (mis. psikiater) mencoba akses yang sama. | Dokter umum diizinkan mengakses data laboratorium, sedangkan klinisi lain ditolak dengan pesan bahwa consent tidak mengizinkan akses. |

| | | | |
|------|---------------------------------|--|--|
| FR-3 | Penegakan policy dan DS4P label | 1) Tandai suatu resource FHIR dengan label DS4P “SENSITIVE”. 2) Klinisi dengan atribut yang tidak memenuhi policy mencoba akses. 3) Klinisi dengan atribut yang valid mencoba akses. | Akses pertama ditolak (policy deny), akses kedua diizinkan. Keputusan akses mengikuti kombinasi consent + policy + label DS4P. |
| FR-4 | Break-Glass Access | 1) Klinisi mencoba akses data sensitif tanpa consent → ditolak. 2) Klinisi menekan tombol “Break-Glass”, mengisi alasan, dan melakukan OTP. 3) Mengakses kembali data selama TTL. | Setelah OTP valid, klinisi mendapatkan Break-Glass Token dan dapat mengakses data sensitif hanya selama jangka waktu tertentu; setelah TTL habis, akses ditolak. |
| FR-5 | Audit Trail immutable | 1) Lakukan beberapa operasi akses (normal dan break-glass). 2) Periksa tabel audit log. 3) Jalankan fungsi verifikasi hash-chain. | Semua event tercatat dengan user, waktu, dan action yang tepat. Verifikasi hash-chain menyatakan log valid (tidak terdeteksi manipulasi). |
| FR-6 | Portal Pasien & Portal Klinisi | 1) Pasien login dan mengelola consent. 2) Klinisi login dan melakukan permintaan akses. 3) Observasi kemudahan navigasi fitur utama. | Kedua portal dapat diakses, fungsi utama (kelola consent, permintaan akses) berjalan, dan antarmuka dapat digunakan tanpa error kritis. |

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.

Tabel V.5 *Risk Assessment*

| Kode | Deskripsi Risiko | Dampak (1–5) | Probabilitas (1–5) | <i>Risk Response</i> |
|-----------|---|-----------------|-----------------------|---|
| R1 | Kompleksitas integrasi FHIR + DS4P menyebabkan keterlambatan | 4 | 3 | Fokus pada <i>subset resource</i> FHIR; lakukan <i>spike</i> awal & modular. |
| R2 | Implementasi <i>policy engine</i> & <i>break-glass</i> terlalu kompleks | 5 | 3 | Implementasi bertahap, batasi skenario darurat, gunakan <i>rule</i> sederhana dulu. |
| R3 | Perubahan kebutuhan dari pembimbing | 5 | 2 | Kunci FR/NFR lebih awal, catat <i>change log</i> , gunakan Git <i>branching</i> . |

| | | | | |
|-----------|---|---|---|---|
| R4 | Risiko penggunaan data pasien nyata | 5 | 2 | Gunakan data dummy sepenuhnya, verifikasi ulang dataset. |
| R6 | Kerusakan <i>environment</i> (Node.js, DB, dependency conflict) | 3 | 4 | Lock version, gunakan Docker, dokumentasikan <i>setup & restore</i> . |

Risk assessment ini berfungsi sebagai panduan untuk menjaga pekerjaan tetap berada dalam jalur yang realistik 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 Ammad-Uddin, Zaigham Abbas, K. Saad, Daniyal Alhussain, dan Florina P. R. 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>
- 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>
- de Oliveira, Matheus T., 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>
- Kariotis, Theodoros, Jennifer L., Martin H., dan Patrick W. 2025. “Patient-Accessible Electronic Health Records and Information Practices in Mental Health Care Contexts: Scoping Review.” International Journal of Medical Informatics 195: 105634. Diakses 25 September 2025. <https://doi.org/10.2196/54973>
- 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.” JMIR Medical Informatics 12(1): e58445. Diakses 25 September 2025. <https://doi.org/10.2196/58445>

de Carvalho Jr., Marcelo A., 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>.

LAMPIRAN A

JUDUL LAMPIRAN

A.1 Contoh Judul Anak Lampiran

Contoh anak lampiran