Technical Guidelines and Requirements Document for FHIR Infrastructure Implementation

Contents

[1. Introduction 3](#_Toc166014350)

[1.1. Goal 3](#_Toc166014351)

[1.2. Covered Scenarios: 3](#_Toc166014352)

[1.2.1. Scenario A (**mandatory**) 3](#_Toc166014353)

[1.2.2. Scenario B (**mandatory**) 4](#_Toc166014354)

[1.2.3. Optional scenarios 4](#_Toc166014355)

[1.3. Supplementary Remarks 4](#_Toc166014356)

[2. Conventions 5](#_Toc166014357)

[3. Infrastructure 5](#_Toc166014358)

[3.1. General requirements 5](#_Toc166014359)

[3.2. National infrastructure 5](#_Toc166014360)

[3.2.1. Registries and Directories 5](#_Toc166014361)

[3.2.2. Sandbox 6](#_Toc166014362)

[3.3. FHIR REST API 6](#_Toc166014363)

[3.4. Notifications and Subscriptions 7](#_Toc166014364)

[3.5. Performance and availability requirements 7](#_Toc166014365)

[3.6. Terminology Services 7](#_Toc166014366)

[3.7. FHIR Profile Validation 7](#_Toc166014367)

[3.8. Authorization Server 8](#_Toc166014368)

[4. Security & Privacy 8](#_Toc166014369)

[4.1. General requirements 8](#_Toc166014370)

[4.2. FHIR-specific Audit and Logging requirements 8](#_Toc166014371)

[4.3. Authentication/Authorization 8](#_Toc166014372)

[4.3.1. Basic Preconditions and Client Authentication 9](#_Toc166014373)

[4.3.2. Common SMART on FHIR guidelines 10](#_Toc166014374)

[4.3.3. Access Control and Enforcement Guidelines 13](#_Toc166014375)

[4.3.4. Access Scenarios 14](#_Toc166014376)

[4.4. Data Minimization Guidelines 15](#_Toc166014377)

[4.5. Security Guidelines for Large Objects 16](#_Toc166014378)

[Appendix A – National Registries API details 16](#_Toc166014379)

[Appendix B – Related Documents 16](#_Toc166014380)

[1. Conceptual Overview of Healthcare Data Portability 16](#_Toc166014381)

[2. Implementation Stages 16](#_Toc166014382)

[3. Information Requirements 17](#_Toc166014383)

[4. REST API Guidelines and Requirements 17](#_Toc166014384)

[5. Certification Process 17](#_Toc166014385)

[6. FHIR Schema Validation Approaches (Informational) 17](#_Toc166014386)

[7. FHIR Attachment Handling Approaches (Informational) 17](#_Toc166014387)

[8. Sub-resource Access Control Approaches (Informational) 17](#_Toc166014388)

[9. Guidelines for Digitally Signing FHIR Payloads 17](#_Toc166014389)

[10. IL-CORE IG 18](#_Toc166014390)

[11. Patient Consent Manager (PCM) Overview (Informational) 18](#_Toc166014391)

[12. Reference architecture (Informational) 18](#_Toc166014392)

[13. General Security Requirements 18](#_Toc166014393)

# Introduction

## Goal

This document provides technical guidelines and requirements for implementing FHIR infrastructure in healthcare organizations (henceforth - the organizational FHIR platform). It addresses key areas such as Infrastructure, Security, and Privacy, and directs readers to additional documents that cover related topics such as *Information buckets*, REST API requirements, and more.

The goal of these requirements is to ensure that healthcare organizations provide a consistent, secure, and scalable FHIR API interface that supports a wide range of clinical data exchange scenarios, both current and future, thereby enhancing operational flexibility and promoting rapid innovation.

## Covered Scenarios:

These technical guidelines primarily address the following two scenarios of healthcare data sharing.

The organizational FHIR platform **SHALL** support *Scenario A* at *Stage I* (as defined in [*[B.2] Implementation Stages document*](#_Implementation_Stages)).

The organizational FHIR platform **SHALL** support *Scenario B* at *Stage III* (as defined in [*[B.2] Implementation Stages document*](#_Implementation_Stages)).

### Scenario A (**mandatory**)

Data sharing between healthcare organizations based on out-of-band agreement

This scenario covers the secure and standardized exchange of healthcare data between two or more healthcare organizations based on a pre-established, out-of-band agreement. The specifics of the data shared are determined by the participating organizations and fall outside the scope of this document. The technical infrastructure outlined here enables secure and efficient data exchange once agreements are in place.

#### Examples:

* Smart Discharge:   
  Streamlining the transition of care by transmitting structured discharge recommendations upon hospital release. This allows for automation and semi-automation of processes like medication approval, referral scheduling, and more.
* Smart Admission:   
  Enhancing patient intake efficiency by electronically transferring a patient's medical history in a structured format upon admission. This allows the admitting doctor to expedite the patient intake process by having access to essential details such as chronic illnesses and prescribed medications.

### Scenario B (**mandatory**)

Data sharing between healthcare organizations based on centrally managed patient's consent

This scenario enables data sharing in a fashion similar to *Scenario A*. However, in this instance, the process does not require individual agreements between organizations. Instead, it operates on the basis of centrally managed patient consent.  
Under this model, the patient grants permission to a service provider, enabling them to access information from various sources withing specific *Information Buckets*.

### Optional scenarios

Additionally, organizational FHIR platform built according to these guidelines can enable other (optional) scenarios.

#### Examples:

* Locally Managed Patient Consent:   
  This scenario enables healthcare organizations to share data based on patient consent managed locally within each organization. For example - a healthcare organization that decides to establish an app store for patients and wants to allow its patients to share information with apps that the organization has chosen to include in the store.
* Practitioner-Focused Applications:   
  The organizational FHIR platform can empower the development of dedicated applications tailored to the needs of healthcare practitioners. These applications could leverage the platform to enhance clinical workflows, improve decision-making, and ultimately, patient care.

## Supplementary Remarks

An effort was made to align these requirements with the capabilities of common platforms used in Israeli healthcare ecosystem to simplify the implementation process. However, this document intentionally avoids prescribing specific platforms, architectures, or strategies, leaving those choices to each organization’s discretion.

This current version of this document explicitly addresses requirements and provides guidelines for *Scenario A*. Additional guidelines and requirements applicable to Scenario B will be provided in the subsequent versions of this document.

A supplementary document offering a broad overview of the Scenario B scope and Patient Consent Manager (PCM) is provided for reference (see [*[B.11] PCM Overview document*](#_Patient__)).

It is important to note that the requirements and guidelines outlined in this version of the document, as well as its future iterations, are designed to progressively lay the foundation for *Scenario A* and subsequently *Scenario B*. Along the way, they also support the implementation of other (optional) scenarios.

The requirements set forth in this document are based on established standards, such as HL7 FHIR and SMART on FHIR. Where these standards provide adequate and explicit guidance, this document will refer directly to them.

# Conventions

* This document uses the conformance verbs **SHALL**, **SHOULD**, and **MAY** as defined in HL7 FHIR documentation (<https://hl7.org/fhir/R4/conformance-rules.html#conflang>). They are to be interpreted as such when, and only when, they appear in all capitals and in bold, as shown here.
* Hyperlinks within this document are denoted by *blue underlined text italicized*.
* Hyperlinks to external resources are denoted by blue underlined text.
* *Italicized* text is used to highlight specific concepts or data fields within the document.
* **Bold underlined** text is used to emphasize specific topics of importance.

# Infrastructure

The following section outlines infrastructure components and requirements for the organizational FHIR infrastructure.

## General requirements

Healthcare Organizations **SHALL** plan and build their FHIR infrastructure as key operational system, with all the relevant implications on availability, redundancy, reliability, monitoring, etc.

## National infrastructure

To facilitate interoperability, several infrastructure components will be provided on the national level. Those components will be centrally maintained and supported.

### Registries and Directories

Several national registries/directories will be provided as described below. Those registries/directories will provide both API access as well as web interface for implementers.

Below is the list of registries/directories relevant for *Scenario A* [scope](#_Scenario_A_(mandatory)). These registries/directories will be augmented, and additional registries/directories will be introduced to support *Scenario B*.

See [*Appendix A*](#_Appendix_A_–) for more details.

#### National Public Key Directory (PKD)

Every organization **SHALL** enroll in this directory to participate in FHIR based information exchange – both as a client and as a server. All information in this directory will be public (i.e. – available for consumption via API and via web interface without authentication)

##### The directory will include the following fields:

* Organization name
* Unique organization identifier
* General contact details
* Contact details for security and privacy issues
* Service label
  + Organization **MAY** use several certificates or expose several FHIR Server REST API endpoints. Service labels are used to distinguish between them.
* Entry type (client or server)
  + Note that organization can be both client and server. In such case there **SHALL** be separate entries for each role.
* client\_id – (for client role, as defined in  [RFC 6749: The OAuth 2.0 Authorization Framework](https://tools.ietf.org/html/rfc6749#section-4.1.3)) - generated by the directory and returned to the client during registration process
* redirect\_uri - (for client role, as defined in  [RFC 6749: The OAuth 2.0 Authorization Framework](https://tools.ietf.org/html/rfc6749#section-4.1.3), **optional**)
* FHIR Server REST API endpoint URL (for server role)
* Organization public key in a JSON Web Key (JWK) structure presented within a JWK Set, as defined in [JSON Web Key Set (JWKS)](https://tools.ietf.org/html/rfc7517).
  + See [*[4.3.1.1] Certificates issuance process*](#_Certificates__requirements) for details on specific certificate requirements and explanation of the process for obtaining, registering and maintaining the certificate

### Sandbox

National Sandbox environment will be provided to facilitate testing of both client and server implementations. Additional details will be provided in the subsequent versions of this document.

## FHIR REST API

Organizational FHIR platform **SHALL** support **all** FHIR REST API functionality defined in the [*[B.4] REST API Guidelines and Requirements document*](#_REST_API_Guidelines) (and accompanying *CapabilityStatement* requirements resource) according to [HL7 FHIR specifications](https://hl7.org/fhir/R4/http.html).

Organizational FHIR platform **SHOULD** also support FHIR REST API functionality not required by the [[[*[B.4] REST API Guidelines and Requirements document*](#_REST_API_Guidelines)](#_REST_API_Guidelines)](#_REST_API_Guidelines)but defined in [HL7 FHIR specifications](https://hl7.org/fhir/R4/http.html).

Organizational FHIR platform **MAY** also support additional functionality that extends the standard FHIR REST API in accordance with FHIR standard (e.g. – custom extended operations)

Organizational FHIR platform **MAY** implement FHIR REST API as part of its EHR system or as a separate component, if all other requirements (i.e. data freshness, performance, API support, security, etc.) are satisfied.

Organizational FHIR platform **MAY** choose to use full FHIR server, a façade, or a combination approach, if all other requirements (i.e. data freshness, performance, API support, security, etc.) are satisfied. Furthermore, it is recommended to review the [*[B.3] Information Requirements document*](#_Information_Requirements), as it may have implications for the choice of architecture.

Organizational FHIR platform **MAY** also support additional modalities (e.g. – messaging), consumption and export of file-based FHIR data via Data Vaults, BULK FHIR, etc. However, this is not part of the required functionality and is not addressed by this document.

## Notifications and Subscriptions

FHIR specifications [define](https://hl7.org/fhir/R4/subscription.html) subscriptions mechanisms that enable push-based change notifications. *Scenario A* scope (as described [*here*](#_Scenario_A_(mandatory))) does not define specific requirements for subscriptions support. However, for *Scenario B* support for push-based notifications will be required as part of PCM.

Additional details will be provided in the subsequent versions of this document.

## Performance and availability requirements

Organizational FHIR platform **SHALL** maintain a minimum annual uptime of **99.95%**.

Organizational FHIR platform **SHALL** meet the following performance targets for 100 concurrent FHIR REST API requests:

* 95th percentile of FHIR REST API responses **SHALL** be returned within **200 milliseconds**.
* 99th percentile of FHIR REST API responses **SHALL** be returned within **2000 milliseconds**.

Note that these requirements only define the criteria for the FHIR platform's uptime, response times, and concurrency. Data latency requirements (i.e. - time between data updates in the source system and their availability via FHIR REST API) are defined in the [*[B.3] Information Requirements document*](#_Information_Requirements).

## Terminology Services

Organizational FHIR platform **SHOULD** include Terminology Services infrastructure that will enable:

* Structured management of organizational terminology assets (i.e. code systems, value sets, maps, etc.)
* Operational terminology scenarios (i.e. – translation of codes between code systems, subsumption testing and resolution, value set expansion, etc.)

Effective management of terminology is crucial for the successful implementation of a FHIR platform.

## FHIR Profile Validation

Organizational FHIR platform **MAY** include FHIR profile validation component to ensure compliance with national (i.e. – [*[B10] IL-CORE*](#_IL-CORE_IG), [*[B.3] Information Requirements document*](#_Information_Requirements)) and organizational FHIR profiles.

Note that regardless of the internal validation components and processes the compliance with the national (i.e. – [*[B10] IL-CORE*](#_IL-CORE_IG), [*[B.3] Information Requirements document*](#_Information_Requirements)) FHIR profiles will be validated during the certification process as outlined in the [*[B.5] Certification Process*](#_Certification_Process) document

## Authorization Server

The organizational FHIR platform **SHALL** include an OAuth2 authorization server compliant with the [HL7 SMART App Launch Framework 2.2.0 Implementation Guide](https://www.hl7.org/fhir/smart-app-launch/index.html) and requirements detailed in [*[4.3] Authentication/Authorization*](#_Authentication/Authorization).

Note, thatfor *Scenario B* [*scope*](#_Scenario_B_(mandatory)) the organizational FHIR platform will also be required to support external authorization server provided as part of PCM – as described in [*[B.11] PCM Overview document*](#_Patient__). Additional details will be provided in the subsequent versions of this document.

# Security & Privacy

## General requirements

Organizational FHIR platform **SHALL** comply with the general security requirements outlined in the [*[B.13] General Security Requirements document*](#_General_Security_Requirements)*.*

## FHIR-specific Audit and Logging requirements

In addition to general audit and logging requirements (as outlined in the [*[B.13] General Security Requirements document*](#_General_Security_Requirements)and other applicable regulation) organizational FHIR platform **SHALL** retain the following audit information for a minimum of two years (unless otherwise specified by the [*[B.13] General Security Requirements document*](#_General_Security_Requirements)and other applicable regulations):

* The platform **SHALL** record the following information for each FHIR REST API data access event:
  + Timestamp
  + The unique identifier of the entity that received the data including client certificate thumbprint and user/patient identity – if available
  + Record of information that was returned
  + Access Justification
* For each successful and failed authentication and authorization event (including token renewal) the platform **SHALL** record the following information
  + Timestamp
  + Source of authentication/authorization attempt
  + Thumbprint of the client’s certificate used for authentication
  + User/patient identity – if available
  + Token identifier, type and lifetime
  + Granted scopes and justification for granting them
  + Operation outcome
* The platform **MAY** record token introspection events

## Authentication/Authorization

The organizational FHIR platform **SHALL** provide an OAuth2 authorization server compliant with the [HL7 SMART App Launch Framework 2.2.0 Implementation Guide](https://www.hl7.org/fhir/smart-app-launch/index.html) and requirements detailed below.

Note, thatfor *Scenario B* [*scope*](#_Scenario_B_(mandatory)) the organizational FHIR platform will also be required to support external authorization server provided as part of PCM for some flows – as described in [*[B.11] PCM Overview document*](#_Patient__). Additional details will be provided in the subsequent versions of this document.

### Basic Preconditions and Client Authentication

#### Certificates requirements and issuance process

To take part in FHIR-based healthcare information exchange as defined by these requirements every participant must prove its identity using standard Public Key Infrastructure (PKI). The X.509 certificates used, must meet specific minimum requirements, be obtained through approved channels, and be registered in the PKD as detailed in [*[3.2.1.1] National Public Key Directory (PKD)*](#_National_Public_Key) section.

##### Minimal certificate requirements:

* Certificates must utilize the ECDSA-256r1 (SECP-256r1) signature algorithm to ensure strong cryptographic security

##### Issuance Channels:

* X.509 digital certificate **SHALL** be issued and signed by one of the following:
  + The Ministry of Health
  + An authorized healthcare organization in Israel with a clear hierarchical CA chain according to ISO27099:2022 standard
  + Globally recognized supplier approved by the General Accountant's Office (חשכ"ל)

##### Certificate Registration:

* Prior to use, an X.509 digital certificate **SHALL** be registered in PKD as outlined in [*[3.2.1.1] National Public Key Directory (PKD)*](#_National_Public_Key) section

Organizations **MAY** opt to use several different certificates. However, all certificates used in FHIR-based healthcare information exchange **SHALL** adhere to the above requirements.

Additional details will be provided in the subsequent versions of this document.

#### mTLS

All access to the FHIR REST API and large binary objects URLs **SHALL** be secured using Mutual TLS (mTLS).

Both clients and the organizational FHIR platform **SHALL** utilize X.509 certificates that are issued in accordance with the guidelines specified in the [*[4.3.1.1] Certificates requirements and issuance process*](#_Certificates_requirements_and) section and registered in PKD as outlined in [*[3.2.1.1] National Public Key Directory (PKD)*](#_National_Public_Key) section.

Both clients and the organizational FHIR platform **SHALL** validate the following for each presented certificate during the mTLS handshake:

* Certificate validity (e.g. - not expired or revoked)
* Registration in the PKD for the corresponding organization

This validation process ensures that all communications are securely authenticated and authorized, to maintain the integrity and confidentiality of sensitive healthcare data accessed through the FHIR REST API and related large binary object URLs.

See [*[4.3.2.3] Client Authentication and Token Binding*](#_Client_Authentication_and) section for additional related information.

### Common SMART on FHIR guidelines

The organizational FHIR platform **SHALL** support SMART on FHIR according to [HL7 SMART App Launch Framework 2.2.0 Implementation Guide](https://www.hl7.org/fhir/smart-app-launch/index.html) and requirements detailed below.

Note that for *Scenario A* [*scope*](#_Scenario_A_(mandatory)) only partial support of full SMART on FHIR specifications is mandatory (as outlined below). For *Scenario B* additional requirements will be introduced.

Only *confidential clients* (as defined in  [RFC 6749: Auth 2.0 specification: client types](https://tools.ietf.org/html/rfc6749#section-2.1)) **SHALL** be granted access to the FHIR REST API and large binary objects URLs, contingent upon successful completion of the authentication process outlined below. For the avoidance of doubt – *public clients* (as defined in  [RFC 6749: Auth 2.0 specification: client types](https://tools.ietf.org/html/rfc6749" \l "section-2.1)) **SHALL NOT** be allowed.

#### Client Registration

The organizational FHIR platform **SHALL** support use of PKD (as detailed in [*[3.2.1.1] National Public Key Directory (PKD)*](#_National_Public_Key) section) for implicit client registration. PKD contains all the fields required by the [HL7 SMART App Launch Framework 2.2.0 Implementation Guide](https://www.hl7.org/fhir/smart-app-launch/index.html).

The organizational FHIR platform **MAY** support additional client registration methods (e.g. - [OAuth 2.0 Dynamic Client Registration Protocol](https://tools.ietf.org/html/rfc7591)).

#### Client Authentication

The organizational FHIR platform **SHALL** support *client-confidential-asymmetric* authentication as detailed in the [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/client-confidential-asymmetric.html). For the avoidance of doubt – *client-confidential-symmetric* authentication (as defined in the [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/client-confidential-symmetric.html)) **SHALL NOT** be allowed.

The organizational FHIR platform **MAY** support B2B Authorization Extension Object as defined in [FHIR UDAP Security Implementation Guide](https://build.fhir.org/ig/HL7/fhir-udap-security-ig/b2b.html#b2b-authorization-extension-object). Note that for *Scenario B* [*scope*](#_Scenario_B_(mandatory)) this requirement may be extended and become mandatory.

#### Client Authentication and Token Binding

To prevent token replay attacks and to enhance security, the organizational FHIR platform **SHALL** enforce binding between access tokens used for authentication (OSI layer 7) and the certificate used for mTLS (OSI layer 6).

##### Client-Side Requirements:

* Clients **SHALL** use the same certificate for both the mTLS handshake and for signing the JSON Web Token (JWT) used for authentication to OAuth2 authorization server’s *token* endpoint.

##### Server-Side Requirements:

* The organizational FHIR platform **SHALL** deny access in case there is a mismatch between the certificate used for mTLS handshake and for signing the JSON Web Token (JWT) used for authentication to OAuth2 authorization server’s ***token*** endpoint.
* The organizational FHIR platform **SHOULD** also enforce token binding for FHIR REST API and large binary objects URL access.  
  (That said, considering the short-lived nature of access tokens and the known identities of all participants, the organizational FHIR platform **MAY** opt **not** to enforce token binding for FHIR REST API and large binary objects URL access.)   
  Note, that the use of mTLS with valid, registered certificates and the enforcement of token binding at the OAuth2 authorization server's ***token*** endpoint remain mandatory.
* All failed access attempts due to certificate mismatch shall be logged for security auditing purposes as outlined in [*[4.2] FHIR-specific Audit and Logging requirements*](#_FHIR-specific_Audit_and).

#### User Authentication

*Scenario A* [*scope*](#_Scenario_A_(mandatory)) does not define specific requirements for user authentication (whether it’s a patient or a practitioner). However, for *Scenario B* support for **patient** authentication will be required as part of PCM (described in [*[B.11] PCM Overview document*](#_Patient__)).

Additional details will be provided in the subsequent versions of this document.

#### Token Format

The organizational FHIR platform **SHALL** support opaque tokens and Token Introspection as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/token-introspection.html) and [RFC 7662: OAuth 2.0 Token Introspection](https://datatracker.ietf.org/doc/html/rfc7662).

The organizational FHIR platform **MAY** include additional information in token introspection response (e.g. – thumbprint of the certificate used for client authentication to the *token* endpoint of the Oauth2 authorization server)

The organizational FHIR platform **MAY** also support JWT tokens as defined in [RFC 9068: JSON Web Token (JWT) Profile for OAuth 2.0 Access Tokens](https://datatracker.ietf.org/doc/html/rfc9068). However, note that PCM support (described in [*[B.11] PCM Overview document*](#_Patient__)) that will be mandatory in *Scenario B* will require support for opaque tokens.

#### Refresh Tokens

The organizational FHIR platform **SHALL** always issue refresh tokens for *SMART App Launch* flow defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/app-launch.html) (i.e. – when using OAuth 2.0 authorization code flow)

The organizational FHIR platform **SHALL NOT** issue refresh tokens for *SMART Backend Services* flow defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/backend-services.html) (i.e. – when using OAuth 2.0 client credentials flow)

#### Lifetime of Authorization Codes and Tokens

The organizational FHIR platform **SHALL** set the lifetime of authorization code to **30 seconds**.

The organizational FHIR platform **SHALL** set the lifetime of access token to **300 seconds**.

The organizational FHIR platform **MAY** determine the lifetime of refresh token according to specific business scenario while taking into consideration *online\_access* and *offline\_access* scopes – if granted to client. In any case the lifetime of refresh token **SHALL NOT** exceed **24 hours**.

#### SMART on FHIR Scopes

The organizational FHIR platform **SHALL** support SMART on FHIR scopes according to v2 syntax – as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#scopes-for-requesting-fhir-resources).

The organizational FHIR platform **SHALL** support fine-grained resource constraints using search parameters – as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#finer-grained-resource-constraints-using-search-parameters), including search modifiers, chaining and reversed chaining, named lists and all FHIR REST API search functionality as outlined in [*[B.4] REST API Guidelines and Requirements*](#_REST_API_Guidelines) document.

The organizational FHIR platform **SHALL** support requesting *openid* scope – as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#scopes-for-requesting-identity-data).

The organizational FHIR platform **MAY** support requesting *launch/patient* and *launch/encounter* scopes.

The organizational FHIR platform **MAY** support custom scopes – as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#extensibility).

For the avoidance of doubt the above requirements are applicable both to the OAuth2 authorization server and to the FHIR REST API and large binary objects URLs.

#### Accessor Identity and Context

The organizational FHIR platform **SHALL** include *patient* context parameter containing logical ID of the Patient resource in the access token (accessed via introspection or in JWT) if any patient-level scopes are granted.

The organizational FHIR platform **SHALL** include *user* context parameter containing logical ID of the Practitioner resource in the access token (accessed via introspection or in JWT) if any user-level scopes are granted.

The organizational FHIR platform **MAY** include additional context parameter (e.g. – *fhirContext*, *intent*, etc.) in the access token (accessed via introspection or in JWT).

Note that PCM support (described in [*[B.11] PCM Overview document*](#_Patient__)) that will be mandatory for *Scenario B* [*scope*](#_Scenario_B_(mandatory)) may introduce additional requirements for context parameters support.

### Access Control and Enforcement Guidelines

The organizational FHIR platform (**authorization server**) **SHALL** express access grants via context parameters (e.g. – *patient*) and SMARTv2 scopes as defined in [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html) and according to the requirements outlined in [*[4.3.2.8] SMART on FHIR Scopes*](#_SMART_on_FHIR) and [*[4.3.2.9] Accessor Identity and Context*](#_Accessor_Identity_and).

The specific logic for granting access in *Scenario A* will be determined out of band according to the agreements between individual organizations (as described [*here*](#_Scenario_A_(mandatory))).

For *Scenario B* access will be determined according to patient consent for specific *Information Buckets* (as described [*here*](#_Scenario_B_(mandatory))). Additional details will be provided in the subsequent versions of this document.

The organizational FHIR platform **SHOULD** define one or more scopes per each resource type and avoid use of [wildcard scopes](https://www.hl7.org/fhir/smart-app-launch/scopes-and-launch-context.html#wildcard-scopes). This approach ensures explicit access grants and helps prevent overly complex search queries.

The organizational FHIR platform **SHOULD** use *List* and/or *Group* resources in combination with SMARTv2 scopes to specify access to a large number of specific resources – as shown in the examples below.

The organizational FHIR platform **SHOULD** support identified lists – both standard – as defined in [*[B.4] REST API Guidelines and Requirements*](#_REST_API_Guidelines) and custom – to facilitate business scenarios unique to each healthcare organization.

The organizational FHIR platform **MAY** use *Consent* resources to store and manage access control information.

The organizational FHIR platform (**FHIR server/façade**) **SHALL** be able to interpret SMARTv2 scopes and context parameters when accessing FHIR resources via FHIR REST API and enforce them.   
(To reiterate – there is no specific requirement for a particular implementation strategy. I.e. – façade or server, native support, customization on existing platform or a separate interceptor component or some combination of the above are all valid approaches).

Note, that while using SMARTv2 scopes to limit access to specific *Information Buckets* and time range (i.e. “*system/\*.rs? \_security=http://fhir.health.gov.il/cs-buckets|labs&date=ge2023-01-01*”) is a common scenario, the organizational FHIR platform **SHALL** support any and all scopes with any and all combinations of search parameters as outlined in [*[B.4] REST API Guidelines and Requirements*](#_REST_API_Guidelines) document.

The organizational FHIR platform **MAY** support supplementary mechanisms for expressing access grants and access control enforcement, **in addition** to the mandatory mechanisms defined here.

#### Examples

* Grant access to lab results for a specific group of patients:  
  To grant access to lab results of the specific group of patients to another organization a *List* of *Patient* resources could be created on the FHIR server containing all patients that said organization has access to. Then the following scope could be used:
  + *system/Observation.rs?patient:Patient.\_has:List:item:\_id=[list\_id]* *&date=ge2024-01-01*

Additional conditions could be added (e.g. – only codes in specific value-set) to further limit access.

* Grant a practitioner access to a list of their patients:  
  To grant a practitioner access to a list of their patients (specifically – Patient resources) a *List* of *Patient* resources could be created on the FHIR server for each practitioner, containing all patients that said practitioner has access to. Then the following scope could be used:
  + *user/Patient.rs?patient:Patient.\_has:List:item:\_id=$current-active-patients*

in combination with user context parameter.   
FHIR server can resolve $current-active-patients list reference to the actual ID of the list of patients for practitioner referenced by the user parameter. Additional resources can be referenced by the scope through chaining/reversed chaining as well.

* Grant access to patient’s encounters for the last year:  
  To grant access to patient’s encounters for the last year the following scope could be used:
  + *patient/Encounter.rs?\_security=http://fhir.health.gov.il/cs-buckets|encounters&date=ge2024-01-01*

Note that this scope uses one of the *Information Buckets* defined in the [*[B.3] Information Requirements*](#_Information_Requirements) document and is still not finalized. Additional details will be provided in the subsequent versions of this document.

### Access Scenarios

#### Business to Business (B2B) Flows

The organizational FHIR platform **SHALL** support SMART Backend Services flow according to [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/backend-services.html) and requirements detailed above - to enable *Scenario A* (as outlined [*here*](#_Scenario_A_(mandatory))). The infrastructure required to support *Scenario A* can be leveraged to support additional, similar use-cases.

#### Business to Consumer (B2C) – Practitioner

The organizational FHIR platform **MAY** support SMART App Launch flow according to [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/app-launch.html) and requirements detailed above - to enable access for practitioner-focused scenarios.

While support for this flow is optional, it leverages the infrastructure required for mandatory scenarios and requires minimal additional efforts, enabling valuable use-cases for practitioners.

#### Business to Consumer (B2C) - Patient

The organizational FHIR platform **MAY** support SMART App Launch flow according to [HL7 SMART on FHIR specifications](https://www.hl7.org/fhir/smart-app-launch/app-launch.html) and requirements detailed above - to enable access for patient-focused scenarios.

Note that for *Scenario B* (as described [*here*](#_Scenario_B_(mandatory))) support for SMART App Launch flow will be mandatory as part of PCM – as described in [*[B.11] PCM Overview document*](#_Patient__). Besides mandatory support for *Scenario B* the required infrastructure can be leveraged to enable additional valuable use-cases with minimal effort.

## Data Minimization Guidelines

When sharing patient data, both clients and servers **SHOULD** strive to minimize the amount of patient data shared.  
The specifics of the shared information will be governed by individual agreements in *Scenario A* and by patient consent for specific *Information Buckets* in *Scenario B*.

The organizational FHIR platform **SHALL** employ the permission mechanism (outlined in [*[4.3.3] Access control and enforcement guidelines*](#_Access_control_and)) to reasonably enforce minimal required access to the data.

In parallel, clients accessing the organizational FHIR platform **SHALL** adhere to the principle of data minimization as well - to ensure compliance with privacy guidelines.

Each client **SHALL** only request FHIR resources that are strictly necessary to support its specific business use case. To reiterate - while a robust permission mechanism exists on the server-side (see [*[4.3.3] Access control and enforcement guidelines*](#_Access_control_and)), it is client-side responsibility to complement those controls. Note, that for *Scenario B* additional audit requirements will be introduced to validate client’s adherence to data minimization principles.

The organizational FHIR platform **SHALL** support granular access through relevant FHIR APIs as outlined in [*[B.4] REST API Guidelines and Requirements*](#_REST_API_Guidelines) document to allow clients to precisely specify the data they require.

#### Below are several examples for data minimization:

##### For Clients:

* Request only necessary resource types within *Information Buckets*
* Filter by specific codes (e.g. – on Observation)
* Filter by reference (e.g. – Observations related to specific Encounter)
* Filter by time range (e.g. – lab results from last week)

##### For Servers:

(Enforced via SMARTv2 scopes and context parameters as outlined in [*[4.3.3] Access Control and Enforcement Guidelines*](#_Access_control_and) and according to specific agreements or patient consent as described in *Scenario A* and *Scenario B*)

* Grant access only to necessary *Information Buckets*
* Limit historical depth via corresponding *date* search parameters
* Limit access to specific resource types within *Information Buckets*
* Limit access to resources in specific *Lists* or *Groups* or resources that are **referenced by** the resources in specific *Lists* or *Groups* (e.g. – via reverse chaining)
* Limit access to resources with specific security labels
* Limit access to resources within specific Patient compartment
* Limit access to resources that have specific category, class or code or resources which category, class or code belongs to specific value-set
* Limit access based on *Purpose of Access* – if available

## Security Guidelines for Large Objects

Healthcare data may incorporate large binary objects that are unsuitable for direct storage (i.e. - in a base64 encoded field within a *DocumentReference* resource) within the organizational FHIR platform. A primary example of this is DICOM images, but similar scenarios exist for other types of binary data. Typically, relevant FHIR resources will include a URL that points to these binary objects stored in an external system.

This URL **SHALL** be accessible to the client in the same manner as a FHIR REST API endpoint.

(Note, that in some cases a parent resource will refer to an *Endpoint* resource which will hold the URL. These requirements apply regardless of this optional indirection)

For those binary resources the same access control logic **SHALL** be applied as to the resource containing the link.   
In other words, clients **SHALL** be granted the same level of access to linked binary resources residing in the external systems as they are to the linking FHIR resource, using the same access token mechanism – as outlined in [*[4.3] Authentication/Authorization*](#_Authentication/Authorization).

Note, that binary resources are often requested in a separate API call from the linking FHIR resource. The organizational FHIR platform **SHALL** be capable of identifying the FHIR resource from which the URL to the binary object originated and apply the appropriate access control measures accordingly.

# Appendix A – National Registries API details

National Registries API details will be provided in the subsequent versions of this document.

# Appendix B – Related Documents

Below, you'll find a list of related documents for your convenience. The most recent versions of all documents can be accessed through the certification portal at the following link.

* Link: [[Certification Portal](https://www.fhir-il-community.org/%D7%A1%D7%A8%D7%98%D7%99%D7%A4%D7%99%D7%A7%D7%A6%D7%99%D7%94)]

## Conceptual Overview of Healthcare Data Portability

This document provides a high-level overview of the healthcare data portability concepts, the certification program, and the timelines.

## Implementation Stages

Recognizing the large overall scope of requirements, they are broken into several Implementation Stages. This document outlines the scope of each stage and the relationship between them.

## Information Requirements

This document provides a functional definition of *Information Buckets*, as well as their relationship to FHIR Resources. It defines mandatory fields, outlines data quality expectations, and coverage requirements.   
An *Information Bucket* is a structured collection of medical and/or demographic data associated with a specific semantic concept. Patients can leverage this mechanism to grant access permissions for their healthcare data.

In addition, mapping of functional requirements to FHIR will also be provided.

## REST API Guidelines and Requirements

This document outlines minimal requirement for FHIR REST API coverage that must be supported by the organizational FHIR infrastructure. Whenever possible, these requirements are expressed in a machine-readable format using FHIR *CapabilityStatement*, facilitating automated validation processes.

## Certification Process

To ensure adherence to the technical and informational requirements outlined in this document and its companion resources, a certification process will be established. This process will provide a mechanism for healthcare organizations to demonstrate their data and FHIR infrastructure's compliance with the national standards. The details of this certification process and overview of the test performed are outlined in the referenced document.

## FHIR Schema Validation Approaches (Informational)

This document provides a reference guide for exploring approaches, architecture, and tooling to enable information security-driven schema validation of FHIR REST traffic.  
This is **not** part of the requirements and only provided here for reference.

* This document will be provided at a later stage

## FHIR Attachment Handling Approaches (Informational)

This document explores various approaches, architectures, and tools for secure handling of binary attachments within FHIR REST traffic.  
This is **not** part of the requirements and only provided here for reference.

* This document will be provided at a later stage

## Sub-resource Access Control Approaches (Informational)

This document describes approaches, architecture, and tooling to enable granular access control and enforcement at the sub-resource (data element) level.   
This is **not** part of the requirements and only provided here for reference.

* This document will be provided at a later stage

## Guidelines for Digitally Signing FHIR Payloads

This document outlines technical requirements and provides guidelines for digitally signing FHIR payloads. If required by business use-case, organizational FHIR infrastructure **SHALL** support both signing and validating digitally signed FHIR payloads according to these guidelines.

* This document will be provided at a later stage

## IL-CORE IG

All data is modeled using FHIR profiles derived from IL-CORE FHIR profiles – as published in IL-CORE Implementation Guide.

* Link: [[IL-CORE IG](https://www.fhir-il-community.org/fhir-israel-core)]

## Patient Consent Manager (PCM) Overview (Informational)

This document provides a high-level overview of the Patient Consent Manager (PCM), a central infrastructure component responsible for managing patient consent and authorization on a national level. Support for PCM will be required for *Scenario B* in *Stage III* of the organizational FHIR infrastructure (as defined in [*[B.2] Implementation Stages document*](#_Implementation_Stages)).

## Reference architecture (Informational)

This document showcases a sample architecture that can support the requirements outlined in this document and incorporates best practices and recommended approaches.

However, it is important to stress that this document serves as a reference point only and should not be interpreted as a requirement or constraint on implementation. Each organization is free to design its own architecture tailored for its needs and capabilities.

## General Security Requirements

This document outlines general security requirements mandated by the Ministry of Health that are applicable to all platforms and solutions and not FHIR-specific.

Note that all the guidelines and requirements in this and referred documents are subject to the requirements outlined in the General Security Requirements document.