**REQUIREMENTS FOR THE OBJECT OF TENDER**

OpenEHR software implementation, configuration, and training services

Table of Contents

Contents

[2. OpenEHR deployment project 4](#_Toc189213537)

[1.1. Project description and primary objectives 4](#_Toc189213538)

[1.2. Terms and abbreviation 4](#_Toc189213539)

[3. Functional requirements 5](#_Toc189213540)

[1.3. General requirements 5](#_Toc189213541)

[1.4. Solution to store and manage clinical data based on openEHR specifications 5](#_Toc189213542)

[1.4.1. Clinical data repository (CDR) 5](#_Toc189213543)

[1.4.2. FHIR based-based master patient index (MPI). 5](#_Toc189213544)

[1.4.3. Data integration 6](#_Toc189213545)

[1.5. Solution for creation and managing content 6](#_Toc189213546)

[1.5.1. Content creation and management 6](#_Toc189213547)

[1.6. Other requirements 7](#_Toc189213548)

[1.6.1. General other requirements 7](#_Toc189213549)

[1.6.2. Authorization and access control 7](#_Toc189213550)

[1.6.3. Processing of Personal data. 7](#_Toc189213551)

[1.6.4. Workflow management and automation. 7](#_Toc189213552)

[1.6.5. User task management and internal notifications. 7](#_Toc189213553)

[1.6.6. Tailored non-functional requirements 8](#_Toc189213554)

[1.7. Governance requirements 8](#_Toc189213555)

[1.7.1. Policy-driven workflow design 8](#_Toc189213556)

[1.7.2. Monitoring and compliance 8](#_Toc189213557)

[1.7.3. Language requirements 8](#_Toc189213558)

[4. Non-functional requirements 8](#_Toc189213559)

[1.8. Requirements for reliability 8](#_Toc189213560)

[1.9. Requirements for security 9](#_Toc189213561)

[5. Implementation stages & results 10](#_Toc189213562)

[6. Requirements for project phases and deployment 13](#_Toc189213563)

[1.10. Requirements for analysis and design 13](#_Toc189213564)

[1.11. Implementation and deployment requirements 13](#_Toc189213565)

[1.12. Training requirements 14](#_Toc189213566)

[1.13. Testing requirements 14](#_Toc189213567)

[7. Requirements for general service provision 15](#_Toc189213568)

[1.14. Project language 15](#_Toc189213569)

[1.15. Requirements for documentation and its coordination 15](#_Toc189213570)

[1.16. Requirements for project management 15](#_Toc189213571)

[1.17. Requirements for change management 16](#_Toc189213572)

[1.18. Licensing requirements 17](#_Toc189213573)

[1.19. Requirements for warranty 17](#_Toc189213574)

[1.19.1. General warranty requirements 17](#_Toc189213575)

[1.19.2. Incident management 17](#_Toc189213576)

[1.19.3. Support & maintenance 18](#_Toc189213577)

[1.20. General project requirements 18](#_Toc189213578)

# OpenEHR deployment project

## Project description and primary objectives

The goal of the openEHR module deployment project is to evaluate the suitability of openEHR for modeling and storing medical data and to assess its potential for broader adoption in Lithuania’s healthcare information systems in the future. In this initial phase, the project will focus on developing, testing and implementing an openEHR platform for the Cardiology use case at a pilot hospital. While the pilot platform will function independently, its workflows will align with the existing Health Information System (HIS) (data integration with HIS should be developed during the project).

Key objectives

* Validate the feasibility of openEHR for modeling medical forms and storing cardiology data, with scalability for future use cases.
* Assess openEHR’s interoperability with existing HIS workflows and infrastructure.
* Identify technical, operational, and organizational challenges in integrating openEHR with and into current systems.
* Evaluate the potential for scaling openEHR across Lithuania’s healthcare system to ensure broader adoption and long-term impact.
* By conducting this pilot, Lithuania aims to explore the potential of openEHR as a modern and scalable solution for healthcare data management.

## Terms and abbreviation

Terms and abbreviations used are presented in table 1 “Terms and abbreviations used “.

Table 1. Terms and abbreviations used

| Term/abbreviation | Description |
| --- | --- |
| API | Application programing interface |
| Client | State Enterprise Centre of Registers or RC |
| ESPBI IS | Lithuania's Electronic Health Services and Cooperation Infrastructure Information System (lit. *Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema*) |
| FHIR | Fast Healthcare Interoperability Resources |
| IS | Information system |
| JSON | JavaScript Object Notation |
| RC | State Enterprise Centre of Registers (lit. *Registrų centras*) |
| SAM | Ministry of Health (lit. *Sveikatos apsaugos ministerija*) |
| Service provider | The company that is providing software development services for the implementation of the project. |
| XML | eXtensible Markup Language |

# Functional requirements

## General requirements

1. As part of the openEHR based software, it is anticipated to provide solution that NOT ONLY stores clinical data as clinical data repository based on openEHR standards but also solution that enable full realization of the ecosystem as illustrated by the openEHR architectural overview[[1]](#footnote-2).

## Solution to store and manage clinical data based on openEHR specifications

## Clinical data repository (CDR)

1. Solution to store clinical data and documents. This should support secure insertion, updating, retrieval, version control and access.
2. The CDR to be provided shall support and service the following, including, but not limited to;
   1. Indexing service according to IHE/XDS standards.
   2. openEHR EHR API
   3. openEHR Query API
   4. openEHR Definition API
   5. Audit and monitoring
   6. Bulk insertion and querying capabilities that will not lead to timeouts. Multiple data formats need to be supported; (e.g. PDF, XML, JSON)
   7. Supporting tools for Repository and Knowledge management services.
   8. On premises installation and configuration.
3. While there are no restrictions on the choice of database system, it is important to note that the pilot site uses the OpenShift platform to host applications and services. Therefore, any database system selected/used must support the openEHR software in meeting performance requirements and operate effectively as an on-premise service.

## FHIR based-based master patient index (MPI).

1. Support for FHIR based Master Patient Index (MPI) to manage Demographics data.
2. While an MPI is an external service to the openEHR CDR, it is important to ensure that the correct EHRs are created in the CDR and properly linked to the corresponding patient records. Therefore, the provided CDR must support and integrate seamlessly with the pilot site's master patient record system. Additionally, it must support patient merging in cases where patients are assigned new identifiers.
3. In cases where a patient identifier does not exist, the CDR must still be able to create an EHR for the patient and ensure that each created EHR is uniquely associated with one patient identifier.

## Data integration

1. Solution must ensure that integration with the hospital information system (HIS) of the selected pilot hospital, which will be the sole HIS used for managing clinical data in this implementation, is prepared during the project.
2. Additionally, the OpenEHR-based solution must provide the capability to manage terminology data, including but not limited to SNOMED CT, LOINC, ICD-10, and other relevant classifications.

## Solution for creation and managing content

## Content creation and management

1. The provided solution must support the creation, modification, version control, translation into Lithuanian and management of openEHR artifacts, including archetypes, templates, and compositions.
2. The solution must support the modeling of forms for creating compositions, offering form elements such as radio buttons, checkboxes, and other interactive components.
3. Creation and Modification. The solution provided shall provide tools and SDKs to enable the creation and editing of openEHR artifacts.
4. Version Control. It should include robust version control capabilities to track changes and updates.
5. Translation. The solution must support translation of artifacts into Lithuanian.
6. Management. It should facilitate the efficient management of openEHR artifacts, including archetypes, templates, and compositions.
   1. Categorizing and storing archetypes, templates, and compositions in a structured and accessible way.
   2. Grouping artifacts by use case, clinical domain, or project.
   3. Supporting processes for updating, retiring, or archiving outdated artifacts.
   4. Ensuring compliance with clinical and technical standards throughout their lifecycle.
   5. Enabling collaborative workflows, such as allowing multiple users to work on artifacts with proper access controls.
   6. Implementing user roles and permissions for creating, editing, or approving changes.
   7. Providing tools for tracking changes, including detailed logs of who modified what and when.
   8. Supporting traceability for artifact versions.
   9. Allowing users to easily search for and retrieve specific artifacts using metadata or clinical context.
7. Form Modeling. The solution should enable the creation of forms for generating compositions.
8. Interactive Components. It must support form elements such as radio buttons, checkboxes, and other interactive components.
9. Flexibility. Ensure that the form modeling supports customization to meet diverse clinical needs.

## Other requirements

## General other requirements

1. In addition to delivering the core openEHR-based software, supporting services will be required to ensure a successful pilot implementation. These services will focus on the delivery, installation, and configuration of the openEHR platform within the pilot site's environment. The supplier will provide essential updates and basic modifications necessary for the pilot's functionality, alongside streamlined testing services, including acceptance testing and performance evaluations. The supplier will also prepare testing environments and relevant test data, ensuring controlled and accessible conditions for evaluation by the contracting entities, leveraging the Dev, Test, and Prod environments provided by the pilot site.
2. The pilot's scope prioritizes a lightweight and focused approach, emphasizing critical Software functionality and ease of integration into our environment. While customer-specific extensions and advanced configurations are not central to this phase, minor adaptations that demonstrate feasibility and alignment with our requirements are encouraged. The supplier's role will include supporting the pilot's operational aspects, ensuring a reliable demonstration of the Software's capabilities within the defined timeframe

## Authorization and access control

1. A solution or service for access control must be provided, incorporating role-based access control (RBAC) to ensure data security and privacy. The pilot hospital already has an identity access management system in place, the openEHR platform provider shall integrate this existing component with the openEHR solution. The integration must guarantee that security and privacy filtering functions operate correctly in accordance with established privacy and security policies.

## Processing of Personal data.

1. In compliance with GDPR, patients have the right to request the blocking and access of their personal data. To support this, the provided solutions must align with the pilot site’s approach to data blocking, adhere to established privacy and consent policies, or support integration with the existing patient consent system.

## Workflow management and automation.

1. The solution must enable the management of workflows, including the assignment of workflows to specific medical forms.

## User task management and internal notifications.

1. The solution should provide task management capabilities, allowing users to review assigned tasks, categorize them, and track their progress.
2. Furthermore, the solution must include a notification system that sends reminders to users who fail to respond to tasks within a specified timeframe, ensuring timely completion and accountability.

## Tailored non-functional requirements

1. Non-functional requirements will be tailored to the pilot's scope, focusing on practicality. Unicode UTF-8 encoding will ensure support for Lithuanian data inputs. While long-term goals like SOA adherence and scalability are acknowledged, the pilot will leverage existing components and minimize custom development. This approach emphasizes validating core functionalities and gathering insights for policy-level evaluation.
2. The pilot will deliver a streamlined solution to evaluate feasibility and performance, focusing on core functionalities like storing and querying openEHR data. AQL capabilities, such as "EXISTS," will enable essential data retrieval and analysis. Simple usage metrics, like tracking frequently accessed archetypes, will provide insights for optimization without added complexity. Data integrity, availability, and real-time synchronization will ensure system reliability.

## Governance requirements

1. The solutions provider must ensure that all services and solutions delivered during the pilot are designed to operate effectively, meeting defined performance standards. These solutions should prioritize efficient service delivery, robust security, and seamless operation tailored to the specific needs of the pilot site. Additionally, the provider should ensure that the solutions are reliable, compliant with relevant standards, and adaptable to accommodate feedback and adjustments during the pilot period.

## Policy-driven workflow design

1. Solution provider shall ensure workflows and form triggers align with clinical guidelines, operational policies, and governance standards.

## Monitoring and compliance

Establish oversight mechanisms to review workflow effectiveness, task completion rates, and adherence to reminders, ensuring compliance with established operational goals.

## Language requirements

1. Documentation must be provided in both Lithuanian and English.
2. Communication during the project may take place in either Lithuanian or English.
3. User training must be conducted in either Lithuanian or English.

# Non-functional requirements

## Requirements for reliability

1. Solution must have 99.75% overall availability and 99.99% communication availability outside of scheduled maintenance periods.
2. Solution must have mechanisms established to ensure that, in the event of a system failure, data is not lost.
3. Solution must implement a business continuity process that allows it to continue functioning in the event of a failure, operating at the required volume and processing any backlog within the required period.
4. Solution must be able to restore uncorrupted data from backups to a suitable point, resuming processing without losing or duplicating incoming or outgoing messages.
5. Solution must be able to detect the loss and duplication of messages transmitted to/from it and have the capability to correct them.
6. Solution must be consistent, ensuring that a specific incoming message request yields the same result regardless of how many times it is performed.
7. Solution must support backup, recovery, and restoration of data.

## Requirements for security

1. Security measures should be ensured to be compliant with:
   1. Law on Legal Protection of Personal Data of the Republic of Lithuania and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and by which repealing Directive 95/46/EC (General Data Protection Regulation).
   2. Law on The Management of Information Resources of the State of the Republic of Lithuania, the Law on Cybersecurity of the Republic of Lithuania, the Description of the General Requirements for Electronic Information Security, approved by Resolution No. 716 of the Government of the Republic of Lithuania of 24 July 2013 "On the Description of general requirements for electronic information security, Description of the guidelines for the content of security documents T-29 Description of organizational and technical cybersecurity requirements applicable to cybersecurity entities, approved by Resolution No. 818 of the Government of the Republic of Lithuania of 13 August 2018 "On the Implementation of the Law on Cybersecurity of the Republic of Lithuania", and other relevant legal requirements including government resolutions on electronic information security.
2. During implementation process Service provider shall follow best market practices for cybersecurity as security management standard LST ISO/IEC 27001:2022 "Information technology or similar.
3. Solution must ensure the integrity of medical forms, protecting them from unauthorized modifications.
4. Solution must detect and record unauthorized access attempts.
5. Solution must encrypt data at rest using industry-standard encryption algorithms.

# Implementation stages & results

Table 2. Implementation stages

| **Stage** | **Responsibilities** | **Result** | **Results / Requirements** |
| --- | --- | --- | --- |
| Initiation | Service provider:   * Prepares the Service Provision Regulation and other project planning documents. * Coordinates with the Client on project objectives related to Solution implementation.   Client:   * Provides necessary information regarding the current system architecture and requirements. * Collaborates in defining the goals and expectations for Solution implementation. | R-1 – Solution implementation initiation document | * Prepared Service Provision Regulation, detailing:   1. project goals & priorities,   2. results (deliveries) description,   3. stakeholders,   4. project team & responsibilities (detailing organizational structure of decision-making process)   5. work schedule,   6. risks and their management methods,   7. communication principles,   8. criteria for interim and results acceptance,   9. change management procedures. |
| Analysis | Service provider:   * Conducts assessment of TO-BE situation. * Prepares detailed analysis documentation.   Client:   * Provides necessary information. * Provides comments and recommendations. * Approves the Service Provider's stage results. | R-2 – Solution requirement design report | * Prepared solution design report, detailing:   1. Descriptions of requirements implementation, including references to functions, screens, rules, restrictions, and related information. Describing additional functionalities that would be provided even not mentioned in the specification.   2. Clarification on whether requirements are implemented as part of the standard system or via modifications.   3. Descriptions of system parameters & configuration.   4. System architecture diagram and description of components, detailing how the solution integrates with the existing ESPBI architecture.   5. Detailed integration data, management, and deployment areas.   6. Role and permission details, including a complete list of roles, their definitions, and purposes.   7. Testing scenarios for each requirement. |
| Implementation (deployment) and configuration | Provider:   * Installs and configures Solution according to the agreed requirements. * Develops any necessary customizations or integrations. * Sets up data storage separately from ESPBI IS.   Client:   * Provides access to necessary systems and environments. * Supports in resolving any technical issues * Reviews and approves the implementation progress. | R-3 – Configured Solution report | * Solutions installed and configured. * User roles and permissions configured according to requirements. * Configurations documented, including installation guides and configuration settings, horizontal and vertical scaling strategies, etc. |
| Testing and validation | Service provider:   * Conducts testing, including functional, performance, and security tests. * Collects performance metrics such as response times, throughput, and resource utilization. * Plans and conducts pilot testing with select users.   Client:   * Provides feedback on the proposed validation and testing protocols. * Tests information system against defined testing scenarios. * Approves the testing protocols as part of the overall process. | R-4 – Internal testing report | * Prepared testing and validation protocols, including:   1. Defined evaluation methods for each requirement.   2. Developed test scenarios (Service provider shall prepare testing scenarios) and cases, including criteria for passing/failing.   3. Specifications for testing procedures and tools to be used. * Test results, including:   1. Test results documented, including any issues found and resolutions.   2. Performance metrics collected and analysed   3. Updated documentation reflecting any changes. |
| R-4 – UAT report | * Client could include additional testing scenarios. Client will test identified scenarios. * Service provider shall participate in testing sessions and provide consultations. * Client shall register bugs and client will need to solve the cases and participate in additional testing sessions if needed. |
| User manuals | Service provider:   * Develops user manuals that provide step-by-step instructions on how to use the Solution effectively. * Conducts training sessions for administrators and key users. | R-5 – User manuals and training materials | * Prepared Solutions user manuals and training materials. User manuals should include system configuration, system deployment procedure and other Solutions functions. |
| Warranty documentation | Service provider:   * Prepares a comprehensive document outlining the warranty supervision procedure; * Provides 12 months of warranty service, as stipulated in the contract.   Client:   * Operates the developed system as intended; * Documents any errors detected during the system’s operation. | R-6 – Warranty documentation | 1. Detailed document outlining the warranty supervision procedures. |

# Requirements for project phases and deployment

## Requirements for analysis and design

1. During the implementation of the analysis and design stages, the Service provider must carry out a detailed analysis and design of project needs.
2. The detailed requirements analysis document must include use cases prepared according to the functional and non-functional requirements of the Technical Specification and the needs expressed by the Client. These use cases should include usage case diagrams and detailed descriptions, specifying steps (main course, alternative course), and other constraints using Unified Modeling Language (UML) notation. All functional and non-functional requirements of the Technical Specification must be linked to the content of the detailed analysis document (chapters, appendices, diagrams, etc.). This linking must be clear in illustrating how each requirement of the RPO is designed and realized.
3. During the analysis and design stages, the Service provider shall conduct meetings with operational specialists appointed by the Client and specialists from other relevant institutions to ensure all stakeholder inputs are considered.
4. During the detailed analysis and design stages, the Service provider shall refine the functional and non-functional requirements of the RPO to develop a System that fully meets the expressed needs of the Client.

## Implementation and deployment requirements

1. Service provider is responsible for all configuration of the Solution.
2. For the installation of versions of the system into the Client's environments, the Service provider shall prepare a detailed Installation Plan.
3. The installation of versions of the system must be carried out in stages, with each service station using the System separately to ensure system integrity and minimal disruption.
4. The installation of versions of the system must follow the prescribed order:
5. A new version of the System is installed in the DEV environment.
   1. tests are performed on the installed version of the System.
      1. if testing is unsuccessful, necessary changes are made to the System, and the installation process is repeated.
      2. after successful completion of the tests, the installation process advances to the next stage.
   2. A new version of the System, successfully tested in the DEV environment, is installed in the TEST environment.
      1. tests are performed on the installed version of the System.
      2. if testing is unsuccessful, necessary changes are made to the System, and the installation process is repeated.
      3. after successful completion of the tests, the installation process is deemed complete.
6. During the installation of the version, the server where the installation work is being carried out will be inaccessible to users to prevent interference and maintain security.

## Training requirements

1. Training sessions must be provided for at least 20 designated users.
2. The training shall ensure that each user receives up to 40 hours of training. The training should not exceed 6 hours of training per day.
3. The Service provider shall ensure that the training includes practical, hands-on learning to equip users with the necessary skills for testing and evaluation.
4. Training can be delivered online via video calls.

## Testing requirements

1. Version tests of the Solution (hereinafter referred to as "Testing") must be carried out.
2. User-acceptance testing shall be carried out only if there are no critical issues identified within Service provider’s internal testing. Up to 10 non-critical issues could be identified.
3. The Service provider must select and possibly add to the following testing scenarios based on the business requirements and Client's needs):
   1. Ensure that all functional and non-functional requirements have been implemented.
   2. Verify that the requirements have been implemented to the appropriate extent.
   3. Determine whether the implementation satisfies the Client and other interested parties.
   4. Identify, register, and correct any functionality errors (bugs).
4. Testing should be conducted according to the Service provider prepared scenarios.
5. The Service provider must document the testing protocols and share them with the Client.
6. Service provider shall participate in all UAT testing sessions.
7. The results of the Testing, including any identified issues and their resolutions, must be reported to the Client in a timely manner.
8. All issues shall be registered in Client’s internal issue management system (JIRA).
9. The procurement will include 3 pre-configured forms for testing the capabilities of the modeling tool and server. Client will provide data of existing forms and the Service Provider shall configure these forms for internal testing and provide possibility to change these forms for UAT.
10. The forms should reflect real-world use cases in cardiology to validate the solution’s functionality.

# Requirements for general service provision

## Project language

1. Project documentation must be prepared in both Lithuanian and English languages. Interim documentation (non-final) may be prepared in a single language, however all final deliverables must be provided in both languages.
2. Project communication can be held in Lithuanian or English languages.
3. User training can be held in Lithuanian or English languages

## Requirements for documentation and its coordination

1. All project documentation prepared by the Service provider must be prepared in accordance with the rules of the respective language grammar and formatting rules illustrated with diagrams, tables, graphs and other visual means, the presented material is arranged clearly, consistently and in detail.
2. Project documentation must be updated according to project stages, activities, and all approved decisions. Final versions must reflect any changes (even previously approved documents) unless agreed otherwise.
3. Project documentation must be stored and coordinated in the Client's Confluence environment, while project task management must be carried out in the Client's Jira environment. Access to these systems will be provided by the Client at the start of the project.
4. The Service Provider must align all document templates with the Client. While document structure may evolve during the project, they should be submitted at the beginning each document preparation phase to align initial expectations.
5. The final versions of the documents must be submitted electronically in a format suitable for editing (e.g., .doc, .docx, or another agreed format), including diagrams and other content, unless agreed otherwise. Diagrams must be prepared using the draw.io tool.
6. Client and other relevant parties commit to reviewing the documentation and providing comments within no more than **5 business days**
7. The Client’s GitLab repository must be used to store the system source codes.

## Requirements for project management

1. The Service provider must cooperate directly with the Client, Project partners, and other interested parties involved in the Project. This includes maintaining open lines of communication and collaboration throughout the project duration.
2. The Service provider shall regularly inform the Client about the progress of the Services and, upon the Client's request, prepare and present results at various stages of service provision.
3. The Service provider must submit and agree with the Client on the Regulation of Service Provision, which should detail the stages of the provision of services and their results (presentations), a calendar schedule for the execution of phases corresponding to the detailed deadlines specified by the Client, describe communication and risk management measures and the procedure for combining documents.
4. The Service provider shall prepare and submit to the Client monthly interim reports on the provision of services, which shall include:
   1. Updates on the progress of the Service Agreement.
   2. Information about the risks and problems recorded during the reporting month.
   3. Updates on any agreed changes in the change register.
5. Interim reports on the provision of Services must be submitted to the Client within 5 working days from the end of the reporting period.
6. Upon completion of all works, the Service provider shall prepare a final report on the provision of services. This final report must be submitted to the Client within 10 business days from the end of the last stage of Service Provision.
7. The Service provider must continue to cooperate directly with the Client, the Project partners, and other interested parties throughout the project, ensuring all stakeholders are engaged and informed.

## Requirements for change management

1. Client reserves the right (but is not obligated) to order additional services from the Service Provider based on the hourly rate specified in the proposal. The scope of additional services is up to 1000 working hours.
2. Service Provider must apply an hourly rate no higher than specified in the proposal. Before starting additional work, the Service Provider must provide a detailed task description, time estimates with justifications, and an implementation timeline, all of which must be agreed upon with the Client. The Client reserves the right to approve or reject the change request based on the evaluation. The preparation of the estimate must be done at the Service Provider's expense.
3. Service Provider must establish and agree with the Client on a detailed procedure for providing additional services, including rules for identifying, calculating, and documenting additional service orders.
4. These are preliminary types of possible additional services:
   1. Modifications for unforeseen areas or functionality.
   2. Implementation of additional integration interfaces.
   3. Additional training or consultations.
   4. Other tasks agreed upon with the Client.
5. Service Provider must account for and include in their calculations all project documentation to be prepared or updated, along with any necessary modifications, to achieve the objectives of the change request.
6. Additional services are subject to the same warranty period as the System. If additional service results are delivered near the end of the warranty period, a minimum warranty of two (2) months will apply to those results.

## Licensing requirements

1. Licenses shall be provided for up to 20 users.
2. Number of patients that data will be used for the system will not exceed 10 thousand patients.
3. Licenses shall be perpetual (software-as-a-service (SaaS) shall not be acceptable).
4. If the Solution will be used by external additional organizations or additional users, the licensing model can change and result into separate procurement.
5. Solution should be accessible even without ordered maintenance.

## Requirements for warranty

## General warranty requirements

1. Service Provider must ensure warranty for the developed solution and installed licensed software.
2. Warranty period is 12 months from the signing of the final delivery-acceptance act.
3. If the solution is delivered and implemented in parts (not as a full scope), the warranty will apply separately to each part upon its deployment. However, the overall warranty for the entire solution will start upon final deployment and remain valid for the full specified warranty period.
4. Service Provider must coordinate a detailed warranty maintenance procedure with the Client before the beginning of warranty period.

## Incident management

1. There are 2 types of incidents:
   1. Critical issues. System outages, critical functionality failures, or issues like security breaches or data corruption.
   2. Non-critical issues. Minor disruptions, cosmetic errors, or problems with available workarounds.
2. Response and resolution times:
   1. Critical issues:
      1. Respond within **4 hours**, regardless of time or day.
      2. Resolve and restore the system within **2 business days**.
   2. Non-critical issues:
      1. Respond within **8 hours** during working hours; outside working hours, respond the next business day.
      2. Resolve within **5 business days**.
3. Incidents must be registered and tracked in the Client's issue management software JIRA.
4. Warranty services must operate from 08:00 to 18:00 (Lithuanian time zone), including weekends and public holidays.

## Support & maintenance

1. Telephone and email support ("Hotline") must be available during the Client's business hours.
2. Updates to system source code must be provided for Client review after corrections are made.
3. During the warranty period, the Service Provider must update the software if a new version becomes available

## General project requirements

1. Examples, attributes, criteria, parameters, rules, and classifiers mentioned in the requirements are indicative and not exhaustive. These must be detailed and agreed upon with the Client during analysis and design phases.
2. All necessary data fields for proper system functionality must be included, with character limits and integration methods agreed upon during analysis and design.

1. https://specifications.openehr.org/releases/BASE/latest/architecture\_overview.html [↑](#footnote-ref-2)