Area description

Table of contents

1 Definitions

Term	Definition
ABAC	Attribute-based access control (ABAC), is an access control paradigm whereby a subject's authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment attributes
Bioinformatics/omics	A field of science that develops methods, software tools, and standards for understanding, storing, and sharing biological data such as genomics, proteomics, metabolomics and, microbiomics.
CDR	Clinical Data Repository. Software that stores EHR content, and in the case of openEHR implements the openEHR ITS-REST service specifications including query capabilities.
Compositions	Content of one version in a VERSIONED_COMPOSITION. A Composition is considered the unit of modification of the record, the unit of transmission in record Extracts, and the unit of attestation by authorizing clinicians. In this latter sense, it may be considered equivalent to a signed document.
Consultant	Physical named person employed by the Supplier or otherwise offered by Sub-contractor.
Consulting Services Provider	"Consulting Services Provider" shall refer to a legal person or a sole trader who provides Consulting Services. Consulting Services Providers may either have their own employed Consultants or, alternatively, resell Consulting Services as intermediaries.
Digital Health Platform	Karolinska's new platform that offers integration and data storage services. Partially consists of a clinical data repository (CDR) based on an international standard (openEHR), development tools and a traditional enterprise data warehouse (EDW). Is used as a base for the realization of applications in a health care setting.
DICOM	DICOM is the international standard to communicate and manage medical images and data.
EHR	Electronic Health Record
HL7 FHIR	HL7 Fast Healthcare Interoperability Resources.
HL7 v2	HL7 Version 2.
ICD-10	International Statistical Classification of Diseases and Related Health Problems, 10th Revision.
ICF	International Classification of Functioning, Disability and Health.
KVÅ	"Klassifikation av Vårdåtgärder". National classification of healthcare procedures (Klassifikation av vårdåtgärder), used for reporting and analysing health interventions for clinical, financial, and statistical purposes.
Open Source (Software)	Software that in its entirety is licensed using one or several licenses approved by the Open Source Initiative http://www.opensource.org/licenses/

Term	Definition
openEHR	Even though openEHR is an organisation, see https://openehr.org/, the word is in this, and associated documents, usually referring to the technical specifications or clinical content models defined by the openEHR organization and community. Thus “openEHR-based" refers to something based on the openEHR specifications and “openEHR models” refers to models (templates, archetypes etc.) based on such specifications and on associated work by the openEHR community including Karolinska.
openEHR RM and AM	openEHR Reference Model and Archetype Model.
Patch	Corrections, security fixes and functional improvements of Software. The offering of an Upgrade with the sole purpose of correcting errors shall be defined as a Patch.
Production environment	Deployment environment requiring regulatory compliance where sensitive information is managed.
RBAC	Role-based access control (RBAC) is an approach to restricting system access to authorized users’ roles.
RPO	RPO recovery point objective is a time-based measurement of the maximum amount of data loss that is tolerable to an organization. Also called backup recovery point objective.
RTO	Recovery Time Objective (RTO) is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in continuity.
SNOMED CT	Systematized Nomenclature of Medicine - Clinical Terms.
Software	Software is a set of instructions, data or programs used to operate computers and execute specific tasks.
Solution	The software, technologies, and services that will be procured in/by/from framework agreements.
Supplier	Tenderer who after a finalized procurement process has entered a Framework agreement with the Contracting authorities.
Test environment	Controlled deployment environment where no sensitive information is managed. Low uptime requirements.
Upgrade	New version of Software delivering new or improved functionality.
1177	The Swedish national patient portal web. You can call the 1177 helpline if you or someone in your family is ill and you can get advice from a nurse.

2 Scope of Solution

Karolinska continues to accelerate its investment in IT and digitalization. To take advantage of the continuous modernization of healthcare information standards, Karolinska has begun the development of an open and standardized Digital Health Platform to create more and new opportunities for data-driven care and research. Karolinska's Digital Health Platform will collect, harmonize, and provide data from multiple systems to provide IT support to the various units and sections of the hospital. The platform, and associated applications will increase efficiency and productivity, reduce administration, raise quality, and provide better support for research. This is achieved through the platforms technical capabilities, for example through efficient access to data through consolidated access to data sources from multiple systems.

Functionality in existing applications can gradually be replaced by standardized modules running in the new platform; a shift that will provide a flexible and adaptable solution that can also integrate new applications developed in the future. Karolinska is building this new Digital Health Platform in-house with close cooperation from the hospital's many clinical departments.

Karolinska has made a strategic choice to base parts of the Digital Health Platform on openEHR-based technology. We believe that the openEHR-based standardization has an important role to play in the strategy to reach the following goals:

- Ability to innovate and develop - Faster adaptation of IT systems to meet the constantly changing and developing healthcare, including a more efficient development process.
- Improved governance - Increased control of stored health record data and increased reuse of information structures within and between applications.
- Efficiency - Increased freedom of action by storing data in a vendor neutral and open format.

Karolinska is now reaching out to suppliers to establish a framework agreement regarding delivery of parts of the Digital Health Platform. The scope of the procurement is divided into three categories:

- Category 1: openEHR-based Software
- Category 2: Software for openEHR Content Creation and Transformations
- Category 3: Consulting Services

These categories are described briefly in the following sections to give an overview and in more detail in the following chapters.

2.1 Category 1: openEHR-based Software

As illustrated in the openEHR architecture overview[1], a functioning openEHR-based eco-system is dependent on several other platform services, not only a clinical data repository. In this functional area we seek best-of-breed solutions that helps us realize this architectural vision into a working platform.

Detailed descriptions follow below that specify the services, software and tooling we need to support development of clinical applications and also for managing regulatory requirements in a Swedish healthcare context. We seek Suppliers that can deliver within the following subcategories:

- Subcategory 1a: Software for storing and managing openEHR-based data

[1] Architecture Overview (openehr.org)

- Subcategory 1b: Software for fine-grained access control
- Subcategory 1c: Software for developing and publishing openEHR-based applications
- Subcategory 1d: Software services

In these subcategories the following Software and services are relevant to purchase from a vendor:

- Subcategory 1a: Software for storing and managing openEHR-based data
    - Clinical Data Repository (CDR) component
    - Patient Master Index (PMI) component
    - Distributed Transaction Manager component
    - Auxiliary and administrative tools for the three above components
- Subcategory 1b: Software for fine-grained access control
    - Software for additional functionality to be able to comply with Swedish healthcare regulations and other access control needs. Chapter 3.2 Subcategory 1b: Software for fine-grained Access Control gives information about the regulatory requirements in this area for vendors to understand what is expected in this subcategory.
- Subcategory 1c: Software for developing and publishing openEHR-based applications
    - Software tools for development, publication, and maintenance of openEHR-based applications
- Subcategory 1d: Software services
    - Services to support activities within the software development life cycle (design, implementation, testing, operations etc).

2.1.1 Motivation of bundling subcategories 1a-d into a single procurement category

The Swedish openEHR RFI 2023 indicated that many of the tools and functions described in subcategories 1a-c are often offered in bundles and thus suitable to procure together. Even if form- and query-tools may be supplied by separate system providers and run independently of procured CDR(s) and access control solutions, we at this stage want the main contractors to be responsible for the compatibility and integration of offered combination of important tools, CDR and access control. All provided Software must also have the possibility to include Support services with a well-defined target SLA – this is described in subcategory 1d.

Further it is assumed that some needs may arise that are better covered by tools not offered in category 1 in such cases additional tools, functions etc. may be procured also via category 2.

2.2 Category 2: Software for openEHR Content Creation and Transformations

In Category 2 we are looking for the following tools (but not limited to):

- Software tools for creating and managing openEHR content.
- Software Development Kits for working with openEHR RM and AM. Model objects (in e.g., Java, C#, Python)
- Tools for working with templates and conversions between openEHR template formats, like simplified (e.g., “Flat”) and canonical formats.
- Mapping and integration tools and SDKs, e.g., supporting transformations Between openEHR, HL7 and other non-standardized models and instances.
- SDKs supporting/simplifying generation of forms and applications based on openEHR models.
- Visualization tools (proven to have been integrated with openEHR solutions).

- Specialized solutions for creating process- and/or clinical decision support based on openEHR.

It is assumed that some of the above listed tools may also be partially or fully included in software procured via category 1, but category 2 opens the possibility to complement this with separate specialized solutions from other providers. This includes a possibility for smaller providers to offer solutions even though they may not fulfil all requirements of Category 1. Providers may also offer commercial grade support for open-source tools in the above listed categories.

In this category the following Software and services are relevant to purchase from a vendor:

- openEHR-related software that can be procured separately and that not necessarily are bundled together with a particular CDR. Karolinska is interested the software and associated professional support in this category different suppliers can provide.

2.3 Category 3: Consulting Services

This category concerns consulting services able to deliver expertise regarding openEHR and/or SNOMED CT including software development, integrations, and expertise in information modeling. The same Consulting Services Providers may additionally also provide competence regarding HL7 FHIR, HL7 v2, DICOM and bioinformatics/omic-standards when needed. Collaboration between Consulting Services Providers is encouraged.

In this category the following Software and services are relevant to purchase from a vendor:

- Resource consulting services, and
- Assignment consulting services

3 Category 1: openEHR-based Software

Reading guidance: Please note that subcategory 1b Software for fine-grained access control in this document is described in more detail than the other categories because Swedish context and regulations may be unfamiliar to international solution providers. This does not mean that the other categories are less important in the procurement.

3.1 Subcategory 1a: Software for storing and managing openEHR data

This section aims at specifying the use cases and specific problems that the Karolinska wants to solve with a Clinical Data Storage Solution implementing the openEHR specifications. The Solution will be a core integrated component in the Karolinska Digital Health Platform and must support all aspects of a highly available clinical IT system with low RPO and RTO. The Solution is expected to be modular where individual sub-components are loosely coupled and can be replaced with a reasonable effort.

There is a distinction made between the terms Clinical Data Storage referring to the conceptual abstraction of storing the data, and a Clinical Data Repository (CDR) referring to one or more technical data storage components which builds up the Clinical Data Storage.

Figure 1 shows our simplified view in ArchiMate[2] notation of the surrounding services that together realize a functioning openEHR-based system for storing and managing data.

[2] The ArchiMate® Enterprise Architecture Modeling Language | opengroup.org

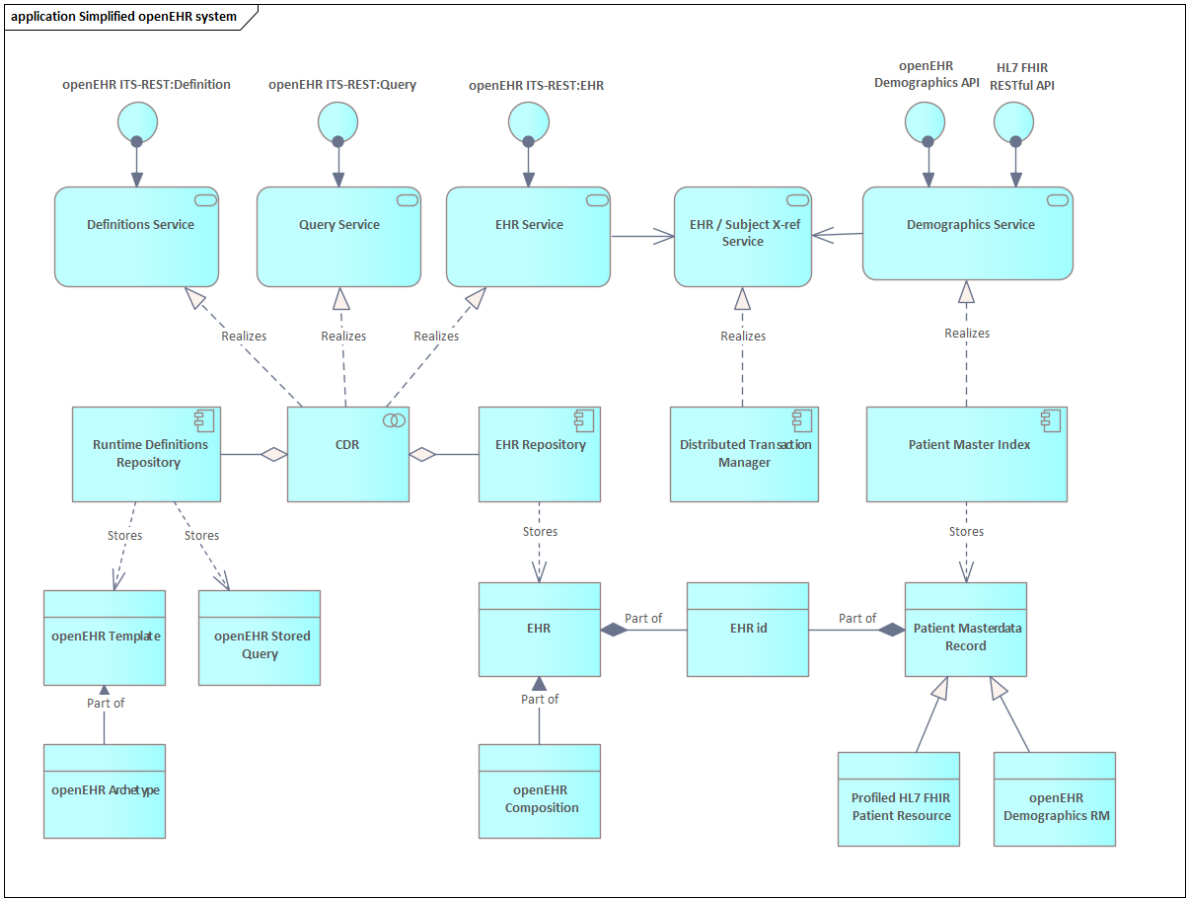


Figure 1 A simplified and opinionated view of a typical openEHR technology landscape, in ArchiMate notation. The standardized openEHR service and interface models realize a CDR where Compositions are stored and queried.

This architecture supports the loosely coupled demographics model of openEHR by only storing directly identifiable patient identifiers in a Patient Master Index component (PMI). The integration between the PMI and the openEHR Services is implemented using standardized APIs for increased modularity. In this picture we use HL7 FHIR, but we could also use a future openEHR-based service model as it matures. The PMI maintains a reference from the patient master data record through a shared EHR id to the corresponding EHR record in the CDR. An EHR/Subject X-ref Service maintains consistency between the two repositories using a distributed transaction mechanism like IHE PIX[3]. EHR records are created through this service by coordinating usage of the EHR and Demographics service API:s.

In this sub-area we seek Software that realize the services and API: s described in Figure 1. For increased modularity and minimization of vendor lock-in, the Software should be delivered as three separate logical components:

- “CDR” - Clinical Data Repository component
- “Patient Master Index” - (PMI) component
- “Distributed Transaction Manager”- component

It is essential that all components needed for the solution work together to form a functioning openEHR eco-system within subcategory 1a, 1b, 1c and category 2 and 3.

[3] IHE ITI TF Vol1

3.1.1 Clinical Data Repository (CDR) component

The Software must implement the openEHR specifications[4]. There is an expectation that the offered solution must comply with the openEHR releases stated as "stable state"[5] e.g., the openEHR ITS domain, as well as having a thought-out process for handing and contributing to the openEHR components stated both as "stable state" and "development state", e.g., openEHR Conformance Specifications (CNF) Component.

To exemplify further this means that the procured Clinical Data Storage Solution will consist of one or more underlying OpenEHR CDRs with full support of (including, but not limited to)

- openEHR RM
- openEHR EHR API
- openEHR Query API
- openEHR Definitions API

It is also of importance that the implementation, database design and supporting technology used ensure that Karolinska can scale the implemented Solution to a vast number of concurrent users and database accesses, without neither losing data integrity nor creating system bottlenecks due to high end-to-end data latency.

3.1.1.1 openEHR CDR and PMI - related capabilities

Alongside the raw technical aspects of openEHR conformance stated above there are additional capabilities associated to the Karolinska platform vision that is of interest to point out.

3.1.1.1.1 Multiple CDR for different purposes

Several CDR instances for different purposes will most likely be bundled together to build the Karolinska Clinical Data Storage Solution in the production environment (multiple instances in same environment).

In addition to this Karolinska will also have a set of different technical environments e.g., development, test and production.

3.1.1.1.2 Administrative support tools, documentation, and documented routines

For the procured openEHR Solution (CDR and PMI components) to comply certain non-functional requirements of Clinical Data Storage systems, the offered Solution should have administrative support tools, documentation and documented routines supporting (but not limited to):

- Bulk operations
    - Import and Export
- Business continuity solutions
- Data retention policies (purging)
- On premises installation and configuration
- Life cycle management (PLM)
- OpenEHR content management
    - E.g., Publishing of templates, definitions etc.
- System monitoring, health checks and alerts

[4] https://specifications.openehr.org/
[5] https://www.openehr.org/programs/specification/changeprocess

- Component IAM: RBAC and external IDP integration
    - Integrations and service accounts
    - Admin
- Logical and physical deletion of Compositions and EHRs

3.1.2 Patient Master Index (PMI) component

The procured Solution must implement an openEHR CDR according to the openEHR information model[6] where demographic data is separated from health records ("pseudonymization"). Consequently, there is a need for a component where demographic data is stored and referenced to related EHR.

For the procured Solution to be compatible and interoperable with related components in the Karolinska environments, the PMI component is expected to support (but not limited to):

- HL7 FHIR API
- Bulk import using HL7 FHIR formats
- Bulk export HL7 FHIR format
- Ability to use Karolinska specific FHIR profiles and extensions

The PMI can also be used in a more general way, supporting patient merging and more enterprise features as defined in IHE PMIR[7] or similar.

3.1.3 Distributed Transaction Manager component

In the openEHR architectural model as illustrated in Figure 1, EHR-ids are linked to patient identities in the PMI component. It is critical that these links are correctly attributed to the patient. Hence, we need a robust system exhibiting transactional properties when these links are established.

This component manages the distributed transaction between the PMI and the CDR by handling transient failures gracefully. It presents a proprietary high-level transactional API to the developer that hides the underlying complexity to allow for safe creation of EHRs that always are linked to the correct PMI record.

3.2 Subcategory 1b: Software for fine-grained Access Control

In this subcategory we seek additional functionality to be able to comply with Swedish healthcare regulations and other access control needs. We are looking for solutions that can be configured rather than developed.

The openEHR specifications do not specify how to implement access control, it is left to the implementor to provide this functionality. To maximize developer productivity and simplify compliance, we want to externalize common functionality like access control from individual applications to common platform services. To support this strategy, we already have platform services in place to manage access control on the HTTP-request level, as described in chapter 7 in document 'Appendix 4 Karolinskas IT-landscape'.

These standardized platform services are necessary to prove some basic level of access control. However, for compliance with Swedish healthcare regulations the openEHR services must be extended with functionality to provide more fine-grained access control than solutions only

[6] https://specifications.openehr.org/releases/RM/latest/ehr.html#_demographic_data_in_the_ehr
[7] IHE.ITI.PMIR\1:49 Patient Master Identity Registry (PMIR) Profile - FHIR v4.0.1

operating at the HTTP protocol layer. It is not sufficient to only govern access to HTTP methods and resources as the openEHR service model also include services for querying. We need to understand what the query is doing and be able to control the resulting replies.

Key to delivering this functionality is the ability to filter outgoing Compositions and query replies. Before a composition is returned to the user, we want to have the ability to remove, rewrite and/or redact it. This filter function should be able to use an external policy engine where we can integrate external sources of metadata and manage access control logic. The type of metadata needed to be managed can be divided into two categories: ownership and information classification, see Figure 2.

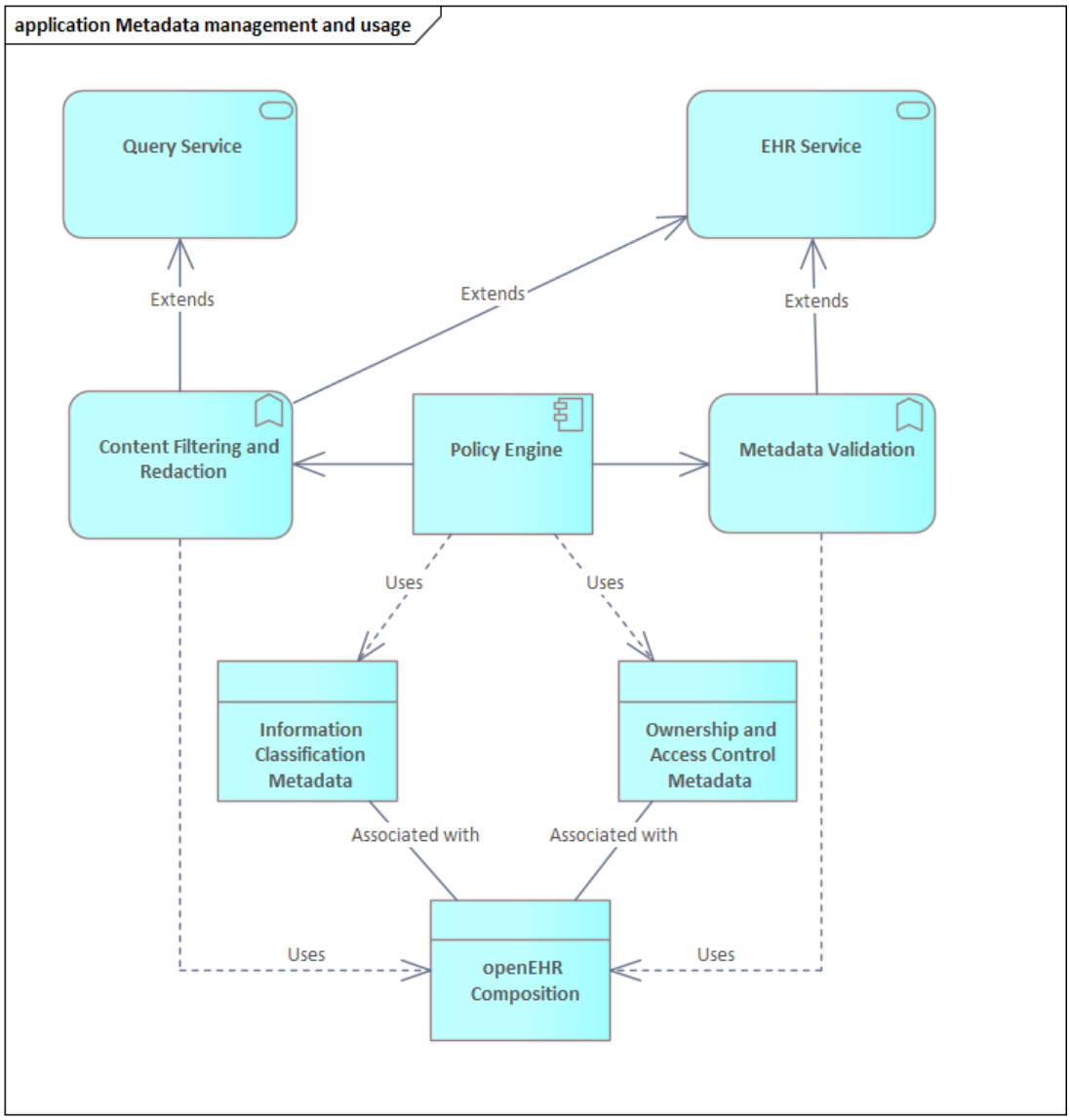


Figure 2 Two types of metadata are associated with openEHR content. This metadata is used by two additional functions governed by an external policy engine for regulatory compliance

An incoming request will contain various claims collected by the application and the user. The policy engine supports the filtering and validation functions by using the metadata associated with the Compositions to verify that the claims match the metadata. In some cases, the metadata must be persisted and reused whereas in other cases, the policy engine might need to support runtime overrides using dynamic metadata from the active session. As this metadata will be used for access

control, we also need robust functionality for run-time validation and management. We need to be sure that the provided metadata is correct and submitted by a trusted party.

This functionality can be configurable as part of an existing CDR implementation or implemented as an independent component that integrates with any openEHR compliant CDR.

3.2.1 Information about laws and regulations in the Swedish healthcare system

The purpose of this chapter is to give detailed information about the laws and regulations in the Swedish healthcare system. It can be regarded as information only to be able to understand the context in which a Swedish healthcare provider acts. Karolinska is responsible for interpreting the Swedish laws and to generate the requirements for IT-functions, services and systems required to meet the interpretations.

The background information is presented according to the following structure, see Figure 3 below:

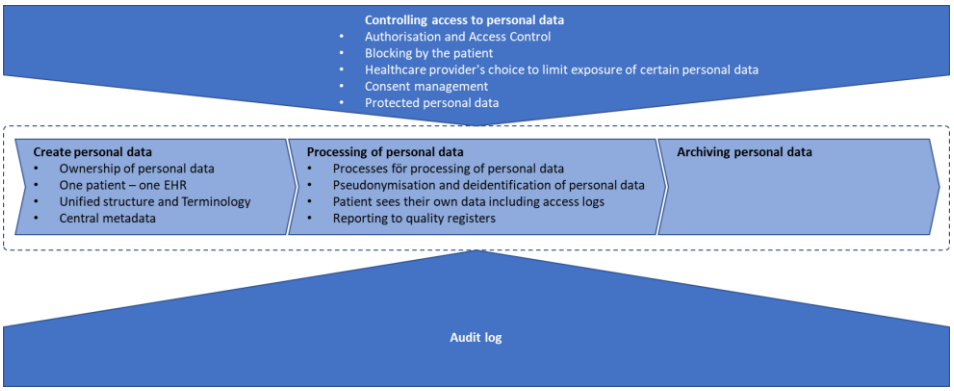
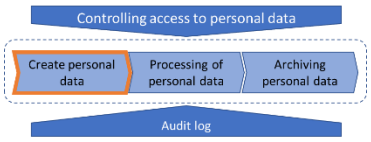


Figure 3 Laws and regulations background structure

3.2.1.1 Create personal data

The following sections describes what “Create personal data” implies.



3.2.1.1.1 Ownership of personal data

Swedish healthcare is organized by the state, regions, and the municipalities. Care assignments are given to various healthcare providers. Healthcare is financed through tax funds, and healthcare providers can be both publicly and privately owned. What is commonly referred to as "healthcare provider" is hereafter referred to as PDL[8] healthcare provider[9] to clarify the legal definition.

The legal definitions that govern how a healthcare provider is allowed to handle information about personal data are based on both a definition of an organizational PDL healthcare unit[10] and a

[8] **PDL**: an abbreviation of the Swedish “Patient Data Law” (Patient Data Act), SFS no: 2008:355 one of several laws regarding the Swedish healthcare.

[9] **PDL healthcare provider**: Organizational unit which in the Swedish Patient Data Act is the legal person which rules and laws are related to

[10] **PDL care unit**: Organizational unit which in the Swedish Patient Data Act is the unit which rules and laws are related to.

definition of a process - a PDL healthcare process[11]. These two "divisions" can be seen as equivalent to each other in terms of how personal data is handled. In addition to this, the lowest organizational level - the care delivery unit - is significant. It is the level where an employee logs into a system and the level which controls the authorization for writing permission.

All personal data[12] created in a patient record will be "owned" by the organizational unit where the personal data was created. The information about by in which unit personal data was created is crucial in determining how and who the information may be processed at a later stage.

3.2.1.1.2 One patient – one EHR

A patient record must be kept for one patient and cannot be shared by multiple patients. It must be possible to create data in a patient record even if a patient's identity cannot be established, i.e. has no Swedish social security number, or has a protected identity. This means that a record may need to be created with an alternative patient ID, which later needs to be merged with the record created in the patient's unique ID. In addition, the customer will have multiple instances of CDRs (described in 2.1.3.1), one EHR ID per CDR, which means that functionality for Patient Master Index (PMI) needs to be included in the solution, to enable a complete and consolidated view of personal data for a patient.

3.2.1.1.3 Unified Structure and terminology in the EHR

The healthcare provider must ensure that the information in an EHR is unambiguous, and the data in the EHR should be documented only once. This means that information in the EHR must be easily accessible, in a clear way to authorized healthcare personnel. A shared structure with less unstructured text improves accessibility and provides better possibilities for obtaining an overview of the data in the EHR. Having a standardized and structured record documentation with uniform terms and concepts makes the record more accessible and manageable, while also enabling information reuse and searchability. This requires that the stored data in the EHRs adheres to international, national, and regional publications for the standardization of healthcare information, such as Snomed CT, ICD-10, KVÅ, ICF, and others. To enable this, the solution needs to integrate with the customer's FHIR terminology services and should fulfill the functionality required to be categorized as Snomed CT Maturity Framework level 4[13].

3.2.1.1.4 Central metadata

The below-listed metadata areas are essential and compulsory for managing access to, and governance of, personal data. Therefore, the below described metadata areas shall be associated with all personal data stored in the CDR. The specific metadata to be stored for a certain personal information shall be configurable.

- Information about organization and unit: Which PDL healthcare provider, specific PDL care unit/PDL care process, and care delivery unit the data was created at or requested from.
- The information domain to which the personal data belongs (e.g., medication, warning information). The mapping to correct information domain for certain personal data will need to be handled.

---

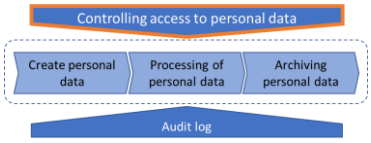
[11] **PDL care process**: the process of healthcare that handles one or more related healthcare problems or healthcare conditions to promote an intended result. The PDL care process is defined by each PDL healthcare provider.

[12] **Personal data:** All information that can be directly or indirectly linked to a physical person.

[13] Implementation Maturity - SNOMED Implementation Support - SNOMED Confluence (ihtsdotools.org)

- General descriptive metadata such as timestamps (when the personal data was created and stored in the CDR).
- Status information (e.g., signed/unsigned, blocked/not blocked). Some of the status information will come from the application where the data was created and other will come from external meta data sources (see description of components related to subcategory 1a Software for storing and managing openEHR-based data).
- The source/lineage of the personal data (ex. from which person or MT-equipment, IT system/application the data originates from).

3.2.1.2 Controlling access to personal data



This section describes the different ways to control and limit whether - and how - personal data can be processed by a user, resulting in an intricate "web" of different rules to take into account.

3.2.1.2.1 Authorization and Access Control

The employer defines which personal data a user has access to and what the employee may do with the data. Each PDL healthcare provider controls its own authorization structure and management, and all authorizations and logins must be personal/individual via strong authentication. Each healthcare professional can have a large number of different authorization levels and when logging in, the user needs to be able to select employee assignments and care delivery unit.

The Identity Access Management needs to be handled by integration to the external components Identity Access Management, chapter 3.2.2.8, and the Customer´s existing Master Data Management solutions that will be utilized by several applications/systems.

3.2.1.2.2 Blocking by the patient

A patient can request to block their personal data from persons outside the PDL care unit/PDL care process where the personal data was created. Patients can choose to block data organizationally or by information areas. Metadata about a patient's blocks need to be stored and handled in the external component Patient blocks repository and service, chapter 3.2.2.2 that can be utilized by several applications/systems.

Data relating to e.g. children can in general not be blocked, either by the patient themselves or by a guardian or other representative.

The following information on a patient's unblocked and blocked personal data must be available to display in different situations with different rules and requirements for functions (the rules on unblocking are described in chapter 2.2.1.3.1 Processes for processing of personal data):

- For an employee within the same PDL healthcare provider but at another PDL care unit/PDL care process:
    - that blocked and unblocked personal data exists.
    - on which PDL care unit/care process the blocked or unblocked data is located.
- For an employee at another PDL healthcare provider:
    - That blocked or unblocked personal data exists (but not on which PDL healthcare provider).

- That the blocked or unblocked personal data exists with a specific PDL healthcare provider.
- That blocked or unblocked personal data is located in a specific PDL healthcare unit/process within a PDL healthcare provider.

It must not be possible to block the information about a patient's blocked data as described above.

A block is valid until further notice. The patient may at any time request the PDL healthcare provider which blocked the data to unblock it.

Blocked personal data should apply to all personal data defined by the patient, regardless of the system in which the personal data were created. This requires that the information about blocked data follows the personal data when transferred to another application/system. Thus, there must be metadata about all personal data that describes whether the data is blocked, and which organization and PDL care unit/PDL care process (as well as which healthcare personnel) has blocked the personal data for the patient. Metadata about blocking need to be stored in the external area Patient blocks repository and service chapter 3.2.2.2 that can be utilized by several applications/systems.

3.2.1.2.3 Healthcare provider's choice to limit exposure of personal data

A PDL healthcare provider may decide to exclude certain types of personal data from the patient's ability to block it. Each PDL healthcare provider may also decide to restrict the sharing of personal data in certain situations, e.g., a healthcare professional may also decide to exclude a parent from accessing their child's record.

The restriction needs to be able to cover the following perspectives, either individually or in combination with each other:

- generic policies regarding certain specific types of personal data such as warnings, adverse reactions, or alerts
- generic policies regarding certain types of personal data (such as sensitivity)
- patient-specific overrides
- policies applying to groups (cohorts) of patients
- personal data created within a particular organizational entity, such as a PDL provider, a PDL care unit/care process or a care delivery unit.

Metadata about PDL provider's restrictions need to be stored in the external component Limiting exposure of personal data, repository and service, chapter 3.2.2.5 that can be utilized by several applications/systems.

3.2.1.2.4 Consent management

This includes both the patient's active consent to something (opt-in) and the patient's right to oppose to something (opt-out). Examples of opt-in are consent to a PDL healthcare provider's direct access to the patient's personal data according to coherent health and care documentation or to the collection and storage of tissue samples in a biobank. An example of an opt-out is the patient's choice not to authorize the transfer of their personal data to a quality register. Metadata about consent need to be stored and handled in the external component Patient consent repository and service, chapter 3.2.2.3, that can be utilized by several applications/systems.

The consent itself is a sort of contract between two parties, i.e., between the patient and the healthcare provider. The validity period depends on the situation and consent can be withdrawn by the patient at any time.

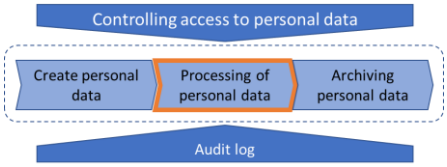
For patients with reduced/lack of decision-making capacity, an authorized representative can give consent on behalf of the patient. If this is the case, it should be possible to document the source of the consent. In the case of a child's personal data, consent to access them via electronic and direct access is implied and does not need to be explicitly obtained from the child.

3.2.1.2.5 Protected personal data

A citizen who feels threatened can apply for different types of protected personal data, which results in a flag, i.e., different types of metadata, on the person's data. Metadata about protected personal data need to be stored and handled in the external component Patient master index, chapter 3.2.2.7, that can be utilized by several applications/systems.

3.2.1.3 Processing of personal data

The following sections describes what “Processing of personal data” implies.



3.2.1.3.1 Processes for processing of personal data

After a healthcare personnel are correctly logged in with the right authorization, there are various rules for how the employee may access personal data and how it may be processed.

A basic prerequisite for a healthcare personnel to access a patient's personal data is that the PDL healthcare provider where the healthcare personnel is employed has an active patient relationship. A patient relationship can arise in many ways and exist for shorter or longer periods of time.

Another prerequisite for accessing a patient's personal data is that the healthcare personnel participate in the care of a patient. Participating in the care of a patient may, for example, involve preparing and carrying out the visit or care of the patient, counselling the patient, cooperating in a team, and participating in different types of rounds or patient conferences or answering questions from a colleague...

To access information created in either another PDL care unit/PDL care process within one's own care provider, or within another PDL care provider, information must be able to be displayed step by step. There are various situation-driven processes for accessing personal data that need to be configured in the Solution. The currently known elements are (may change with Swedish legislation):

Active choices: Active choice means that an authorized user decides whether he or she is entitled to access additional data and that the user indicates the reason for the active choice. Active choices are used in different situations for different positions.

View different information and at different levels of personal data: It should be possible to view personal data information at different levels:

- See if there is unblocked or blocked personal data.
- See that personal data is available on a particular PDL healthcare provider.
- See on which PDL care unit/PDL care process on which PDL healthcare provider the personal data exists and when it was created.
- See the personal data in its entirety

Emergency access or emergency opening: If the patient's consent cannot be obtained because the patient is temporarily incapacitated, for example due to unconsciousness, the healthcare personnel can still access personal data. This applies only in those situations and for the personal data that can be assumed to be relevant to the care the patient urgently needs when there is a danger to the patient's life or a serious risk to the patient's health. .

Consent: the fact that the patient has given his/her consent for the user to access personal data should be able to be provided as a reason for access.

Temporary unblocking: patients' blocks that are temporarily unblocked are valid for a specific period, which is documented in connection with the temporary unblocking.

Request for access to personal data created by another PDL healthcare provider: If emergency access to blocked personal data is required, the current PDL healthcare provider can contact the PDL healthcare provider with blocked data and request that the block be temporarily lifted and that the current PDL healthcare provider can access blocked data at the other PDL healthcare provider.

A staff member must then contact the PDL provider with the blocked data who can decide and then implement a temporary unblocking of the patient's personal data for a period specified by the unblocking PDL provider.

3.2.1.3.2 Pseudonymization and deidentification of personal data

Pseudonymization refers to the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of supplementary information.

The solution should include a function to pseudonymize and deidentify patient data. The supplementary data is stored in the external Patient master index, chapter 3.2.2.7.

3.2.1.3.3 Patient sees their own data including access logs

Personal data (in the form of a medical record) from a PDL provider must be provided to the patient or a relative of the patient as soon as possible upon request. This can be done by transcription, printing or by giving the patient access to his or her personal data through direct access or other electronic disclosure, (e.g., by viewing personal data in 1177).

However, there may be cases where a decision has been made that a medical record or part of it should not be disclosed to the patient or relatives, which requires that information in a patient record can be exempted from disclosure. Please refer to Healthcare provider's choice to limit exposure of certain personal data, chapter 3.2.1.2.3.

For patients to be able to access their own personal data via direct access, the patient must be able to be identified via proper authentication.

There must also be functionality to provide the patient with extracts from the medical record in writing, which requires it to be possible to print out information.

In addition to accessing their own records, patients have the right to access logs relating to their patient records.

3.2.1.3.4 Reporting to quality registers

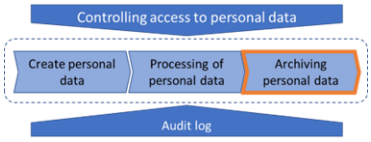
To develop and ensure the quality of healthcare, there are national and regional quality registers, which enable an automated and structured collection of personal data continuously and systematically. There are more than 100 quality registers in Sweden, each with a clear specification of what personal data can be collected for the scope of the specific quality register and how long it

can be stored in the quality register. Reporting to a quality register means that personal data is copied to an external system/platform managed by an external party.

The handling of personal data linked to quality registers must be carried out as follows:

- Only the personal data needed for the purpose of the register may be reported by a PDL healthcare provider to a quality register (data minimization). It must be possible to create selection criteria at personal data level. Information that personal data has been reported to a quality register must also be stored as metadata for the personal data.
- A PDL healthcare provider may only report personal data created within its own PDL healthcare provider to a quality register, i.e., a PDL healthcare provider cannot report to a quality register on behalf of another PDL healthcare provider. It must therefore be possible to sort out individual personal data based on which PDL healthcare provider created them.
- A patient must have the opportunity to oppose the transfer of their personal data to a quality register (opt out). In these cases, this must be documented, and their personal data cannot be processed for this purpose. A patient's choice not to authorize the transfer of personal data to a quality register only applies per PDL healthcare provider.
- Upon patient request, their personal data reported to a quality register may be deleted. The request is made to the party that manages the register, but even in CDR, the metadata that personal data has been reported to a quality register must be able to change status (sent, deleted, etc.).

3.2.1.4 Archival of personal data

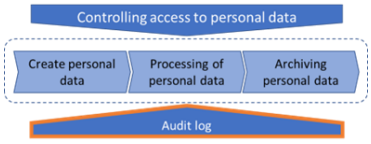


Personal data, medical records and patient records is saved for ten years after the last entry was made, or even longer in some situations. Thereafter, the data and associated metadata are either erased (i.e., permanently deleted), preserved (i.e., archived in a separate medical records archive) or anonymized.

Under certain conditions, patient records need to be taken care of, stored separately with an archive authority, and then be returned.

Data in the CDR need to be searched for, exported in standardized formats, packaged, deleted from, and returned to the CDR. In some situations, bulk operations of data are necessary such as deletion or anonymizations of data that meet certain criteria.

3.2.1.5 Audit Log



Audit logs shall occur in all components in the solution and shall be designed in a standardized manner, following international and national standards[14], to:

- to ensure that the information stored in a log is sufficient to clearly reconstruct a detailed chronology of events that have affected the content of the stored data.
- ensure auditing of actions related to personal data can be reliably tracked

[14] ISO/IEC 27002:2022 - Information security, cybersecurity and privacy protection — Information security controls, ISO 27789:2021 - Health informatics — Audit trails for electronic health records, ISO 27789:2021 - Health informatics — Audit trails for electronic health records, IHE ITI TF Vol1, AuditEvent - FHIR v4.0.1 (hl7.org)

- ensure that the customer can store logs from different components and applications in the solution in a unified manner.

All audit logs from the components in the solution will be exported to the Karolinska's own SIEM-system. The system shall provide a rich set of triggers (instrumentation) where the customer can configure the triggers. The metadata to be included in a log shall also be under the control of the customer, allowing them to adjust the content according to changes in laws and local regulations.

3.2.2 Components for fine-grained metadata-based access control

The purpose of this chapter is to describe the functions and components resulting from Karolinska's interpretation of the laws and regulations as described in chapter *3.2.1.* Figure 4 show a more detailed overview of the logical components and services needed to augment a standard openEHR-based system to comply with regulations. The different components and their behaviors are described in more detail in the following sections.

These components and their exact behavior will be part of a joint development/integration effort in later stages in the procurement. The scope in this chapter is for the Supplier to understand the complexity of this delivery.

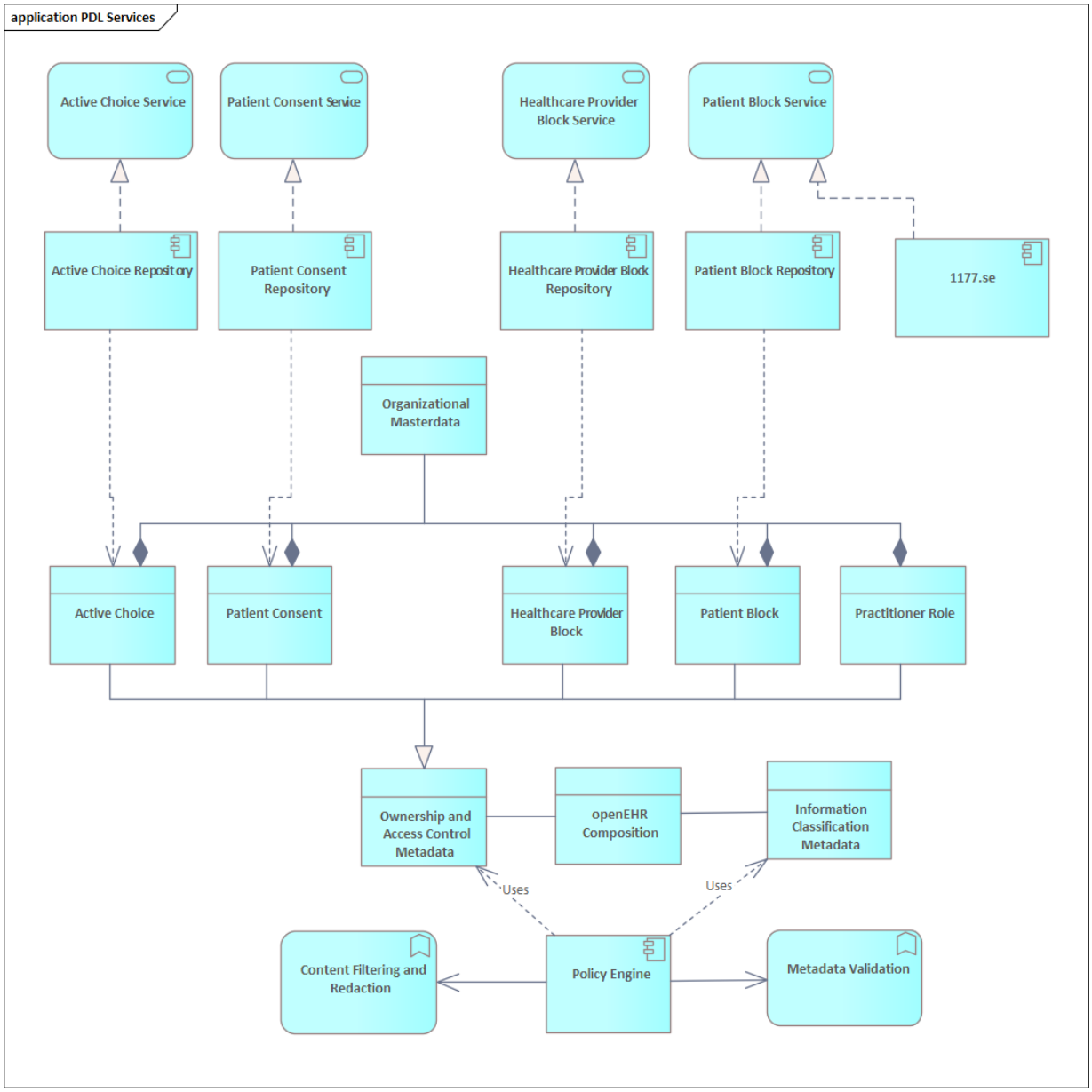


Figure 4 Specialization of ownership and access control metadata to implement PDL. Specific types of metadata are managed in a dedicated repository each with its own set of services. These specializations all include organizational master data.

The described repositories in Figure 4 can be seen as logically separated, there are relations between the information in the different repositories. For example, an active choice can be utilized to temporarily unblock a patient consent.

3.2.2.1 Content Filtering and Redaction

One of the most important functions to fulfil the requirements in Swedish laws and regulations is the Content Filtering Redaction function. All the information from the mentioned services below should be usable in this filtering function. The function shall be able to filter the information in the CDR, based on what a user in an application connected to the CDR is authorized to access. The function should come with an open specification and administration interface.

3.2.2.2 Patient blocks repository and service

The solution should include a repository where information about patients' blocks can be stored. The solution should also include an administrative function with a graphical user interface where a user should be able to read, create, cancel, and temporarily inactivate patient blocks. The repository shall integrate with the Swedish national block service, provided by Inera AB[15] and blocks created via this service should be used in the requested solution. The requested solution should also have the ability to manage patient blocks beyond those defined by Inera AB, to cover local needs that have not yet been developed or are out of scope for the national consent service or are managed in the main Electronic Health Record (HER). Information about patient blocks is also managed in Karolinska's main EHR, which means that the solution should have the ability to communicate this data with the main EHR.

3.2.2.3 Patient consent repository and service

The solution should include a repository where information about patient consents can be stored. The solution should also include an administrative function with a graphical user interface where a user should be able to read, create, cancel, and inactivate patient consents, (some types of patient consents must also be possible to be document trough an end user application). The repository should integrate with the Swedish national consent service provided by Inera AB[16], and consents created via this service should be used in the requested solution. The requested solution should also have the ability to manage consents beyond those defined by Inera AB to cover local needs that have not yet been developed or are out of scope for the national consent service. Information about patient consents is also managed in Karolinska's main EHR, which means that the solution should have the ability to communicate this data with the main EHR.

3.2.2.4 Active choice repository (and service)

In the applications connected to the CDR, various types of active choices will be made, and certain active choices will remain valid for a specific period. This means that the user will not be required to make the same active choice repeatedly during the valid timeframe.

In the solution, various types of active choices shall be able to be configured, so the active choices related to the CDR can be uniformed in what information that can or are required to store.

3.2.2.5 Services and repository for limiting exposure of personal data

The solution should include a repository and associated services where information classification metadata can be stored and retrieved, see chapter 3.2.1.2.3. This metadata is typically managed by a PDL healthcare provider to protect or release specific types of data. The services should also be able to integrate with the Electronic Medical Record and other healthcare systems.

This metadata can be scoped and applied on multiple levels:

- Entire CDR (all EHRs and Compositions)
- Groups of EHRs (cohorts of patients, all Compositions)
- Single EHRs (all Compositions)
- Groups of Compositions
- Single Composition

[15] rivta.se/tkview/#/domain/informationsecurity:authorization:blocking
[16] rivta.se/tkview/#/domain/informationsecurity:authorization:consent

3.2.2.6 Metadata validation function

The solution needs to come with a function for metadata validation, that can be used when a composition is written to the CDR, e.g., to validate the correctness of the data. Masterdata for organization and person (e.g., healthcare practitioners) must be retrieved from Masterdata sources.

3.2.2.7 Patient Master Index

The solution must have functionality for a patient master index (PMI) to allow healthcare providers to access a complete and consolidated view of a patient's demographical data. The PMI component will integrate with public and regional sources of Masterdata, like census databases.

Please also refer to chapter 3.1.2 for a broader description of the PMI component.

3.2.2.8 Identity Access Management

The openEHR specification does not specify in detail how to implement access control. This is left to the organization who implements the solution. As the service APIs are all exposed using the HTTP protocol it makes sense to adopt relevant web-standards for a modular and open realization.

Figure 9 shows a typical architecture where HTTP-based standards like OAuth2 and OpenID Connect are used to implement access control.

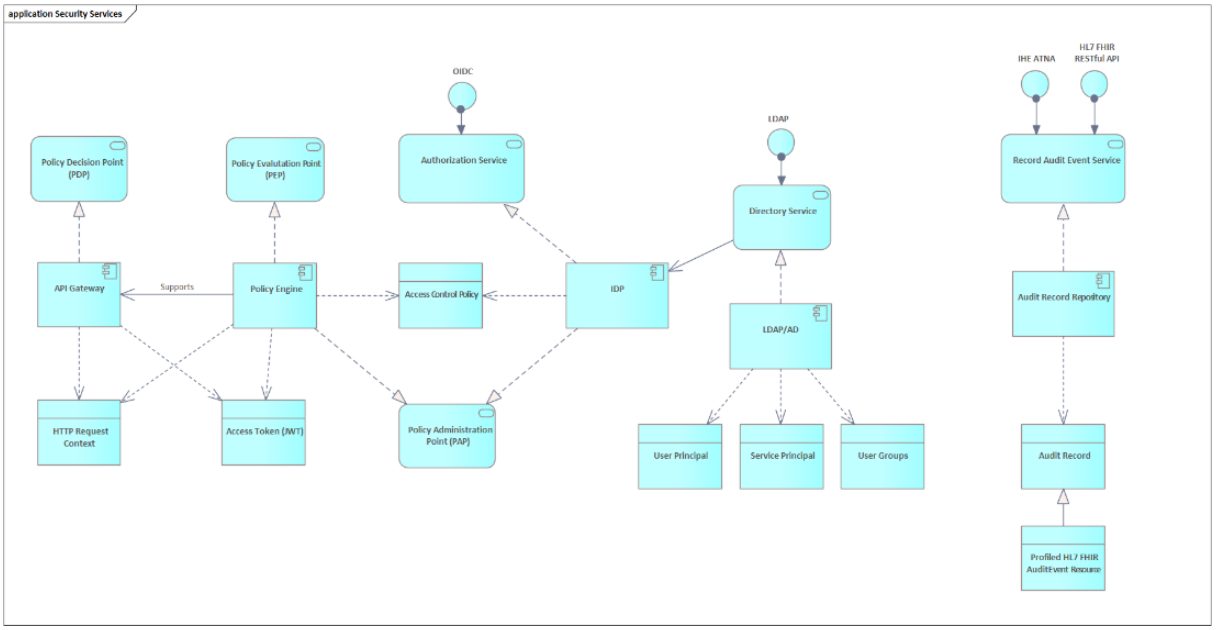


Figure 5 Typical supporting services for access control and audit logging. In this opinionated view, policy logic is externalized to a dedicated Policy Engine

The IDP component and the Policy Engine are used together to implement RBAC or ABAC based access control policies. However, to comply with Swedish regulations additional functionality must be added to the architecture, see 3.1.2.

3.3 Subcategory 1c: Software for rapid development, publication, and maintenance of openEHR-based applications

Subcategory 1c covers important tools and resources that are needed to configure and get an openEHR CDR-based system up and running with end user entry forms, dashboards etc. This should be done in a way so that the combination of subcategories 1a, 1b and 1c can be used in daily work by clinicians. It must be possible to configure the user interface and content (templates, forms, simple form logic) by informaticians and super users that are not software developers.

To extract maximum value of an openEHR-based eco-system we want to procure tools for building applications. The openEHR formalism lends itself naturally to generative and low code approaches. Simple application components such as forms can be completely or in parts generated from a template specification by informaticians and subject matter experts who are not software developers.

The forms-based applications can be statically generated or rendered at runtime from an intermediary specification, see Figure 6. The form builder service typically include support from a terminology service and a library of snippets or widgets to help developers bind terminology excerpts to form input fields.

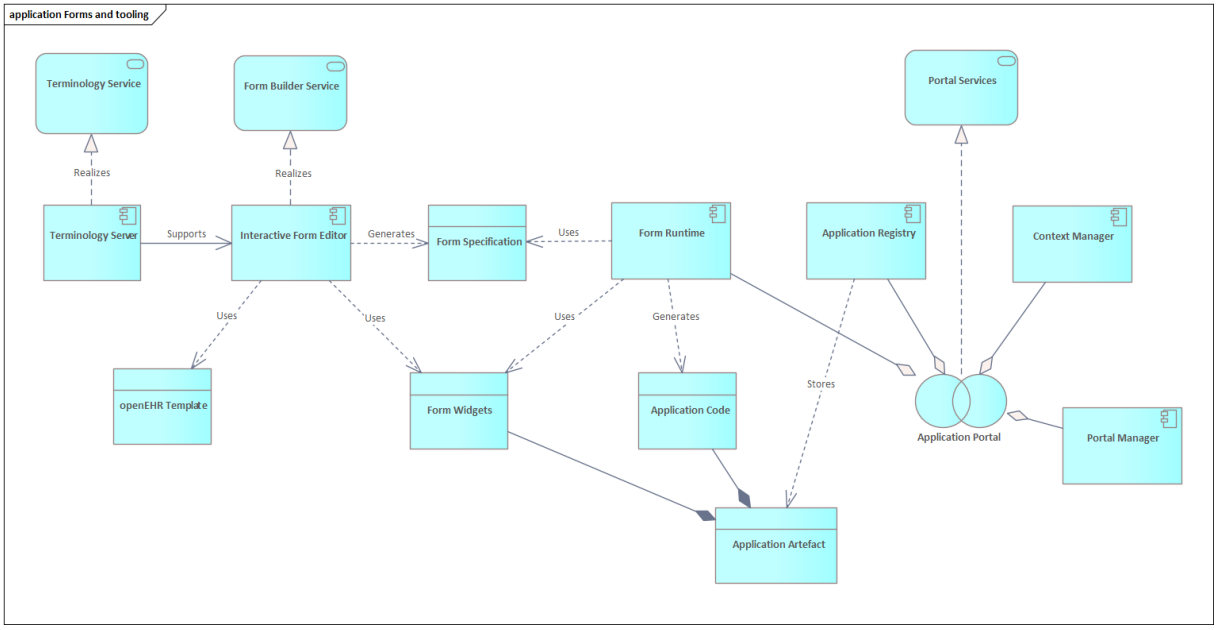


Figure 6 Example architecture for a form builder service. openEHR templates are used by an interactive form editor to provide input to a code generator. Application artifacts are published to an application portal where the application can be operated and accessed.

The applications can then be published to a shared application portal service where the applications can be accessed and operated. Another possibility is to embed applications into existing systems like an existing EMR/EHR system or separate web applications.

Karolinska's vision is to be able to quickly build needed clinical functionality based on platform services and expose this functionality as applications in a cohesive and easy to use manner. For further ease of use, the application portal could also expose context management services to be able to maintain a given patient context across multiple application instances.

Main functions that likely will be procured in this area are (but not limited to):

- Low-code (or similar) tools for creating and rendering UI entry forms, dashboards, other views, and overviews. Some pluggable openly published architecture for additional widgets may also be requested, see e.g. discussion in https://discourse.openehr.org/t/standardised-api-for-custom-gui-widgets-for-openehr-based-form-editors-renderers/1936
- AQL query building and execution tools. A tool or tools are needed to create, manage, validate, and save AQL queries, including parametric queries. There is also the need to visualize and export AQL query responses.
- End user facing portal functions. In some cases, software developers will build separate applications that do not need a portal, but often simple applications built/configured using low code tools for data entry forms, dashboards, other views, and overviews will be enough. Such simple applications need a framework to run in to select patient, select view and look at existing data.
- Design language and pre-made configurable widgets. A coherent set of UI design principles and widgets that can be used also in our own custom development in a way that can be seamlessly combined with low code generated parts of the UI.

During the Swedish 2003 RFI responses and demos, proprietary low-code UI building tools were presented. Since there is no standard for these, there is a risk of future lock-in effect regarding forms and applications if we would choose to change vendor for such functions later (requiring a lot of conversion work during short time). We will expect solutions to support a soft exit strategy with continued use of *already created* forms/apps (and use of design language) for some years by contractual, technical, or other means.

3.4 Subcategory 1d: Software services

In addition to the delivery of Software, as described above, we also need supporting services for operations, testing, implementation, and other Software life-cycle activities. We envision a holistic implementation approach, where the supplier of Software manages the delivery of these services for all Software in subcategories 1a, 1b and 1c.

These services include:

- Upgrades and updates to delivered Software
- Installation, configuration, and implementation services
- Acceptance- and performance testing services
- Services for operating installations in our IT-environment or as an external Service (SaaS)
- Customer specific modifications and extensions of delivered software

The testing services include managing and providing test data as well as controlled environments for testing. These environments can be operated by the Supplier but must be accessible by the Contracting entities.

4 Category 2: Software for openEHR Content Creation and Transformations

Category 2 is rather openly defined and primarily has some high-level requirements. It covers openEHR-related tools, SDKs (Software development Kits) and other utilities. We assume that many such tools will be included in the software and service offerings of subcategories 1a, 1b and 1c, but want a way to access the market for openEHR-related software that can be procured separately and that does not necessarily come bundled together with a particular CDR. We are interested the software and associated professional support in this category different suppliers can provide. Open-Source software can also be listed, provided that professional support for such software is included.

Tools in this category are tools that can be used to perform tasks related to the core components of the ecosystem which are described in the previous sections, i.e., an openEHR-based clinical data repository and relating systems and services. Development tools are needed to manage and further develop content in these core components as well as applications based upon them.

Examples of software

- Tools and SDKs (Software Development Kit) for creating, maintaining, or transforming openEHR models such as archetypes, templates, AQL queries, process- or decision support rules.
- Tools and SDKs for creating, maintaining, or transforming openEHR data instances such as Compositions and other CDR content. This includes integration tools that have specific support for openEHR formalisms and has been proven to work for openEHR content.

5 Category 3: Consulting services

This category concerns consulting services. The Consulting Services Providers must be able to deliver expertise regarding openEHR and/or SNOMED CT. The same Consulting Services Providers should also be able to provide competence regarding HL7 FHIR, HL7 v2, DICOM, bioinformatics/omic-standards and related terminologies/ontologies etc. when needed.

The openEHR-, SNOMED CT- and other health IT-standards-communities are global, but non-European or small companies sometimes find it difficult to engage with European public organizations and their procurement processes. Therefore, collaboration between Consulting Services Providers is encouraged, e.g., European and non-European partners via subcontracting etc.

Region Stockholm and Karolinska already have other contracts, agreements, and ways to procure general IT-consulting services. Responding Consulting Services Providers that are **not** providing proof of the requested openEHR or SNOMED CT expertise will be rejected.

The consulting service requested in this RFP are resource and assignment consulting services, defined and exemplified below in separate sections.

Region Stockholm and Karolinska have good internal competence regarding openEHR and SNOMED CT. In addition to this we seek to procure the following services:

(a) Experts to advise and train our staff, or to solve thorny issues,
(b) Staff augmentation in cases where we have a lack of staff with enough assignable time to perform planned tasks.

Issues of type (a) usually require far more experienced consultants than issues of type (b).

In the procurement process (step 2) selected companies will have the opportunity to offer consulting services within defined competence areas and competence levels. We will likely make use of formal competence level descriptions based on the general profile descriptions in “Kammarkollegiets kompetensmodell”[17] from the Swedish Chamber of Commerce and consider different pricing options for different services and competence levels.

Skilled authors and maintainers of (e.g., open source) software, tools and frameworks intended for openEHR- and SNOMED CT-related needs/tasks can be considered to have (narrow) top level competency regarding those specific tools/frameworks, access to such competence is thus of interest to us.

Karolinska will purchase consulting services in subcategories:

1. Subcategory 3a: Resource consulting service, and
2. Subcategory 3b: Assignment consulting service

[17] For example visible in chapter 2 of https://www.avropa.se/globalassets/bilagor/1.-aktuella-rao/itk-2020/4.-arkitektur-och-utveckling/gemensamt-for-ao4/exempelroller-och-kompetensnivaer-delomrade-4---arkitektur-och-utveckling_230207.pdf and an unofficial English translation at https://support.cinode.com/en/articles/4255561-skill-levels-definitions

5.1 The consulting services (category 3) in relation to other categories and subcategories

The general assumption in Category 3 Consulting Services is that any resulting solutions will be owned by Region Stockholm or Karolinska which includes that we have the right to e.g., publish them as open source at our own discretion.

Consulting services relating to proprietary software solutions tools and frameworks, or improvements and customer specific modifications and extensions of them, made by and maintained by providers belong to the provider and is covered in as different services included in Categories 1 and 2.

5.2 Subcategory 3a: Resource consulting service

Resource consultant refers to a consultant who constitutes a resource reinforcement, in a certain project or for a certain assignment, who is supervised by Karolinska.

Example tasks for top *expert* (international guru) consultants can be to help solving specific complicated issues and designs. Other tasks include training within specific subjects and support our informaticians or integration experts.

Example tasks for *general* openEHR- and SNOMED CT-competent resource consultants can be as a part of a project team creating or maintaining some openEHR templates including associated SNOMED CT bindings and value sets. Other tasks include to create and maintain forms with built in conditional logic based on openEHR and SNOMED CT.

There will likely not be a need for junior inexperienced resource consultants.

5.3 Subcategory 3b: Assignment consulting service

Assignment consulting service means that the framework agreement supplier provides consultants and takes the main responsibility for the execution of a certain specified task and produces a certain agreed result.

Example assignments may be to develop clinical applications, EHR modules or functionality based on openEHR and SNOMED CT. This could for example be ordered as something either built from scratch or alternatively based on relevant open-source frameworks. Assignments may also include improving or creating open-source frameworks where Karolinska finds needs for improvements.