Appendix I to the CALL FOR TENDERS FOR THE PROVISION OF IT SERVICES FOR THE PRISON HEALTH CARE IN ARMENIA

2021AO72

UNDER THE PROJECT OF THE COUNCIL OF EUROPE “ENHANCING HEALTH CARE AND HUMAN RIGHTS PROTECTION IN ARMENIA”

BUSINESS AND TECHNICAL REQUIREMENTS

CONTENTS

Abbreviations

2FA	Two-Factor Authentication
BP	Business Process
EKENG	e-Governance infrastructure implementation agency
EMS	Electronic Medical System
FLM	First name, Last name, Middle name
GIP	Government Interoperability Platform
Id document	Identity document
IT	Information Technology
LAN	Local Area Network
MFA	Multi-Factor Authentication
MoJ	Ministry of Justice
PC	Personal Computer
PI	Penitentiary Institution
PMS	"Penitentiary Medicine Center" SNCO
PS	Penitentiary Service of the Ministry of Justice of the Republic of Armenia
SNCO	State Non-Commercial Organization
SRoP	State Register of Population
SSN	Social Security Number

Introduction

The Council of Europe implements the Project "Enhancing health care and human rights protection in prisons in Armenia" (hereinafter referred to as "the Project") funded under the Council of Europe Action Plan for Armenia 2019-2022.

One of the Project component aims at improvement of the material conditions and the provision of healthcare in prisons, including enhancement of health care equipment of the "Penitentiary Medicine Centre" SNCO (PMS) and introduction of new technologies in the health care area.

For this purpose, an initial assessment was completed to evaluate (i) the status of medical data management within the penitentiary system; (ii) available IT equipment and data networks; (iii) technical options for out-patient medical consultations. As result, the assessment report on telemedicine and IT system for medical files (hereafter – Assessment Report) provided overview of the current situation and possible solutions.

The current document presents business and technical requirements for introduction of the electronic medical systems (EMS) and purchase of the equipment for the health care in prisons in Armenia. The document is based on both the data presented in the Assessment Report and the additional study implemented with the specialists of the PMS and penitentiary service (PS). It consists of two parts:

1. **Lot 1 - Development and setting up of the Electronic medical system (EMS)** – The functions of the separate modules of the system and general technical requirements are described including security, development methodology, testing, and training requirements. The implementation schedule is also included in this section.
2. **Lot 2 - Hardware** – The hardware requirements are presented which should provide the reliable and convenient operation of the pilot project on telemedicine and EMS. The hardware technical specifications are presented in the corresponding Annexes.

Part I - LOT 1 - Development and setting up of the Electronic Medical System (EMS)

1. Development and setting up of the Electronic Medical System

1.1 Scope of work

The scope of the work is to develop and set up a new electronic medical system (EMS) in sphere of the penitentiary service to ensure process management of the medical data of persons deprived of their liberty in all penitentiary institutions (PI - Penitentiary Institutions of the Ministry of Justice of the Republic of Armenia).

The main technical requirements, the functional description, and the implementation schedule for the development and setting-up of the EMS are described below and in respective annexes. The provider would need to conduct a detailed study of the system to identify the particularities for the implementation of work. The detailed study should be carried out at the initial stage as presented in the implementation schedule.

Note

The medical services in PS are providing by "Penitentiary Medicine Center" SNCO (PMC). So, the main beneficiary of the EMS is PMC.

1.2 Requirements to the Electronic Medical System (EMS)

1.2.1 General requirements

1. **Design of the system**

EMS should be designed as standalone web-based system, which will have the modules of the following types:

- Functional modules (detailed description of the modules in the sections 1.3.1-1.3.8),
- Reporting module (section 1.3.9)
- Notifications and communications module (section 1.3.10)
- User management module (section 1.3.11)
- Interoperability module (section 1.3.12)
- System support and management module (section 1.3.13)

These modules should interact together to meet the functional requirements described in the section 1.3.

From the architectural point of view the system should be designed as shown in the figure 1.1

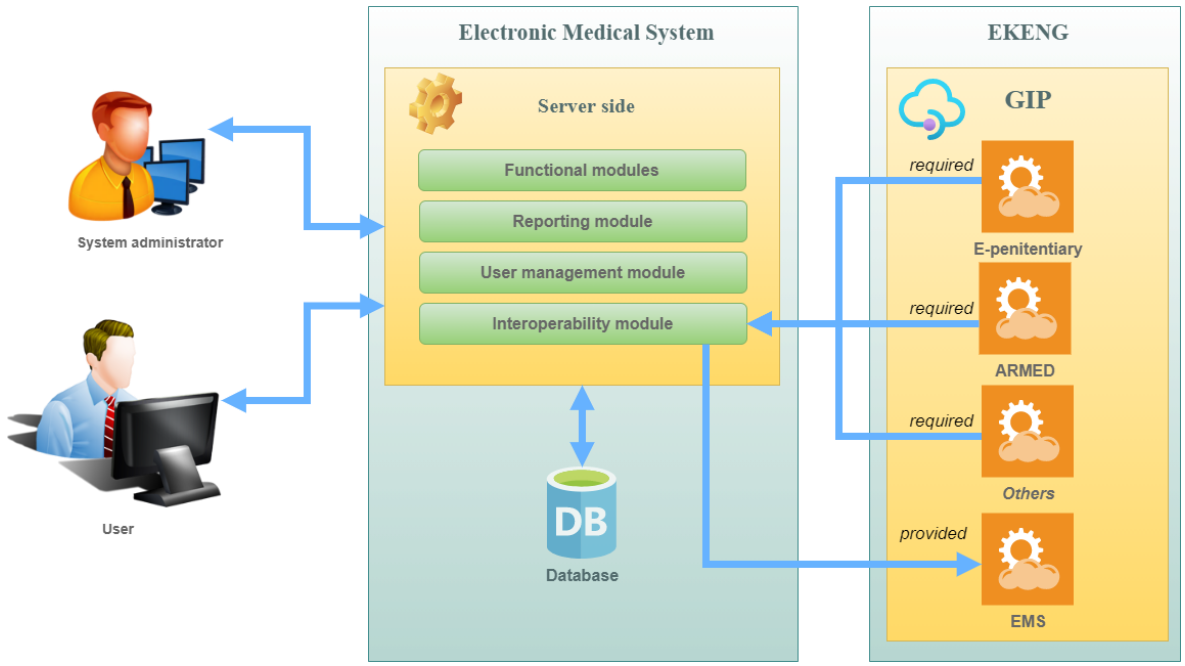


Figure 1.1 Architecture of EMS

2. Integration with the E-penitentiary system

The e-penitentiary system is used by the Penitentiary Service of the Ministry of Justice of the Republic of Armenia (PS) and collects/processes information regarding persons deprived of their liberty in all PIs.

EMS should allow to process the medical data of the mentioned persons through reusing the data collected under the e-penitentiary system.

Data collected and processed under the e-penitentiary

The e-penitentiary system processes the following group of data regarding persons deprived of liberty.

- Passport data
- Basic information
- Physical data
- Medical data (not applicable)
- Fingerprints, tattoos, scars
- Family, relatives
- Education, profession
- Military service
- General information of the penitentiary (PI)
- Prison cell card
- Found (confiscated) items and things
- Barriers
- Incentives
- Penalties
- Self-harm

- Courses, events, self-made associations
- Job
- Visits
- Appointments
- Parcels
- Departures
- Transfers
- Incompatible people
- Closing data
- Archive

Many of the above data relating to the functions of the PS itself, which will not be used in EMS. However, some data in the e-penitentiary system can be re-used by EMS. Such data sets are:

- Passport data
- Some of the basic data (for example: is a detainee or a convict, size of the sentence, date of the end of a sentence, etc.)
- Physical data
- Tattoos, scars
- Family, relatives
- Education, profession
- Military service
- Self-harm
- Job

Note

The data contained in these groups hereinafter will be referred to as personal data provided by the e-penitentiary system or, in short, personal data. Exchange of personal data between electronic systems (in this case e-penitentiary and EMS) should be carried out in accordance with the requirements described in Government Resolution of 19 December 2019, 1849-N.

A detailed description of the data groups and its fields can be found in Annex 2.1.

Note

Medical data are not currently processed under the E-penitentiary system. Medical services are provided by the "Penitentiary Medicine Center" SNCO (PMC), and data processing should be ensured by the EMS which should be the electronic tool of PMC.

E-penitentiary system is a web-based client-server solution. Besides main functional modules it has separate modules of catalogue management, user management and external interoperability.

From the architectural point of view, the e-penitentiary system includes:

- The server part, which implements the business logic of all subsystems (modules), processes the data,
- The database in which processed data is stored,

- The module of interaction with external systems, allowing to receive passport data from the web service of the State Population Register (SRoP) through GIP (provided by EKENG[1]).

The architecture of the e-penitentiary system is shown in figure 1.2.

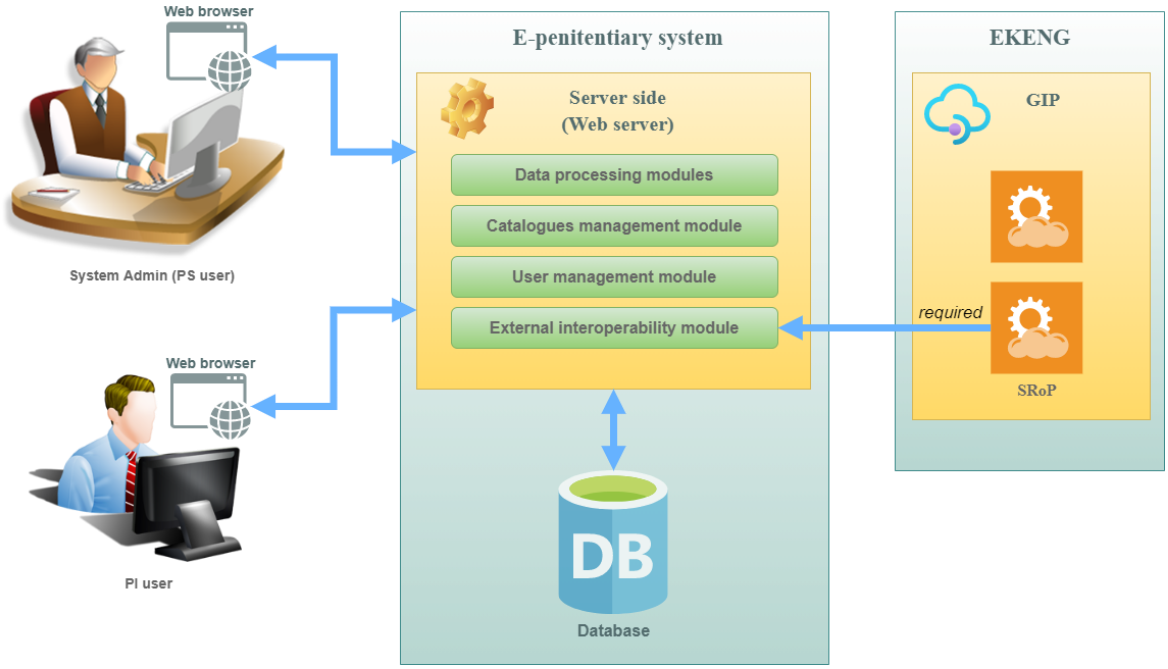


Figure 1.2 Architecture of the e-penitentiary system

As it follows from the discussion with the e-penitentiary system development team, the e-penitentiary system does not have data provision services in the moment of creating this document (it was not planned).

However, it is developed with flexible technologies (Enterprise Level Software), that allows to further develop data provision services. The system is also capable to integration (receiving and providing data) with other systems, such as EMS.

Therefore, at the technical level it is possible to integrate EMS with the e-penitentiary.

To meet this requirement of integration with e-penitentiary, the EMS can be designed as a standalone system (software application), which in addition to data management modules, should also have data exchange (interoperability) module with external systems. This should allow data interoperability between EMS and e-penitentiary systems:

- reuse e-penitentiary system data (common for both systems) by EMS,
- provide data that can be reused by the e-penitentiary system.

[1] EKENG is the operator of the Government Interoperability Platform (GIP), which integrates the information systems of state bodies, local self-government bodies, as well as other legal entities, ensuring the exchange of data between them.

To achieve this solution, it will be necessary to develop additional application interfaces in the interoperability module of the e-penitentiary system, which will provide the necessary data for EMS and integrate that application interfaces with GIP (more details in section 1.3.12).

The integration of the developed application interfaces with the GIP should be carried out in accordance with the requirements described in Government Resolution of 31 August 2015, 1093-N and 1849-N of December 19, 2019.

In overall, the architecture of the e-penitentiary system must be changed as shown on the figure 1.3.

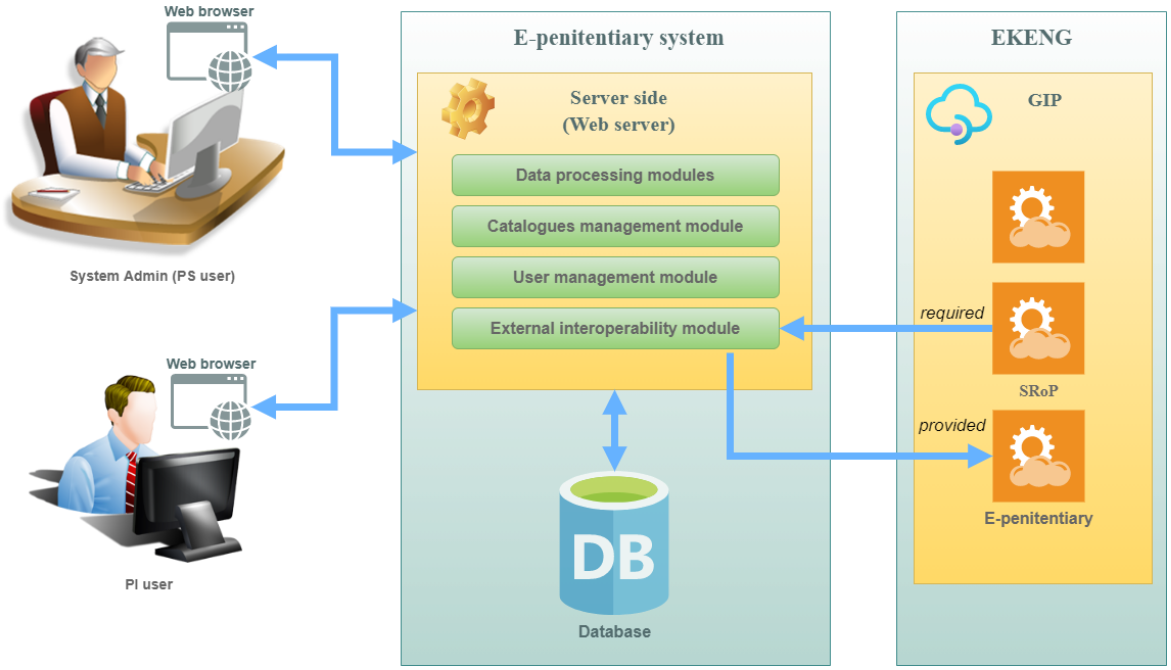


Figure 1.3 Required architecture of the e-penitentiary system

3. Integration with the ARMED[2] system

ARMED is a United Information System of Electronic Healthcare in the Republic of Armenia. It's synchronous data-transmission platform for three types of data: clinical, administrative, and financial. The civil patients' up to date medical data is entered and stored within this system. This allows doctor to access patient's health history and use it for diagnostic and treatment decisions.

The EMS should interact with ARMED also:

- to receive information regarding civil medical cases (in hospital-outpatient) of a person deprived of liberty (before imprisonment),
- make medical referrals,
- before the expiration of the term of imprisonment provide information about person (personal data, address, diagnosed disease, etc.) diagnosed with a special group of

[2] ARMED - Served by "National e-Health Operator" CJSC (https://www.armed.am/). ARMED services are paid.

diseases to the relevant medical institutions (in whose service area the person should be located).

To meet this requirement, the interoperability module should ensure the necessary data exchange with the ARMED system also.

Note

Detailed requirements of the interoperability with ARMED system are described in the section of "Interoperability module" - 1.3.12.

Note

The requirement of interoperability with the ARMED is not mandatory as it depends on existence of data providing interfaces of ARMED system which is not at this moment (details in section of "Interoperability module" - 1.3.12).

4. Overall interconnection of the systems

The overall interconnection scheme of the systems which should be achieved shown in the figure 1.4

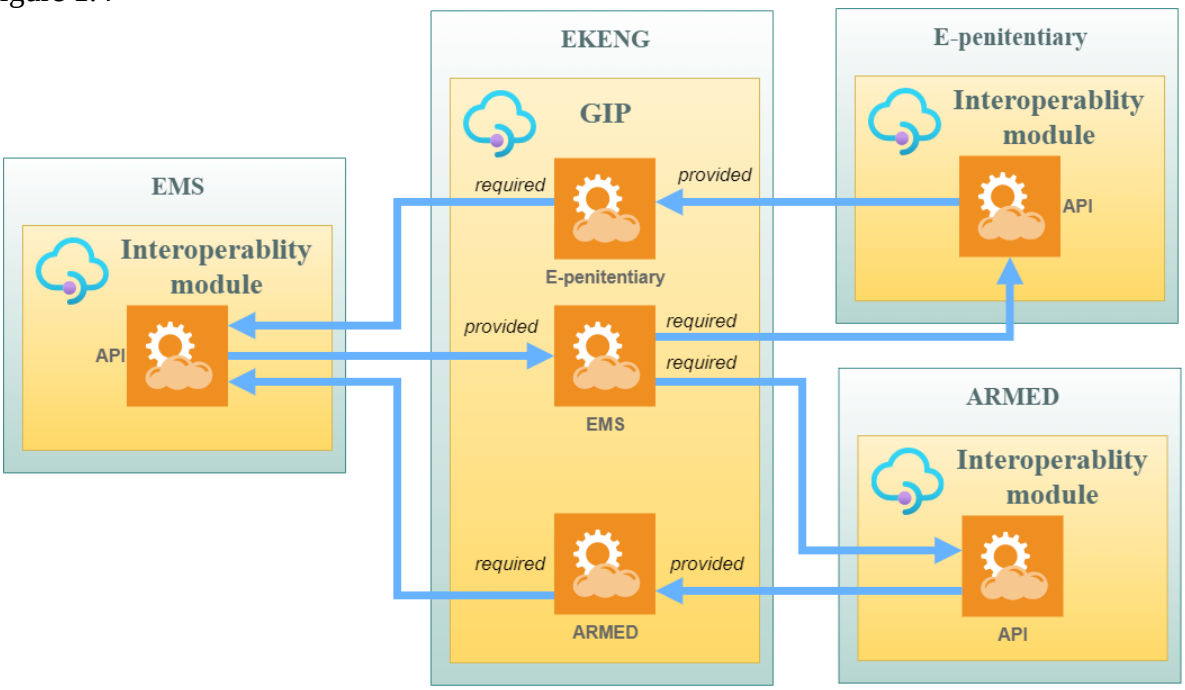


Figure 1.4 Overall interconnection scheme of the systems

5. Integration of video module

The introduction of the telemedicine in the penitentiary medical system is also a part of this project. The first phase of the project should serve as a pilot, within which the telemedicine will use for the following purposes:

- online concilium with participation of two or more doctors (member of the PMS or other institutions),

- outpatient medical consultations for persons deprived of liberty, which not require direct consultation with doctor and can be done online.

As a telemedicine solution, it was recommended to use one of the well-known online communication tools in the first pilot phase: Skype, Google Meet, Zoom, Microsoft Teams, BlueJeans, etc.

However, the government of Armenia planned to introduce Video Module for E-Consulate System and Integration to E-Notary (Bidding document - PSMP3-GO-2-2-8/1 - https://gnumner.am/). At the time of creating this document the bidding of the mentioned project was in the assessment stage. 32 weeks scheduled for the module implementation.

The requirements regarding video module integration within this project are:

- Study the TOR of the module (Bidding document - PSMP3-GO-2-2-8/1 - https://gnumner.am/) to understanding how that meet the requirements of the telemedicine described for this project (Assessment Report).
- In case of meeting the requirements the video module should be integrated into the EMS if there will not any technical restrictions.

Note

The requirement of video module integration is not mandatory as it depends on existence of the module. This is not developed yet.

1.2.2 System technical requirements

Web application, independence of the platform

The EMS must be developed as a web-based application. This allows:

- Ensure independence of the platform - cross-platform
- Avoid installation on the devices
- Use by both PC and mobile devices

Mobile adaptive

To be able to use the system with portable devices (the system is intended for use with a PC or laptop, but may need to be accessed via portable devices), it must be adapted to that (mobile adaptive).

User Interface Design

The user interface (UI) must be user friendly, easy and flexible to use and match but not limit to the following requirements:

- **Simple interface** - avoiding of unnecessary elements and ensure clear labels and in messaging.
- **Consistency and use common UI elements** - By using common elements, users feel more comfortable and can get things done more quickly. It is also important to create patterns in language, layout, and design throughout the site to help facilitate efficiency. Once a user learns how to do something, they should be able to transfer that skill to other parts of the site.

- **Adapted to business processes** - Sequence of actions in UI must be like of user known business processes.
- **System communication** - Users always must be informed regarding current user, actions, changes in states, post-action information, errors etc. Tips for different actions.

Open standards
To make further functional additions or improvements, the system should be developed using open standards. All components should be open standards:

- software code,
- frameworks,
- database.

Multi-layered architecture
The system should be designed as a multi-layered, Service-Oriented Architecture (SOA). It must include at least the following layers:

- Presentation
- Business Logic/Services
- Database

Such architecture will allow functional additions and improvements for further.

Documentation
The following manuals are required that should ensure the training presented in section 1.8.

- User Manual that describes the step-by-step user (routine) actions of the system. It will be required to introduce the electronic version of the manual in the "help" section of the system.
- Administrator Manual that describes the step-by-step administrative actions: installation, archiving, restoration, etc.

In addition to manuals, in different phases of implementation the following documents must be developed:

- System Architecture
- System Functional Description
- Test plan and report
- Training plan and report

Detailed information regarding such documentation is described in appropriate sections.

Warranty service
The system must have at least 8 months of warranty service, during which the bugs or malfunctions that were not detected in the testing phase must be corrected. Details regarding testing are presented in section 1.7 below.

The bugs or malfunctions including but not limited to:

- The system is not accessible.
- The system is not functions as expected.
- The system performance is too slow, which is not connected with the network speed.

- The response is not processing logical requests resulting in performance issues.
- Not all entered data is saved in the system or saved correctly.
- Reports/documents/pages do not display the expected results.
- The system generates messages of unsolvable problems and shows errors to the users.

The detailed general technical requirements of the system are summarized in Annex 2.2.

1.3 Functional description of the system

The previous study phase (Assessment Report) showed that the penitentiary system conducts medical data in a non-electronic way, instead of conducting register books, filling in outpatient cards, etc. As a recommendation, in the Assessment Report presented the introduction of an electronic medical system (EMS) that will allow medical service data to be processed electronically.This approach will ensure:

- Avoid storing medical data of patients in various locations on hard copy (currently, medical data for each patient are processing at subdivision of PMC with outpatient card, in case of transfer to another PI, the data in the previous subdivision are archived, and a new outpatient card is opened in the new subdivision),
- Store data of all patients electronically in a centralized way,
- Transferring data electronically,
- Define permissions and provide for individual users to use/transfer the above mentioned data,
- Make reports,
- Perform analysis that will allow making decisions for further improvement of services.

This section of document provides a more detailed functional description of the EMS - which data should be processed in the system and which functions should be performed towards them.

The medical services performed by PMC can be divided into several areas:

- Patient data management,
- Outpatient case management
- In hospital case management
- Dispensary case management
- Distribution of drugs
- Etc.

In the system, the functions of each domain of medical services should be separated by functional modules.

Non-medical service functions should be separated by modules also, for example:

- management of users and accesses,
- development of reports and analyzes,
- data exchange with external systems,
- notifications and internal communications,
- administrative service: archiving, restoring, etc.
- development of catalogues: lists of regions, cities, PIs, subdivisions of PMC, and etc.

The interconnection of the mentioned modules with each other and the external systems is shown in the component diagram of figure 1.5.

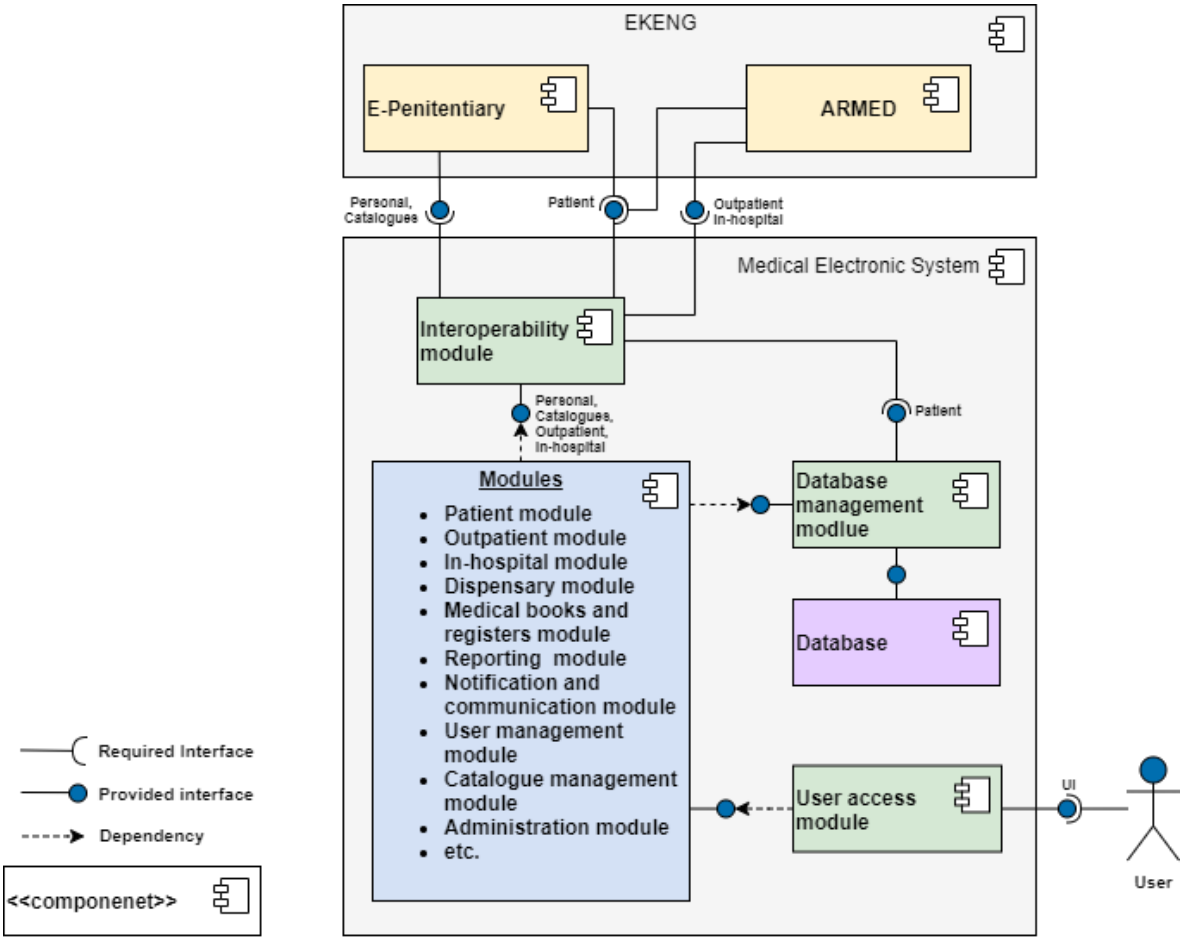


Figure 1.5 Component diagram of Electronic Medical System

The diagram shows the high-level interconnection, by combining many modules in one component. The interconnection of each module to the others is presented in more detail in the corresponding subsection of the module.

The functional descriptions of the individual modules (processed data, functions performed towards them) described in the next sections.

The data processed by all subdivisions in its own modules must be kept centralized to ensure getting the information or the reports (in timeline format) regarding received medical service from all subdivisions of individual patients. In other words, the system must ensure forming of medical history which will contain all services provided by all subdivisions.

The centralized keeping of the submodules data can also be used to obtain an information or reports of other types. E.g., may be used by reporting module 1.3.9 to form standard or advanced reports.

Summary of the system functional requirements are given in Annex 2.30.

1.3.1 Patient management module

As the system is designed to store data of medical services provided to the persons deprived of liberty in PIs, the main object of the system should be the records of these individuals (in this case - patients).

This module should ensure the input of patients' records to whom medical services should be provided. As already mentioned, the proposed system should be integrated with the e-penitentiary system, which processes the data of persons deprived of liberty in PIs. Therefore, the patient management module, with the support of the interoperability module (section 1.3.12), should receive the personal data[3] of the patient from the e-penitentiary system.

The interconnection of the patient management module with the other modules is shown in the component diagram of figure 1.6.

To input data of the patient, the module must provide the following functions and capabilities:

1. To send a request with identifier (SSN) to the e-penitentiary system and receive personal data of the patient. It should be noted that the e-penitentiary system should also have an opportunity to serve this request.

2. To use the passport data, education data and type of imprisonment from the personal data received from the e-penitentiary system (response of request). To add them additional data (details in Annex 2.3) to form data of the patient (patient object).

3. Save patient data in the database.

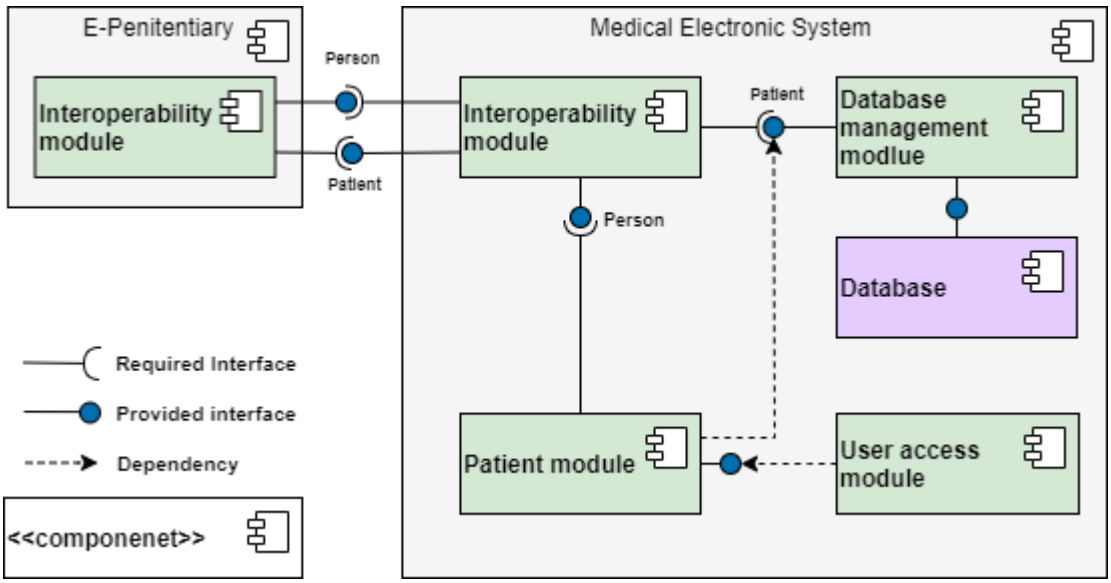


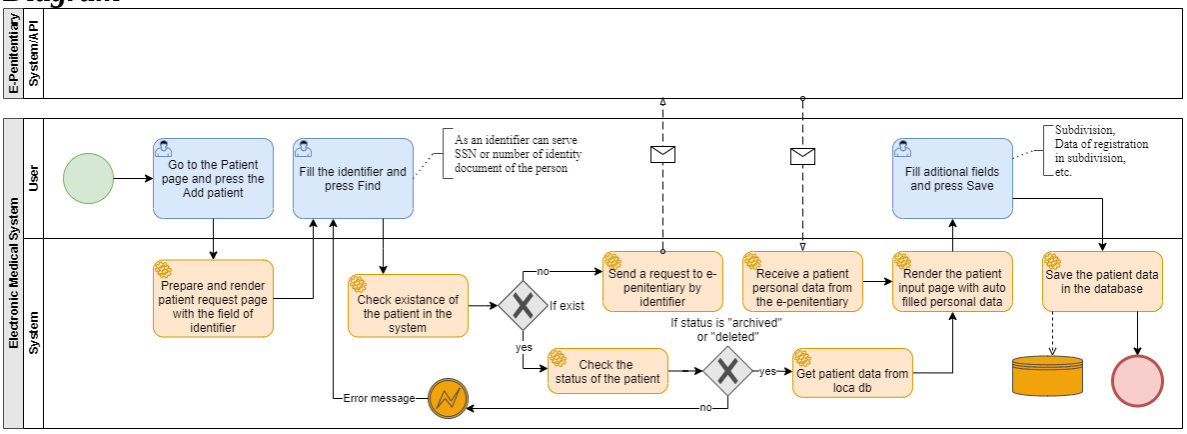
Figure 1.6 Component diagram of patient management module

[3] Personal data - a separate set of data provided by the e-penitentiary system (detailed description in section 1.2.1. and Annex 2.1.

Patient data input carried out by the users of subdivision who have appropriate permissions. The process of patient data input described in BP 1.3.1.

BP 1.3.1 - Patient data input

Diagram



Description

Boundaries	**EMS, E-penitentiary**
Actors	User with permission to input the patient
Flow 1 – Patient is existing in the system	1. The user goes to the Patient page and press the Add patient. 2. The system prepares and render the patient request page with the field of identifier. 3. The user fills fill the identifier and press Find. 4. The system gets the patient data from the system database. 5. Renders the patient input page with auto filled personal data. 6. The user fills the additional fields (date of registration and so on) and press Save. 7. The system saves the patient data in database.
Flow 2 – Patient is not existing in the system	1. The user goes to the Patient page and press the Add patient. 2. The system prepares and render the patient request page with the field of identifier. 3. The user fills fill the identifier and press Find. 4. The system sends a request to e-penitentiary system by identifier. 5. Receives the personal data from the e-penitentiary system. 6. Renders the patient input page with auto filled personal data. 7. The user fills the additional fields (date of registration and so on) and press Save. 8. The system saves the patient data in database.
Output	Registered patient
Exceptions to normal flow	1. After step 3 (Flow 1) the system checks the status of the existing patient. If the status is not “archived” or “deleted”,

	the system generates error message and return to patient request page/window allow the user to fill another identifier.

In addition to input individual patient data, the module should be able to input patient group data from the file (.xls, .xlsx, .csv). This will allow the user to quickly input pre-processed information. This may be more useful when pre-entering data.

In addition to the above, the module should also provide the following features:

- Display, search, and export (in .xls, .xlsx, .csv, .pdf formats) patient data by parameters (if logged in user belongs to any subdivision, only the data of this subdivision must be available).
- Edit individual patient data (non-personal data obtained from e-penitentiary system).
- Archive individual patient data (due to discharge, transfer or termination of detention).
- Delete individual patient data (in case of incorrect input).

For convenience, the module should have the opportunity to access and process data of other modules (outpatient, in hospital, dispensaries, and others) for individual patients.

Each patient can be enrolled by one subdivision. If a patient has already been enrolled by a subdivision, another subdivision should not be able to enroll that patient. Enrollment may be made by another subdivision if the patient's record has been archived or deleted by the user of the previous subdivision.

The data of the patient entered from all subdivision’s sides should be able to be kept in the form of a history, which will be available to the authorized authorities.

The preliminary estimated data that must be processed in the module are given in Annex 2.3.

1.3.2 Outpatient module

This module should provide processing and storage of outpatient data of patients. It is preferrable that this module is able to interact with the ARMED system and obtain medical information of the patient (described in section 1.2.1.). This can be used to get more detailed information about past diseases, research, and treatment.

The interconnection of the outpatient module with the other modules is shown in the component diagram shown of figure 1.7.

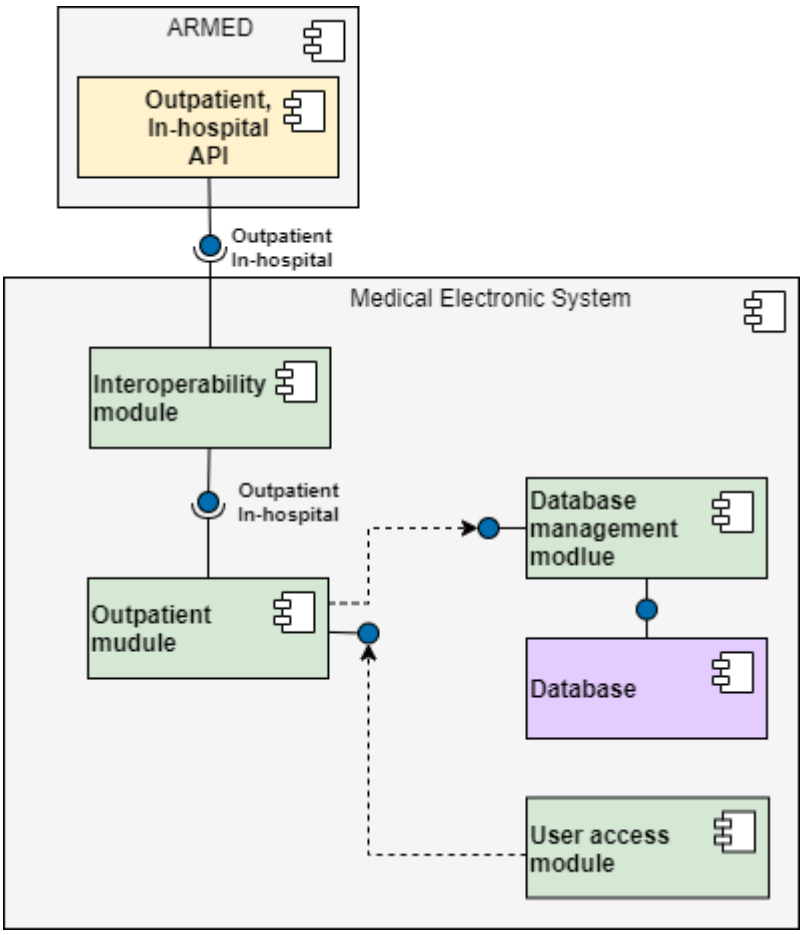


Figure 1.7 Component diagram of Outpatient module

The module should be able to handle data of several operations. The data for each operation must be implemented in the corresponding submodules. Such submodules are:

- **Annual preventive examination,**
- **Preventive fluorographic examination,**
- **Visits –** when the patient applies to the outpatient service with the health issue,
- **Primary examination -** performed after arrival of the patient to penitentiary institution (PI),
- **Gynecological examination -** which is performed only in the Abovyan PI (women prison),
- **Mandatory situational examination performed by the medical staff -** (for example, regular examinations of patients detained in the punishment cell and on hunger strike),
- **Polyclinic visits -** performed at the attached polyclinic,
- **Stomatological service**
- **Emergency call**

The following functions are common to all submodules:

- Add a record regarding submodule data,

- Display, search, and export (.xls, .xlsx, .csv, .pdf formats) data of submodule by parameters (if logged in user belongs to any subdivision, only the data of this subdivision must be available).
- Edit data of individual record (in some cases do not need to have this function – this must be checked in initial study phase).
- Archive data of individual record (if there is a need).
- Delete individual record (in case of incorrect input).

The preliminary estimated data that must be processed in the submodules are given in Annexes from 2.4 to 2.12.

In addition to the data presented in the annexes, some submodules (or other modules - to be specified in the initial study phase) may also contain the "outcome" field (should describe the outcome of the operation), which should contain the following values:

- recovery
- improves
- unchanged
- deterioration
- death.

Death, in turn, must have causes.

- suicide
- due to illness
- other.

This data can be processed in the Catalogue Management Module (Sections 1.3.13.1) and used in these submodules or modules.

There are also submodules (or other modules - must be specified in the initial study phase) in which transfer data to other external medical facilities need to be processed. This is done (based on the patient's health condition) when the patient transferred to another medical institution for treatment, examination or counseling. In this case, only the transfer information (details are given in Annex 2.13) should be processed. The information must be kept receiving a report regarding transfers in the future.

The **Visits** submodule, which processes data of the medical consultation, should include additional information whether the consultation was performed using telemedicine or not. In case of telemedicine the video record, date time, and information regarding doctor (who perform remote consultation) must be attached to the main data. The mentioned doctor may not be in staff of PMC, and the data of the doctor will not in the system. In this case, the data of the doctor is entered manually. If the doctor who provided remote consulting is in staff of PMC, then it is selected from the system, pre-selecting its subdivision.

The processing of telemedicine data will allow creating various reports and analyses of telemedicine services in the future, which will allow:

- get an idea of the advantages and disadvantages of telemedicine,
- make decisions to improve telemedicine, to introduce new approaches.

The **Emergency call** submodule may not be run separately, as the call is performed after a certain operation, as a result of various examinations or visiting. Therefore, in other submodules (visits, primary examination, gynecological examination, mandatory situational examination) there should be an opportunity to maintain the data of the emergency call submodule as additional data on the activities carried out in the given submodules.

1.3.3 In-hospital module

This module should process and store patient data related to hospital cases. This module is also desirable to be interoperable with the ARMED system to obtain patient medical data for hospital cases (described in section 1.2.1). This can be used to get more detailed information about past diseases, research, and treatment.

The interconnection of the In-hospital module with the other modules is shown in the component diagram of figure 1.8.

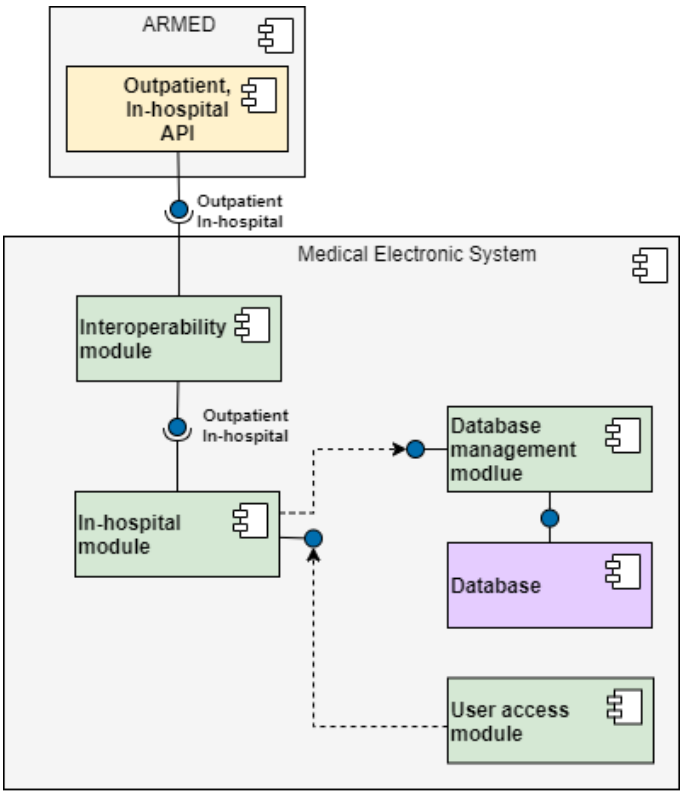


Figure 1.8 Component diagram of In-hospital module

The module should provide data management of the operations performed in both types of medical institutions.

- Internal inpatient services provided by the subdivisions of PMC (prisoners' hospital, inpatient service provided by other subdivisions of PMC),
- External inpatient services provided by the medical institutions of the healthcare bodies.

The data of the operations performed in each type of medical institution should be performed in the relevant submodules.

The following functions are common for all submodules:

- Add a record regarding submodule data,
- Display, search, and export (in .xls, .xlsx, .csv, .pdf formats) data of submodule by parameters (if logged in user belongs to any subdivision, only the data of this subdivision must be available).
- Edit data of individual record (in some cases do not need to have this function – this must be checked in initial study phase).
- Archive data of individual record (if there is a need).
- Delete individual record (in case of incorrect input).

Notice

The last-mentioned functions are common for the modules and sub-modules described in the document, with some differences that need to be adjusted during further study or development. Therefore, the general functions presented above will not mention the document. Only the functions specific to the given module or submodule will be mentioned.

The preliminary estimated data that must be processed in the submodules are given in Annexes 2.14 and 2.15.

In addition to the data presented in the annexes, the data in the submodules can also contain the "output" field, on the same principle as described in section 1.3.2.

In the internal inpatient submodule (to be adjusted at the initial study phase), transfer data to other external medical facilities should also be processed in the same way as described in section 1.3.2.

There must be consultations in the data of each submodule. One or more medical consultations can be carried out within one in-hospital case. The details of the medical consultation should include additional information whether the consultation was performed using telemedicine or not. Telemedicine information processing is in the same way as described for the outpatient module (section 1.3.2).

In all submodules, it should be possible to include the processing of gynecological data (like the data processed in the outpatient module, in the gynecological examination sub-module, section 1.3.2). In the internal inpatient submodule, gynecological data processing should be **available only for the subdivision of Abovyan PI.**

The emergency call data are also processed in these submodules on the same principle as described in section 1.3.2.

1.3.4 Disability management module

This module should ensure the processing and storage of medical data of patients with disabilities in accordance with the procedures developed and the information processed in them.

The interconnection of the disability management module with the other modules is shown in the component diagram of figure 1.9.

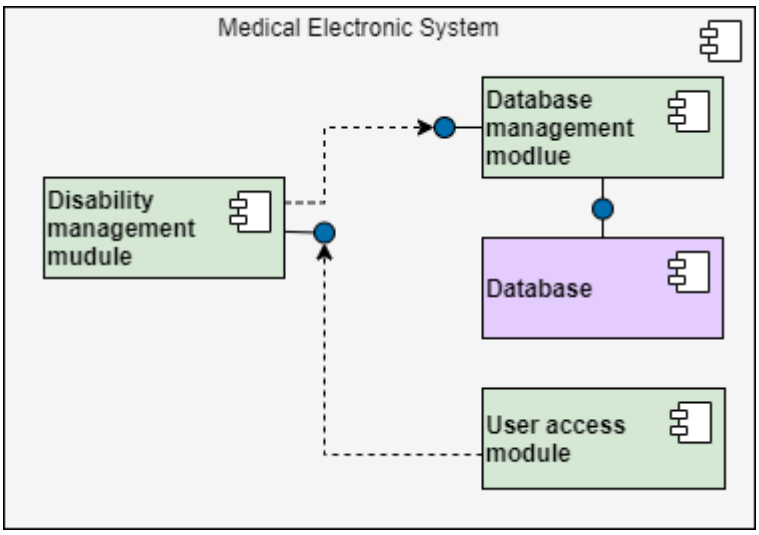


Figure 1.9 Component diagram of disability management module

Notice

All general functions are described above.

The preliminary estimated data that must be processed in the module are given in Annex 2.16.

1.3.5 Mental health module

This module should process the data of patients who have mental health problems. In terms of treatment, similar patients are divided into two groups:

- patients with psychological problems,
- patients with psychiatric problems.

I.e., different treatments are performed for these two groups of patients, for which different data are collected and processed. Therefore, it should be possible to process the patient data of these two groups in separate submodules.

Patients with psychiatric problems in turn are divided into two subgroups:

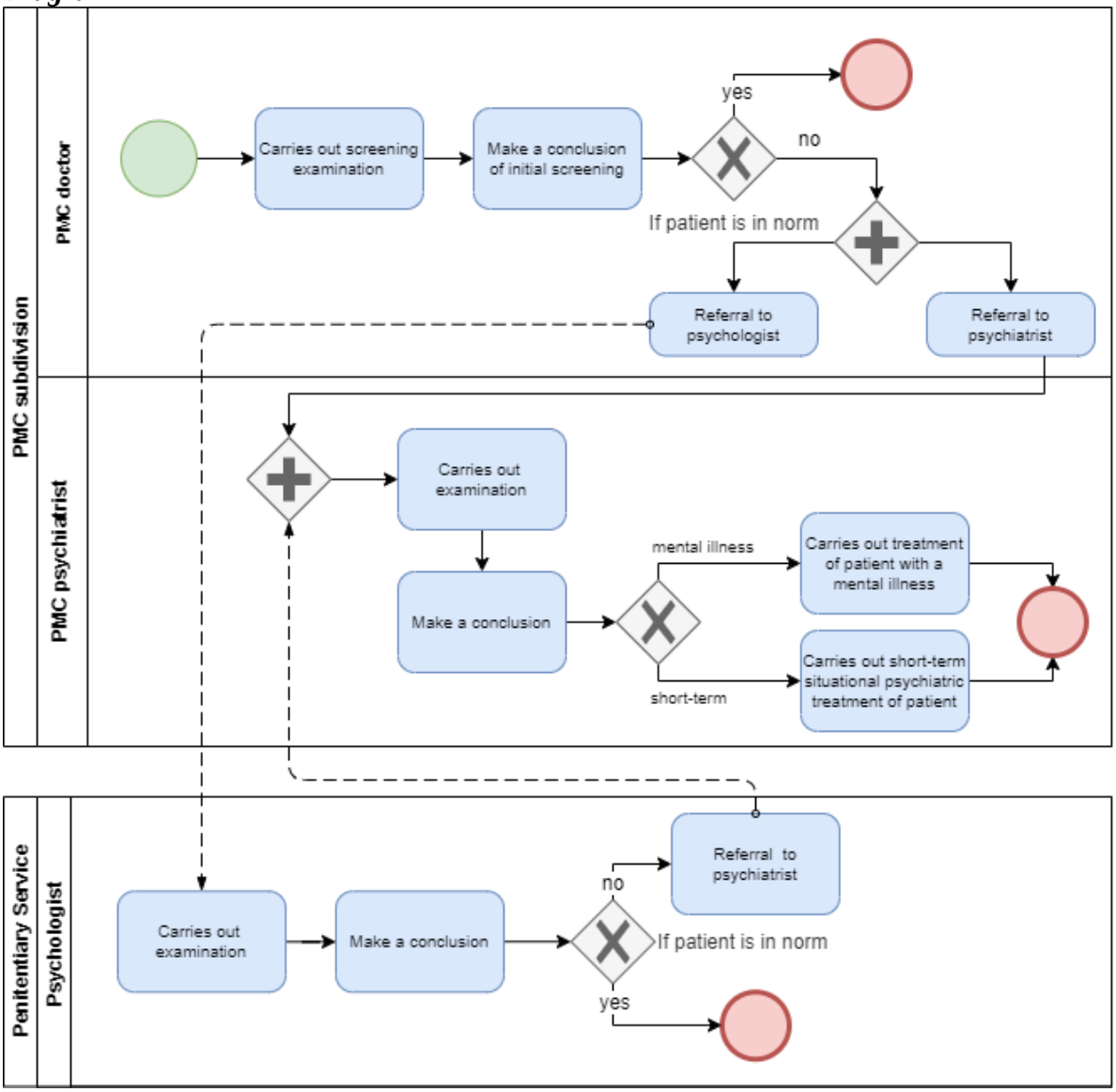
- patients with a mental disorder who are registered with a diagnosis,
- patients receiving of short-term situational psychiatric treatment.

Different medical procedures are performed for the latter two groups of patients too. Therefore, it is necessary to process the data of the latter with separate submodules too.

In general the module must ensure the realization of the processes described in BP 1.3.5 in the correct sequence and enter the data corresponding to the process.

BP 1.3.5 - Mental health process

Diagram



Description

Boundaries	**PMC subdivision, Penitentiary Service**
Actors	PMC doctor, PMC psychiatrist, PS psychologist
Flow	1. The PMC doctor carries out screening examination. 2. Makes a conclusion of initial screening: a. If patient is in norm the process is ended, and data of examination is entered into the system. b. Otherwise, the patient is referred to psychologist or psychiatrist based on conclusion. If patient is referred to psychiatrist, the flow will continue from step 5. 3. The PS psychologist carries out examination. 4. Makes a conclusion: a. If patient is in norm the process is ended, and data of examination is entered into the system.

	b. Otherwise, the patient is referred to a psychiatrist. 5. The PMC psychiatrist carries out examination 6. Makes a conclusion to carry out one of the following treatments: a. registration and management of the patient with mental disorders, b. carries out short-term situational psychiatric treatment of the patient.

The preliminary estimated data that must be processed in the module are given in Annexes 2.17 and 2.18.

The interconnection of the mental health module with the other modules is shown in the component diagram of figure 1.10.

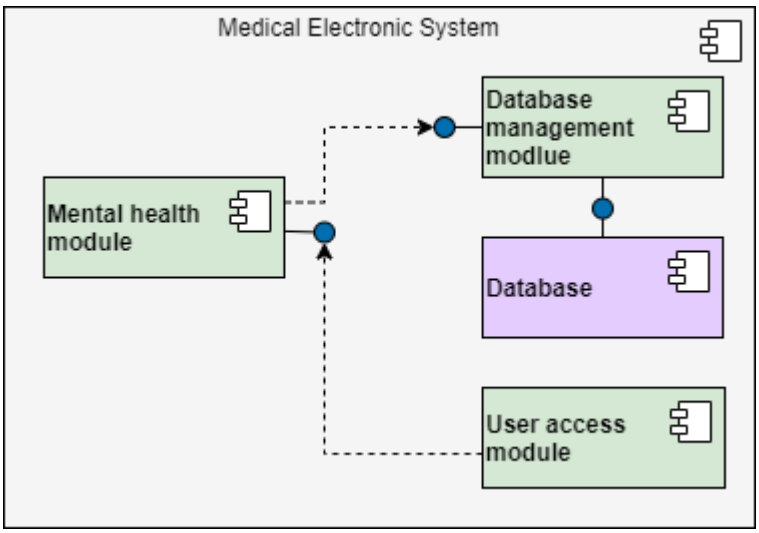


Figure 1.10 Component diagram of mental health module

Notice

All general functions performed in the submodules are described in the previous.

1.3.6 Dispensary module

This module should provide dispensary registration and dispensary control data management of the patients, each of which should be done in a separate submodule.

In dispensary registration submodule data of the following registration groups must be processed:

- Psychiatric
- Oncology
- Narcological
- Anti-tuberculosis

- Infectious
- Dermatological
- Endocrinology

The preliminary estimated data that must be processed in the submodule (for the above-mentioned groups) are given in Annex 2.19.

In dispensary control submodule data of the following control groups must be processed:

- Cardiovascular
- Gastrointestinal
- Neurological
- Urogenital
- other

The preliminary estimated data that must be processed in the submodule (for the above-mentioned groups) are given in Annex 2.20.

The interconnection of the dispensary module with the other modules is shown in the component diagram of figure 1.11.

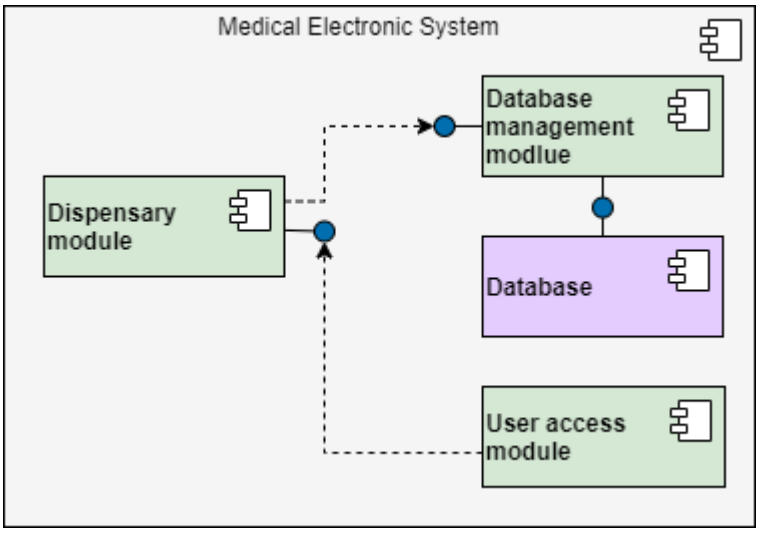


Figure 1.11 Component diagram of dispensary module

Notice

All general functions performed in the submodules are described in the previous.

1.3.7 Drug addiction module

This module should provide data processing and storage for patients who are addicted to drugs. The module should implement the following functions:

- Registration of drug-addicted patients,
- Management of a drug addiction treatment program.

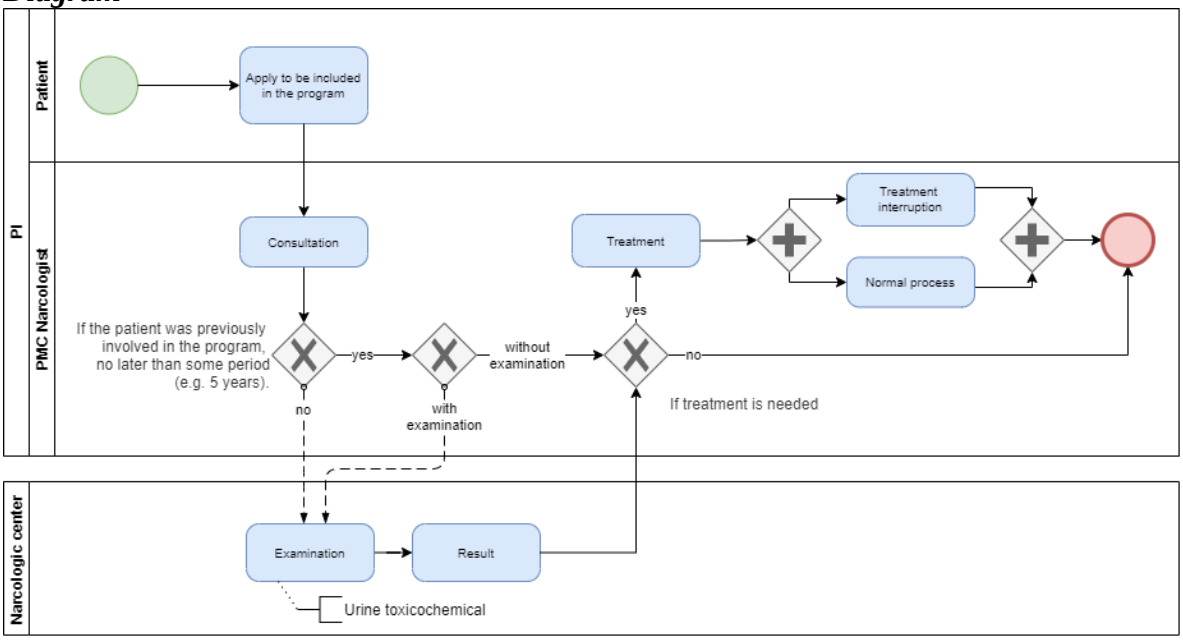
The data management of each function must be performed in a separate submodule.

The preliminary estimated data that must be processed in the "Registration of drug-addicted patients" submodule is given in Annex 2.21.

As for "Management of a drug addiction treatment program" submodule, it must ensure the realization of the processes described in BP 1.3.7 in the correct sequence and enter the data corresponding to the process.

BP 1.3.7 - Drug addiction treatment program

Diagram



Description

Boundaries	**Penitentiary Institution, Narcological Center**
Actors	Patient, PMC narcologist
Flow	1. The patient applies to include into the program 2. The administration of PI organizes the consultation of PMC narcologist. 3. If the patient was previously involved in the program, no later than some period (e.g., 5 years): a. the PMC narcologist can organize the urine toxic-chemical examination in narcological center or without the examination can decide regarding treatment. b. Otherwise, the decision regarding treatment must be based on urine toxic-chemical examination. 4. If the PMC narcologist has determine that treatment is needed: a. the treatment regime is determined - dosage, medication schedule etc. and process continue from step 5. b. otherwise, the process is ended saving the information in the EMS.

	5. The treatment may continue in normal way or interrupted by some reasons (on doctor's instructions, at the will of the patient, others). In all cases data entered into the system.

The preliminary estimated data that must be processed in the above-mentioned process is given in Annex 2.22.

The interconnection of the drug addicted module with the other modules is shown in the component diagram of figure 1.12.

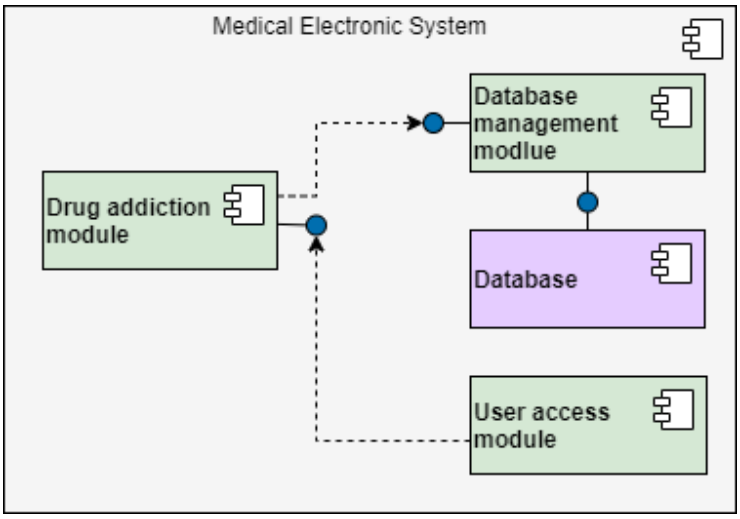


Figure 1.12 Component diagram of drug addicted module

Notice

All general functions performed in the submodules are described in the previous.

1.3.8 Medical books and registries module

This module is intended for an accounting of medicines and medical supplies. Several types of such accountings are currently carried out by the PMS:

- Quantitative accounting of medicines and medical supplies - storage in subdivisions of the PMC,
- Accounting of distributed medicines and other medical supplies - transfer from the subdivision storage to the residential area,
- Accounting for the provision and receipt of drugs - provision of a specific patient in the residential area,
- Accounting of drugs brought by relatives.

Each type of accounting must be performed in the appropriate separate submodule.

In each module or submodule of the system where processing data regarding medicine/drug that information must be auto processed in the submodule of “Accounting for the provision and receipt of drugs”.

The preliminary estimated data that must be processed in the module are given in Annexes form 2.23 to 2.26.

The interconnection of the medical books and registries module with the other modules is shown in the component diagram of figure 1.13.

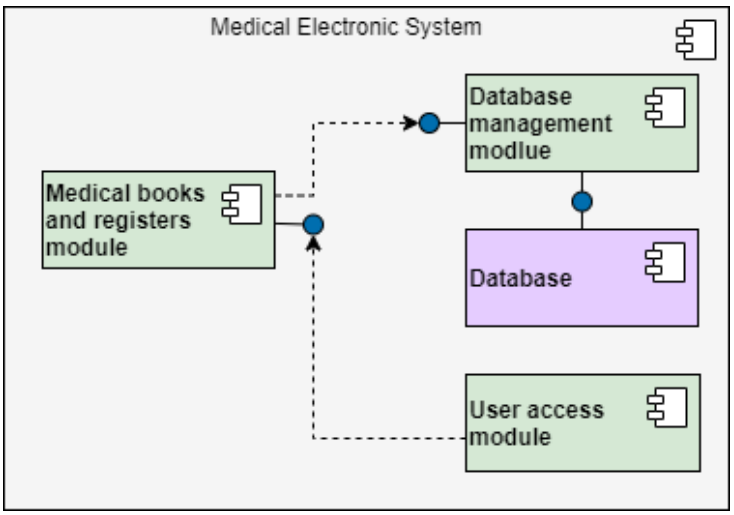


Figure 1.13 Component diagram of medical books and registries module

Notice

All general functions performed in the submodules are described in the previous.

1.3.9 Reporting module

The reporting module should provide a variety of reports based on the data stored in the system. The interconnection of the latter with other modules is shown in the component diagram of figure 1.14.

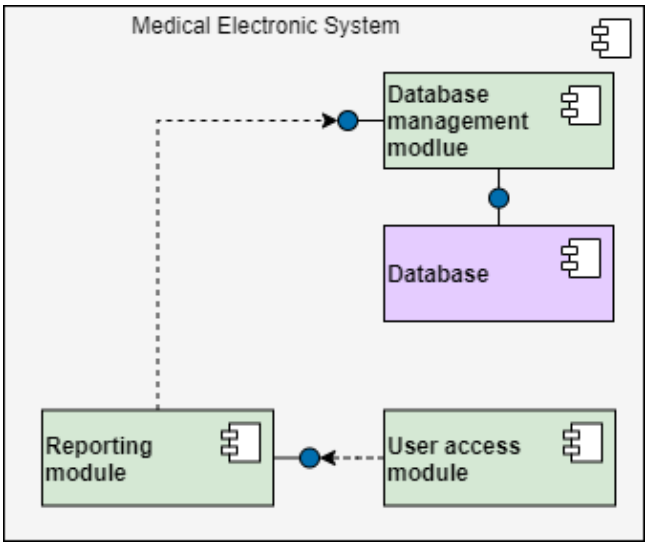


Figure 1.14 Component diagram of reporting module

The system must provide two types of reports, the descriptions of which are given below.

1.3.9.1 Standard reporting

These are reports that are considered standard reports related to the PMC working activities, such as an annual activity report in a PIs or a prisoners' hospital.

These reports are a collection of quantitative aggregated data on the various health operations performed in the system, the form and format of which are clear (to be provided at the initial study stage).

These reports must be exportable in at least .xls, .xlsx, .csv, .pdf formats.

1.3.9.2 Advanced reporting

This should ensure the creation of reports that allow the user to obtain any combined and/or aggregated data from any area of activities without the intervention of developers (Ad hoc reporting).

This is more applicable to analyzes that will allow decision-making, for example, for further improvements in medical services.

This is also applicable to provide different data expected by different state departments.

These reports should also be able to export data at least .xls, .xlsx, .csv, .pdf formats.

1.3.10 Notifications and internal communication module

This module should provide notifications to relevant users regarding certain changes and/or events in various modules (submodules) of the system as well as in external systems.

In addition to notifications, the module must provide communication between users.

1.3.10.1 Notifications

Notifications should serve to provide certain information to the users of EMS. Depending on them, the system does not perform any function but must notify the user of any changes or events in the modules (submodules) or e-penitentiary system.

Example 1. When a person deprived of liberty is transferred to another PI within an e-penitentiary system, the following users should be notified in the EMS:

- The users of the current PI subdivision - for completion of the processing and archiving the patient's medical data.
- The users of PI subdivision where transferred the person deprived of liberty - for adding a new patient within subdivision (from existing data) and continue the data processing.

Example 2. As the period of imprisonment approaches the relevant user in the EMS should receive a notification a few days in advance (the number of days should be determined at the phase of initial study) to take the necessary action.

According to the preliminary assessment, the following notifications are necessary:

- On transfers,
- On the expiration of the term of imprisonment,
- On deaths - must be performed bilaterally between the e-penitentiary system and EMS. When a death is registered in one system, the other system must be notified,
- On the transfer to the punishment cell. When information about the transfer to the punishment cell is recorded in the e-penitentiary system, the EMS user (physician) of the relevant PI subdivision should be notified to carry out a visit-examination,
- Daily reminders about a person who has declared a hunger strike or a water strike for regular inspections.

Information on additional required notifications should be obtained at the initial study phase. However, the system should be designed so that in the future (even after commissioning) the addition of new notifications will not be associated with technical difficulties.

1.3.10.2 Internal communications

This should provide internal communication between system users in the following ways:

- Instant messaging,
- E-mail service (operated within the system).

This will allow the users (doctors) of different subdivisions of the system to transmit certain information and files to each other via instant messaging, as well as e-mail service.

1.3.11 User management and user access modules

Entry and secure access of the system should be based on modules of user management and user access. The functional difference between these two modules is as follows: the first one should define the user and its scope of permitted functions and the second one should check the user's belonging to the system and allow to implement only what is defined in its permissions.

The interconnection of these two modules with the other modules is shown in the component diagram of figure 1.15.

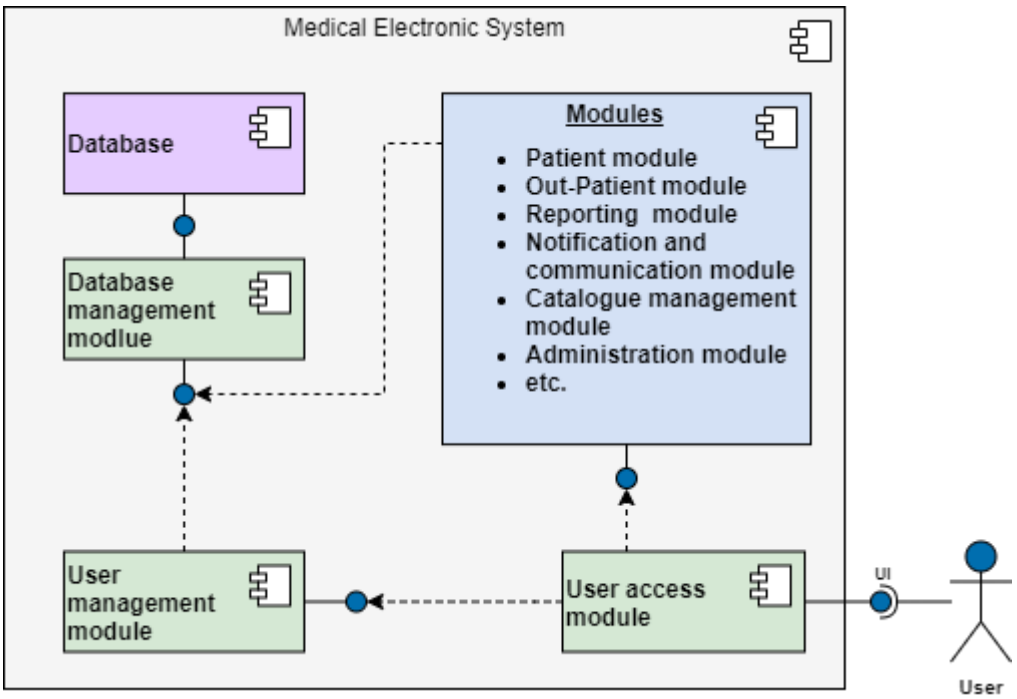


Figure 1.15 Component diagram of user management and user access modules

1.3.11.1 User management module

As already mentioned, the user management module should define the permissions of the user. To achieve this, it is desirable to use the idea of roles. The role should determine the scope of permitted modules and their separate functions, which can be assigned to the user.

Therefore, the user management module must deal with two concepts: role and user.

Role

Roles must be manageable. Management should allow:

- create a role that defines the modules and its functions permissions.
- edit an existing role - allows editing the role name and the modules and its functions permission domain.
- remove the role - will allow removing the role if it is not provided to any user.

The role should have the following data.

- name,
- permission for one or more modules and its functions,
- subdivision domain (specifies which subdivision(s) data will be available to the user in that role).

This allows for a flexible setup user permission. For example, one user may have some permissions within one subdivision and other permissions within another subdivision.

User

The module also should allow:

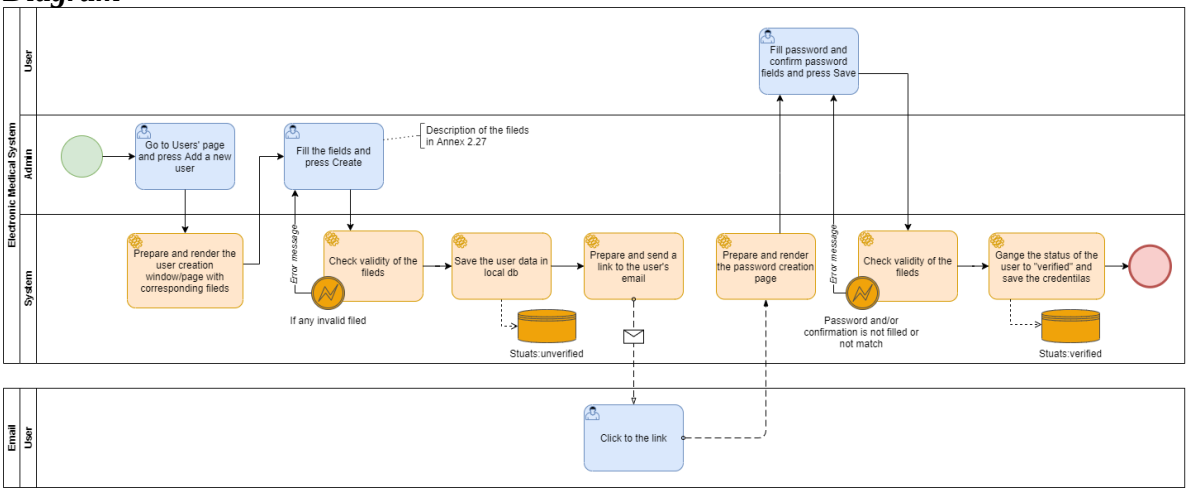
- create a user that will define a username, email address, some personal information and one or more roles (list of data in Annex 2.27),
- assign one or more roles to each user,
- create a password for the user by e-mail confirmation (the user creation process described in BP 1.3.11.1),
- edit user - only some personal information can be edited (no username, no password, no email address), adding or removing the roles can be performed.
- remove the user.

Before creating a user, it is necessary to create at least one role, which will be provided to the user when creating the latter's record.

It should be noted, that during the initial release of the system, it must have at least one user that has permission for all functions of the user management module: create a role, create a user, assign a role to the user, etc. This will allow creating the necessary users with permissions, which in turn can be administrator or regular user.

BP 1.3.11.1 - User creation

Diagram



Description

Boundaries	**EMS and email of the user**
Actors	Admin user, User
Flow	1. Admin user goes to the users' page of the system and performs an action of "Add a new user". 2. The system prepares and render the user creation page/windows with the corresponding fields. 3. The admin user fills all the required fields and press Create. 4. The system saves the user data with "unverified" status in local db. 5. Prepare the and send the link to the user's email. 6. The user presses the link in email.

	7. The system prepares the password creation page and takes the user to that page. 8. The user fills the password and confirmation fields and press the Save. 9. The system changes the status of the user to verified and save the credentials (password).
Output	Creates user
Exceptions to normal flow	1. After step 3 the system checks the validity of the filed fields. If any invalid filed, the system generates error message and return to user creation page/window allow the admin user to fill the correct data. 2. After step 8 the system checks the validity of the password requirements and matching with the confirmation. If any invalid filed, the system generates error message and return to password creation page/window allow the admin user to fill the correct data.

1.3.11.2 User access module

This module is the mediator of the communication with the whole system for the user. This makes available the permitted functions of the system to the user.

The user access module must perform the several general actions.

- verify the applying user affiliation to the system,
- verify user credentials - authentication,
- allow the logged in user to perform only the functions defined in the range of role permission(s) provided to it.

If a function is not allowed to the user, then its buttons, fill-in fields, pages, etc. should not be visible to the latter.

Authentication

One of the key functions of the user access module is **Authentication**.

As mentioned early, the main beneficiary of the EMS is "Penitentiary Medicine Center" SNCO (PMC). The system (EMS) must operate within an internal network of the beneficiary which is not direct accessible for the users from external networks. As studies have shown, there will some cases when the beneficiary user will need to access the system through public network (e.g., working from the home - in the situation of pandemic). In this case the system must provide sufficient security to access to the significant data. For this reason, it is expedient to implement the Multi-Factor Authentication (MFA) which requires the user to provide two or more verification factors to gain access to the data. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

The main benefit of MFA is it will enhance security by requiring from the users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties.

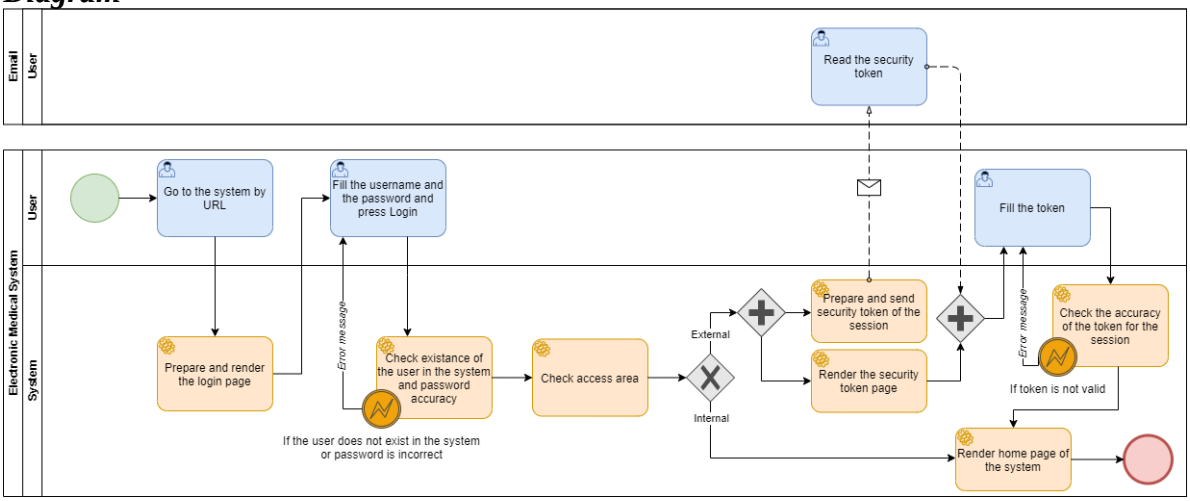
The MFA must apply only in cases when user try to access to the system from the external networks. In case of access from the internal network it is not necessary to apply MFA, only user and password combination enough to authenticate the user.

So, as MFA in the system may be implemented email based Two-Factor Authentication (2FA) which is easy to use and can secure identify the correct users. Email based 2FA uses a security token as a second factor which is sent to the user email every time when the user wants to access to the system from outside of the internal network.

The login process is described in BP 1.3.11.2.

BP 1.3.11.2 – Login

Diagram



Description

Boundaries	**EMS and email of the user**
Actors	User
Flow – access from Internal network	1. The user goes to the system by URL. 2. The system prepares and renders the login page. 3. The user fills the username and the password in the login page and press Login. 4. The system checks the credentials of the user. 5. The system renders the home page of the system.
Flow – access from External network	1. The user goes to the system by URL. 2. The system prepares and renders the login page. 3. The user fills the username and the password in the login page and press Login. 4. The system checks the credentials of user. 5. If the credentials are valid the system generates and sends a security token of the session to the user email. The token is valid for some time-period. 6. In parallel the system renders the security token entry page. 7. The user fills the security token received in email into the security token entry page. 8. The system checks the validity of the security token.

	9. If the security token is valid the system renders the home page of the system.
Output	Logged in user
Exceptions to normal flow	1. After step 4 (for both flows) the system checks the existence of the user in the system and password accuracy. If user doesn't exist in the system or password is incorrect the system generates error message and return the user to login page allow to fill the correct data. 2. After step 8 (for the second flow) the system checks the validity of the security token for the current session. If security token is not valid, the system generates error message and return security token entry page allow the user to fill the correct token.

In addition to multi-factor authentication, the system must also ensure access to the system with an identification card (eID) and a mobile identification card (mID), the requirement of which is defined by the Government Decision N 572-N of 2017. This type of authentication can only replace the user and password entry. That is, the user can use either the username and password pair or one of the mentioned authentication methods to log in to the system. In case of access from external networks, multifactorial authentication should follow the same principle as been described previous.

1.3.12. Interoperability module

This is one of the most important modules of the system, which should allow data exchange with the other external systems. As already mentioned, the most important data for the system is the patient (section 1.3.1), and its data is formed based on personal data received from the e-penitentiary system. Data receiving from the e-penitentiary system is one of the functions of this module.

The next function of the module is to provide data to the e-penitentiary system.

As already presented (section 1.2.1), the e-penitentiary system currently does not have the ability to provide the necessary data. Therefore, when designing the system, it should be considered that in the e-penitentiary system also should be developed the necessary data providing interfaces.

The exchange of data with the e-penitentiary system should be done through GIP. This mean, that data providing interfaces of the e-penitentiary system must be integration in GIP. The GIP integration should be carried out in accordance with the requirements described in Government Resolution of 31 August 2015, 1093-N and 1849-N of December 19, 2019.

Besides exchanging data with the e-penitentiary system, the module must be able to provide data exchange with the ARMED system. However, at the time of the study, the ARMED system did not have the ability to exchange data. Therefore, the requirements for the module in this regard are as follows:

- should be designed to allow future interconnection with both the ARMED system and the other systems.

- Discuss possible data exchange solutions with ARMED system, as well as service technical teams of other involved organizations.
- If there are no technical or legal restrictions, develop and implement interoperability with ARMED system in the EMS, according to the data presented in the section 1.2.1. The exchange of the data with the ARMED system must be carried out in accordance with the requirements described in Government Resolution of 31 August 2015. 1093-N and 1849-N of December 19, 2019, through the Government Interoperability Platform Operator (EKENG).

Note

The requirement of interoperability with the ARMED is not mandatory as it depends on existence of data providing interfaces of ARMED system which is not at this moment.

The structure of the module and the interconnection with the other modules is shown in the component diagram of figure 1.16.

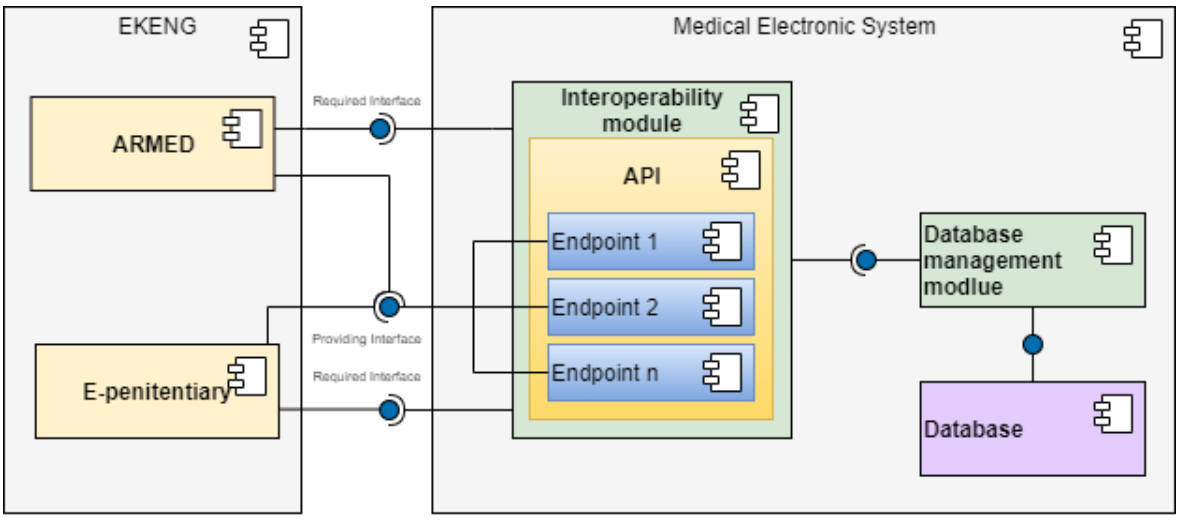


Figure 1.16 Component diagram of the interoperability module

Data providing should be done in a secure manner, using at least the following techniques:

- Authentication and Authorization solutions such as OAuth2.0 and OpenID Connect
- Using encrypted channel TLS
- Validate input

Notice

The requirement of security measures may not be limited to the above. Additional requirements may arise during the initial study or development phase that must be considered.

The Annex 2.28 provides preliminary descriptions of the required (receiving and providing) interfaces with external systems. Additional requirements may arise during the initial study or development phase.

1.3.13 System support and management modules

This section presents several modules that should perform management and support functions in the system. The following sections present their descriptions.

1.3.13.1 Catalogues management module

This module must be designed to process data that will be reused by other modules in the system. Among such data are:

- doctors operating within the system,
- departments of PMC,
- regions,
- cities,
- etc.

A preliminary list of data (including the fields) is provided in Annex 2.29.

This data should be processed as catalogues (master data), which will be selected from the available lists to perform functions in other modules.

Notice

All general functions performed in the module are described in the previous.

1.3.13.2 Database management module

The main function of this module should be to ensure secure, reliable interconnection of other modules with the database:

- provide database query tools - select, delete, insert, update,
- do not allow unauthorized inquiries,
- do not allow duplication of identical data,
- do not allow the same data to be changed simultaneously by different users (or notice about changes),
- and other secure tools when working with the database (if needed).

All modules must perform database queries only through this module.

1.3.13.3Administration module

The scope of the functions of this module should be the follows:

- Perform initial installation of the system.
- Define the database connection string.
- Define URLs for both receiving and providing interfaces to interaction with external systems.
- Archive the data of the database at any time, as well as by scheduling (daily, weekly, monthly, yearly).
- Recover system data from previously archived data.

- and others (if needed).

1.4 Security requirements

The system will deal with the medical data of person deprived of liberty, which has security requirements and should be available only to users of the authorized group. Access for authorized users is provided by the user management and user access modules (section 1.3.11).

Due to data security, the system should operate within an internal network which not accessible for the users from external networks (the proposal of the internal network of PMC is described in the Assessment Report). This solves many risks of external influence.

However, given the fact that the system will be a web-based application, and it can also be operated from an external network, so it will be necessary to ensure data security, to solve the issues that may arise in case of access from external networks. To do this, it is necessary to implement the measures that will allow avoiding the following risks:

- **Injection:** Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
- **Broken Authentication:** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
- **Sensitive Data Exposure:** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
- **XML External Entities (XXE):** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
- **Broken Access Control:** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
- **Security Misconfiguration:** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
- **Cross-Site Scripting XSS:** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

- **Insecure Deserialization:** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
- **Using Components with Known Vulnerabilities**: Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
- **Insufficient Logging & Monitoring:** Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

The above list is the risks and vulnerabilities in the OWASP (Open Web Application Security Project) Top Ten[4] guide. The risks and vulnerabilities presented in the guide should be considered and solved in development.

Besides solving the above-mentioned risks and vulnerabilities, for the security meaner the following should be implemented also:

- Access to the system must be ensured using an SSL certificate issued by a trusted provider with the HTTPS protocol.
- Multi-Factor Authentication (MFA) must be implemented - Particularly email based Two-Factor Authentication (2FA).
- A logging & monitoring mechanism should be introduced in the system, which will allow registering the actions[5] performed by the users.
- Data removal in the system must perform by specially authorized users. In other cases, the deletion of data by the user means archiving the data - keeping it in the database, making it inaccessible to users. Special permissions users must be able to view and/or recover archived data.

1.5 Data migration

As mentioned earlier, in current the medical data is stored in a non-electronic way. Thus, after implementation of the system the non-electronic data must be transferred to the electronic system (EMS) and data will be stored in database – data migration. For supporting data migration process, the manual data filling functionality will need. The functionality must ensure as entry of separate data and as group of data from the file (.xls, .xlsx, .csv, etc.). After end of data migration may need to restrict some manually filling functionality and automate filling processes.

[4] The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

[5] The actions that are considered important for logging can be adjusted during the initial study or development phase.

So, after end of data migration stage it's possibly new functional requirements of the system may arise and need of changes in system functionality.

1.6 Methodology

The developer must choose a methodology that will allow regular communication with the beneficiary and client in process of development. In the methodology it is necessary to consider at least the following points:

- Regularly (once a week or once two weeks) present the progress of the work and the results obtained to the beneficiary,
- Discuss the raised issues with the beneficiary and/or the client asap,
- Record the results of all meetings and discussions (meeting minutes),
- Create a platform for document circulation, which will allow the sides to exchange the necessary documents (laws, legal regulations, working procedures, protocols, proposed functional descriptions, current documents, etc.),
- Provide an electronic platform through which it will be possible to carry out task management: tasks and instructions of the sides and their status, tasks performed, pending tasks, notifications about them.

The listed points will allow to manage many implementation risks: misunderstanding of the sides, deadlines, downtime, etc.

1.7 Testing requirements

The system developer must submit a test plan, which must describe the testing phases, methods, scenarios, environments, and processes. The testing plan must be agreed upon with the client and/or the beneficiary.

In parallel to the system development, during the regular meetings (section 1.6), the developer together with the beneficiary must test the functional part of the system developed at the given phase.

After the complete development and integration with external systems of the system, several tests should be performed:

- **integration testing** - data exchange testing with external systems,
- **load testing,**
- **security testing,**
- **acceptance testing** – to test the functional and technical requirements of the system according on which the system must be accepted.
- other (if necessary).

All tests must be pre-designed in the testing plan. After performing all the tests, the developer must make a test report and submit it to the client and/or the beneficiary.

1.8 Training requirements

The knowledge transfer of the system the developer should carry out through the trainings, which should implement after the complete development.

As already mentioned in the technical requirements, the developer must provide the user and administrator manuals. These should be developed before the start of the trainings, with which the trainings should be conducted.

Trainings should be organized for two groups of participants:

- System support specialists – should implement administrative tasks. The trainings of this group must implement by the administrator manual.
- Employees using the system (medical, nursing, operators, etc.). The trainings of this group must implement by the user manual.

Based on the data provided by the "Penitentiary Medicine Center" SNCO, by preliminary estimation, it is necessary to train:

- 6 specialists as system support specialists,
- 36 employees using the systems: 12 subdivisions, 3 employees in each.

The trainings must be implemented according to the training plan previously submitted by the developer, which will indicate the day, place, instructor, agenda, etc.

The training plan must also be agreed upon with the beneficiary.

1.9 Implementation schedule

1.9.1 Work plan

N°	Key activities	Weeks																	
		1	2	3	4	5	6-14	15-23	24	25	26	27	28	29	30	31	32	33-64	Total weeks
1	**Phase 1 – Initial study**																		2
1.1	Study and adjustment of necessary data and their types																		
2	**Phase 2 – Development** (development and testing of each module)																		25
2.1	Database management and catalogues management modules																		
2.2	User management and user access modules																		
2.3	Patient management and interoperability modules																		
2.4	Outpatient and In-hospital modules																		
2.5	Disability management, psychiatric treatment, dispensary, drug addiction, medical books and registries																		
2.6	Reporting module																		
2.7	Notifications and internal communication module																		
2.8	Administration module																		
3	**Phase 3 - Acceptance**																		5
3.1	Installation of system on beneficiary environment																		
3.2	Presentation of the system, acceptance testing																		
3.3	Trainings																		
3.4	Warranty service																		32

1.9.2 Expected results

	Phase	Deadline	Type	Description
1	Phase 1	2-nd week	Documents	1. Records of meetings and study
2	Phase 2	27-th week	Presentation, Documents	1. Regularly presentations of functions 2. Testing plan and report (documents) 3. Training plan (document)
3	Phase 3	32-nd week	Installation, source code, documents, trainings	1. Installation of the system 2. Source code package 3. System architecture (document) 4. Final functional description (document) 5. Acceptance testing plan and report (document) 6. Administrator and user manuals (documents) 7. Training report (document) 8. Warranty

Part II -LOT 2 - Hardware

2. Hardware

This part describes the requirements of the hardware which need for implementation of the electronic medical system and a pilot project on telemedicine in prison environment.

There is also a reference to the technical requirements for the data exchange network, the presence of which is important for the implementation of both - telemedicine and EMS.

Considering the fact that the medical services in the penitentiary system are provided by the PMC, solutions and hardware of both - telemedicine and EMS, should be introduced on its side - in the head office and subdivisions.

The subdivisions are located in the Penitentiary Institutions[6] of the Ministry of Justice. There are 11 medical subdivisions. Besides the operating subdivisions of the PI, the personnel of the head office of the PMC also must be provided with the necessary equipment for implementing both - telemedicine and EMS. Therefore, introduction of the systems should be done in 12 points: 11 subdivisions and head office.

2.1 Hardware for the introduction of a pilot project on telemedicine

The implementation of pilot project on telemedicine should ensure:

- online Concilium with participation of two or more doctors (member of the PMS or other institutions),
- outpatient medical consultations for persons deprived of liberty, which not require direct consultation with doctor and can be done online.

As a telemedicine solution it is recommended to use on the pilot phase one of the well-known online communication tools (see Assessment Report): Skype, Google Meet, Zoom, Microsoft Teams, BlueJeans, etc. The choice of any of the above-mentioned solutions is conditioned by certain technical requirements.

A summary table of comparisons of the above-mentioned solutions is given in Annex 1.1.

Regardless of the choice of solution, it will be necessary to provide quality, reliable and uninterrupted conference, including:

- PC or laptop
- High-quality portable camera
- Microphone
- Internet access

The **PC or laptop** can be a medium-size office computer, the specifications of which are given in Annex 3.1.

A **camera** is required for researching from different positions during the conference (consultation). It must also provide high resolution frame and frequency. These parameters will

[6] See the Assessment Report for information on PIs.

allow to get the most accurate picture during the consultation of a doctor-patient. Detailed specifications of the camera are given in Annex 3.2.

There are no special requirements for the microphone, it is necessary to ensure the conversation of the participants. It can be built-in into the PC/laptop or camera.

The **internet connection** should suffice to exchange high-resolution frames. To provide a frames 4K at 30 fps 5mbps bandwidth will require. If a WI-FI network will be used, it is also necessary to provide a strong signal.

In the subdivisions of the PMC, access to the Internet should be provided through the data exchange network of the Penitentiary Service (PS) as mentioned in the Assessment Report. However, for joint use, it will be necessary to install a network router in the subdivisions of the PMC which will allow to separate traffic of the itself and the PS. The router may also have LAN interfaces to interconnect the network equipment of the subdivision and provide internet access to the necessary equipments. This approach will allow avoiding the need for additional network switches. Detailed technical specifications of the network router are given in Annex 3.3.

Notice

The network requirements in the last paragraph also satisfy to the EMS. Therefore, the requirements are common for the implementation of both systems.

Summarizing the above mentioned, we can say that for the introduction of telemedicine it is necessary to provide the following equipment and internet network access in all subdivisions of the PMS:

- One PC or laptop for each subdivision (total 12),
- One high-quality portable camera for each subdivision (total 12),
- Internet access with a bandwidth at least 5 Mbps in each subdivision,
- One network router for each subdivision (total 12).

A diagram of the connection of all the necessary equipment for the introduction of telemedicine is shown in figure 2.1.

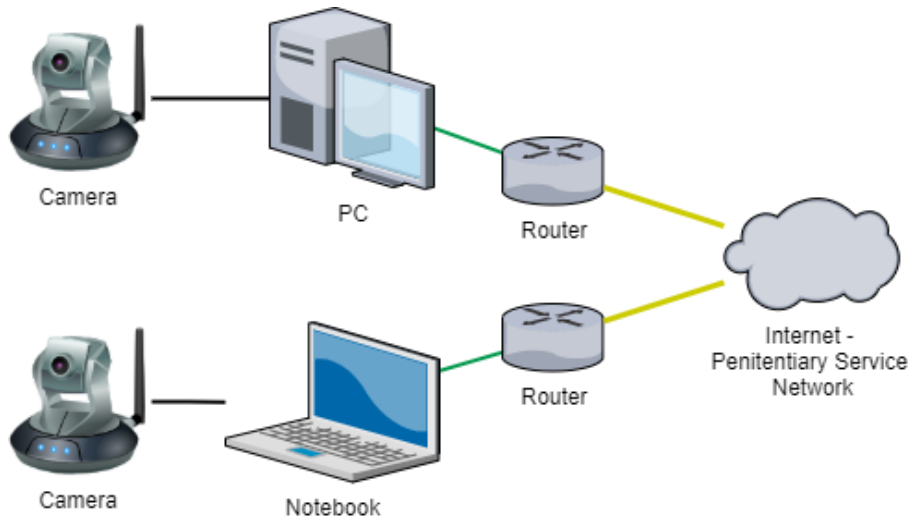


Figure 2.1 Connections of telemedicine equipment

Detailed technical specifications of the equipment are given in the corresponding annexes (3.1 - 3.3).

2.2 Hardware for the electronic medical system

As already presented in the technical requirements of the electronic medical system (EMS), it should be developed as a web-based client-server application. The following hardware components are required for the implementation and operation of such systems:

- **A server** - that receives requests sent by clients, processes, and returns the necessary responses,
- **A client** - through which the requests are formed and sent, as well as the rendering of the results of the responses.

To take full functionality of the system, additional components are also required.

- **A printer** - that allows to print reports, exported lists, etc.
- **A scanner** - that will allow to scan the necessary documents and upload the system.

Besides the hardware, the system also requires a data exchange network: the clients must have access to the server through the network.

Notice

The network requirements of the electronic medical system are the same (are common) as the network requirements of telemedicine, which are already presented in the previous section.

EMS equipment connection diagram is shown in figure 2.2.

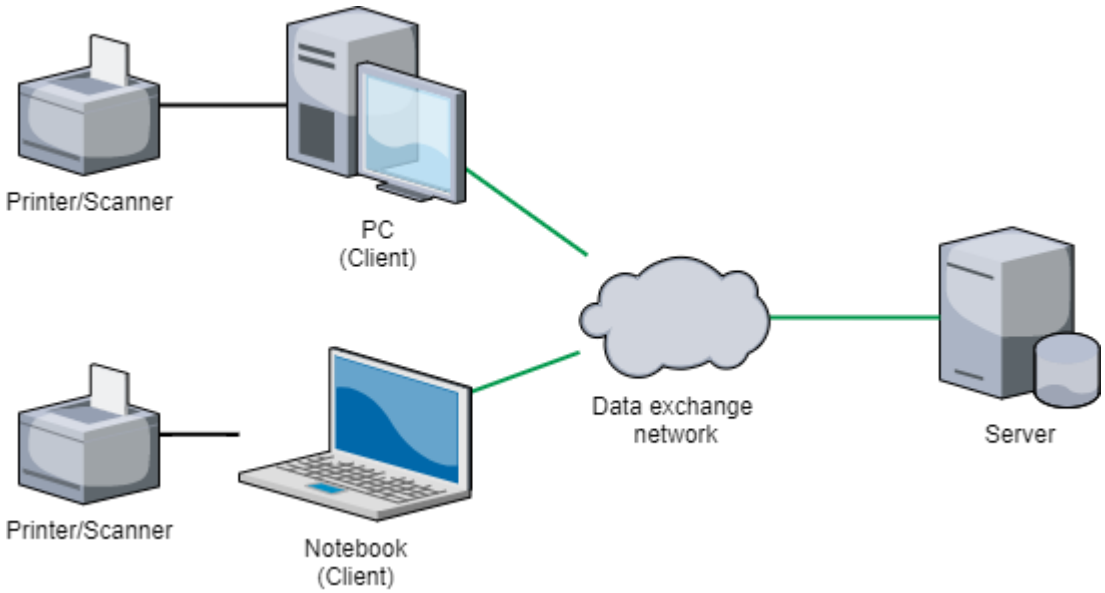


Figure 2.2 Connections of EMS equipment

Server

Besides processing and responding to client requests, the server must store system data. The data will be of two types:

- database data,
- files.

As in many modules of the system, files also will be stored, it is necessary to provide data storage to store that files in it. Beside the files, the video files of telemedicine also must be stored. At this stage, it is not possible to estimate the exact number and the volume of files yet (it can be estimated after some time the system will up and running), but it will continuously grow. However, approximate calculations show that for the next 3 years, it may be required 3-5 TB capacity.

In such systems, in which sensitive data is processed and stored, the implementation of data backup is highly recommended. Archiving should be done regularly - once or twice a day. For archiving, as hardware, need to use tape storage (using magnetic tape). This approach has the following advantages:

- Magnetic tape is not sensitive to crypto virus, so it allows archived data to be protected from such vulnerabilities. In case of crypto-virus damage to the data storage, the data can recover from the tape storage.
- Archived data can be stored outside of the server farm. The data stored on tapes can be moved from the building of the server farm. In case of natural disasters, fires, or other physical damages, data can be recovered from tape drives stored outside the building.

Server farm with required specifications will be provided by EKENG. Within discussions EKENG has approved that the company will provide at least one virtual server with parameters of 2 core CPU, 16 GB RAM. The rest requirements regarding network, data storage, archiving of data, etc. also will be provided by EKENG. The full request to EKENG and the response from the company in details shown in annex 3.4.

As mentioned in the response of EKENG there is a need of additional disks for data storage to ensure a capacity of 3-5 TB. The disks must be meet the specifications provided by EKENG as these will be added in the existing data storage (Netapp AFF A400). The specification of disks is given in annex 3.5.

PC or laptop

As a client equipment can serve devices on which possible to use a web browser, as the system is web-based. PC, laptop, tablet, smartphone are such devices. However, because the data displayed in the system will most likely be displayed in tables, tabs, input windows, where the input fields can be many, it is advisable to use devices with large monitors. Based on this, a PC or laptop should be used as a client device.

In this case, one PC or laptop should provide to all subdivisions of the PMC. They should be separate from those provided for telemedicine, as these two functions (telemedicine and system operation) are different from each other and will be performed by different specialists.

Detailed specifications of the PC or laptop are given in annex 3.1.

Printer and scanner

As already mentioned, to fully use the functionalities of the system, there is a need for a printer and scanner (details at the beginning of the section). A combined device can be used for this purpose. It is more affordable in terms of using and service.

With the implementation of the system, all subdivisions and head office of the PMC should be provided with one similar combined device, the technical specifications of which are presented in annex 3.6.

Additional hardware

In "Medical books and registers module" (1.3.8) of EMS there are actions to accounting medicines and other medical supplies which can have barcodes. For reading and/or input the items (medicine, drug) into the system (EMS) by barcode it's more convenient to use barcode scanners. In this purpose, it is advisable to provide the barcode scanners to subdivisions of PMC with the following distribution:

Subdivision	Quantity
PMC headquarters pharmacy (warehouse)	1
PMC subdivisions	12
Departments of Convicts' Hospital	8

The technical specifications of barcode scanners presented in annex 3.7.

ANNEXES

Annex 1.1 Comparison table for online communication tools

	Zoom	Microsoft Teams	Skype	Google Meet	BlueJeans
Number of participants	Up to 100 participants (additional - in the paid versions)	Up to 100 participants (additional - in the paid versions)	Up to 50 participants	Up to 100 participants (additional - in the paid versions)	100 to 200 participants
Duration	Video conference duration: up to 40 minutes (additional - in the paid versions), but for two participants (one-on-one meetings) it is unlimited	Video conference duration: up to 60 minutes (additional - in the paid versions)	Video conference duration: up to 100 hours per month, no more than 10 hours per day, no more than 4 hours per conference.	Video conference duration: up to 60 minutes (additional - in the paid versions), but for two participants (one-on-one meetings) it is 24 hours	Unlimited
Video recording	Available in the Desktop application (video recording in Mobile and Web applications are available in the paid version)	Available only in the paid version	Available in all versions	Available only in the paid version	Up to 5 hours
Need for an account	No	Yes (Microsoft)	Yes (Skype, Microsoft)	Yes (Google)	No
Need of corresponding software for invitation	No (also through a web browser)	Yes	No (also through a web browser)	No (also through a web browser)	No (also through a web browser)
Authentication	Account / password	Account	Account	Account / password	Account / password
Chanel encryption	256-bit TLS encryption	OAUTH, TLS, Secure Real-Time Transport Protocol (SRTP), PKI	AES 256-bit TLS encryption	Datagram Transport Layer Security (DTLS) and Secure Real-time Transport Protocol (SRTP)	AES 256-bit TLS encryption
Available versions	Desktop, Mobile and Web	Desktop and Mobile	Desktop, Mobile and Web	Mobile and Web	Desktop, Mobile and Web
Free version	Yes	Yes	Yes	Yes	No
Paid version	Starts from $ 149.90 / year	Paid version is available:		Starts from $8/user/month	Starts from $9.99/host /month

		• Microsoft 365 Business Basic ($5/user/month) • Microsoft 365 Business Standard ($12.5/user/month) subscription			

Annex 2.1 Data in the e-penitentiary system that can be reused by EMS

Data	Fields	Sub fields	Type
Passport data	SSN		number (10 sym.)
	First name		text
	Last name		text
	Middle name		text
	Birth date		date
	Sex		select
	Nationality		select
	Registration address		text
	Living place		text
	Citizenship(s)	Country	text
		Id doc. type	text
		Id doc. number	text
		Date of issue	date
		From	number
Imprisonment data	Imprisonment type (detainee, convict)		text or number (id)
Physical data	Height and weight	date	date
		height (cm)	number
		weight (kg)	number
	Skin color		select
	Eye color		select
	Hair color		select
	Blood rhesus		select
	External description		select
	Disability(s)	date	date
		category	select
		Description	text
		Number of certificate	text
		Date of certificate	date
		From	text
	Addiction (s)	Type	select
		date	date
		Description	text
Tattoos, scars	Tattoo(s)		file (photo)
	Scar(s)		file (photo)
Family, relatives	Family status		select
	Husband/Wife	FLM	text
		Passport	text
		Address	text
	Child(ren)	FLM	text
		Passport	text
		Address	text
	Parent(s)	FLM	text
		Passport	text
		Address	text
	Relative(s)	FLM	text

		Passport	text
		Address	text
Education, profession	Education		select
	Profession		multiselect
	Preferences		multiselect
	Abilities, skills		multiselect
	Languages		multiselect
	State awards, prizes, state titles		multiselect
	Notes		text
Military service	Relation to military service		select
	Military service data	Start	date
		End	date
		Military profession	text
		Military rank	select
		Military position	text
	Awards, medals		multiselect
	Participated in the war		multiselect
Self-harm(s)	Type		select
	Start		date
	End		date
	Description		text
Job(s)	Name		text
	Type		select
	Date of involvement		date
	Date of dismissal		date
	Status		select

Annex 2.2 General technical requirements of the system

N/N	Technical requirement	Description
G01.1	Web-based system	Must be developed as web-based application, cross-platform.
G01.2	Languages	Armenian
G01.3	Mobile adaptive	Must be adapted for a well-known web browsers of all sizes (Microsoft Edge, Safari , Firefox, Chrome): • smartphone • tablet • notebook • PC
G01.4	User Interface Design	The user interface (UI) must be user friendly, easy and flexible to use and match but not limit to the following requirements: • simple interface • consistency and use common UI elements • adapted to business processes • system communication
G01.5	Open standards	All components must be of an open standard: • source code • frameworks using in source code • database • etc. (in any) The source code package must be provided to beneficiary.
G01.6	Source codes	Upon completion of the system development, all source codes with all rights must be provided.
G01.7	Multi-layered architecture	Must include at least the following layers: • Presentation • Business Logic/Services • Database SOA - Service Oriented Architecture
G01.8	Performance	Must be able to ensure the requests of 50 users simultaneously, ensuring the processing of queries in no more than 2 seconds.
G02.1	Testing environment	Prior to installation, the test environment must be provided by the developer.

G02.2	Initial installation	Initial installation must be carried out by the developer in the beneficiary's production environment.
G02.3	Testing	• integration testing • load testing • security testing • acceptance testing The testing must be performed with the participation of the developer and beneficiary, according to the test plan previously developed by the developer.
G03.1	Documentation	Must have at least the following documents: • User manual • Administrator manual • Architecture • Functional description • Testing plan and report • Training plan and report
G04.1	Security	Addressing the risks and vulnerabilities presented in the guide of OWASP Top Ten
G05.1	Methodology	Agile methodology that will allow regular communication with the beneficiary and client
G06.1	Trainings	Trainings for two groups of participants: • System support specialists – should implement administrative tasks, • Employees using the system (medical, nursing, operators, etc.):
G07.1	Warranty	8 months

Annex 2.3 Data of patient management module

Fields	Required	Description
Unique identifier	yes	Auto filling taking into account the identity in the system. It can be personal number of the e-penitentiary system, SSN or other identifier.
Subdivision	yes	The data is processed in catalogues. Auto filling based on the data of the logged-in user.
Date of registration in subdivision	yes	
Date of discharge from the subdivision	no	Auto filling during archiving
PI identifier	yes	Identifier of the PI. Receiving from the e-penitentiary system
SSN	yes	Auto filling. Receiving from the e-penitentiary system
First name	yes	
Last name	yes	
Middle name	no	
Date of birth	yes	
Registration address	yes	
Living place	no	
Education	no	
Is in dispensary	no	Auto filling when there is at least one dispensary record in the corresponding module. It can contain one of two values - yes or no.
Disability	no	Auto filling when there is at least one disability record in the corresponding module. It can contain one of two values - yes or no.
Blood group	no	Can be received from the e-penitentiary system
Rhesus	no	Can be received from the e-penitentiary system

Annex 2.4 Data of annual preventive examination submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • PI
Year	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Physical data		
Refusal of medical examination	yes	May contain one of two values, yes or no. In case of selecting "Yes" option, the other fields should not be possible to complete. (This also applies to further similar fields)
Date	yes	
Height	no	
Weight	no	
BMI (Body Mass Index)	no	
Hemodynamic parameters		
Refusal of medical examination	yes	
Date	yes	
Blood pressure	no	
P_S	no	
PO_2	no	
t^0	no	
Objective examination parameters		
Refusal of medical examination	yes	
Date	yes	
Pulm	no	
Cor	no	
Pasternatsky symptom (right side)	no	
Pasternatsky symptom (left side)	no	
Laboratory examination		
Refusal of medical examination	yes	
Date	yes	
Complete blood count (CBC)	no	
U-Total (Urinalysis)	no	
Glucose	no	
Cholesterol	no	
Healthy lifestyle advice		
Date	no	
Notice	no	

Special diet		
Notice	no	
Women's examination ***(Information in this section should be available if the patient is female)***		
Anamnestic data		
Refusal of medical examination	yes	
Date	yes	
Existence of menopause	no	
Number of pregnancies	no	
Number of childbirths	no	
Objective examination parameters		
Refusal of medical examination	yes	
Date	yes	
Inspection	no	
Pelvic Ultrasound	no	
Breast examination		
Refusal of medical examination	yes	
Date	yes	
Left side	no	
Right side	no	
PAP smear		
Refusal of medical examination	yes	
Date	yes	
Result	no	
Conclusion		
Notice	no	

Annex 2.5 Data of preventive fluorographic examination

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Datetime	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues or is filled in manually if the doctor's data is not in the system (doctor from external institution).
Result	yes	May contain one of the following values: • Norm • Pathological changes If the "Pathological changes" option is selected, the user should be able to fill in the data in the sub-modules of the In-hospital module (2.2.3) for processing treatment or additional examination data. The data processed in these two sub-modules must have a reference to each other.
Attached files	no	
Notice	no	

Annex 2.6 Data of visiting submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Type of medical care	yes	Selected from the available data processed in the catalogues.
Short description of medical care	no	
Diagnosis	no	Selected from the available data processed in the catalogues.
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Start date of dismissal	no	
End date of dismissal	no	
Total number of dismissal days	no	
Diet	no	
Carried out by telemedicine	yes	May contain one of two values, yes or no. In case of selecting “no” option, the next fields should not be possible to complete.
Telemedicine doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues or is filled in manually if the doctor's data is not in the system (doctor from external institution).
Video file	yes	Attached file

Annex 2.7 Data of primary examination submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Datetime	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Entry date to PI	yes	
From	yes	Selected from the available data processed in the catalogues. Values must be adjusted in initial study phase (court, institution, etc.)
Additional notice	no	
Injuries		
Existence	yes	May contain one of two values, yes or no. In case of selecting “no” option, the other fields should not be possible to complete.
Nature	no	
Description: location, size, color, form	no	
Patient explanation	no	

Annex 2.8 Data of gynecological examination submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Diagnosis	no	Selected from the available data processed in the catalogues.
Complaint	no	
Medical intervention	no	Selected from the available data processed in the catalogues.
Admission type	yes	May contain one of two values, primary or secondary.
Start date of dismissal	no	
End date of dismissal	no	
Total number of dismissal days	no	
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).

Annex 2.9 Data of the submodule of mandatory situational examination performed by the medical staff

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Datetime of the beginning of the situation	yes	
Purpose	yes	Selected from the available data processed in the catalogues. • Hunger strike • Punishment cell • Other
Examinations	yes	Each case can have one or more examinations data of which is presented in the next.

Examinations

Fields	Required	Description
Date Time	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Complaint	no	
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Physical data		
Height	no	
Weight	no	
BMI (Body Mass Index)	no	
Hemodynamic parameters		
Blood pressure	no	
P_S	no	
PO_2	no	
t^0	no	
Objective examination parameters		
Pulm	no	
Cor	no	
Pasternatsky symptom (right side)	no	
Pasternatsky symptom (left side)	no	
Conclusion		
Notice	no	
Outcome		

Outcome	yes	May contain one of the following values: • Unchanged (status remains unchanged) • Return to normal mode (status removed) • Medical intervention In case of medical intervention: • Status is removed • Provides the opportunity to fill in the data in the Visits sub-module (2.2.2) or the In-hospital module (2.2.3) sub-modules (the data processed in the sub-modules must have a reference to each other).

Annex 2.10 Data of polyclinic visit submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Purpose	yes	May contain one of the following values: • Examination • Consultation • Treatment • Immunization Based on the selected version, the description of the fields is given below.

Examination

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Laboratory • Instrumental
Examination	yes	Selected from the available data processed in the catalogues by type. Laboratory • General blood test • Biochemical analysis of blood • Others Instrumental • ECG • Ultrasound • Others
Conclusion	yes	
Attached files	no	

Consultation

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Surgical • Neurological • Others

Conclusion	yes	
Attached files	no	
Referral	no	May contain one of the following values: • Examination • Consultation • Treatment In case of choosing any option, the user should be able to fill in the data in the sub-modules of the In-hospital module (2.2.3) for examination, additional consultation or treatment data processing for selected patient. The data processed in these sub-modules must have a reference to each other.

Treatment

Fields	Required	Description
Notice	yes	
Attached files	yes	

Immunization

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Covid 19 • Hepatitis • Others
Attached files	yes	

Annex 2.11 Data of stomatological service submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Diagnosis	no	Selected from the available data processed in the catalogues.
Complaint	no	
Medical intervention	no	Selected from the available data processed in the catalogues.
Admission type	yes	May contain one of two values, primary or secondary.
Start date of dismissal	no	
End date of dismissal	no	
Total number of dismissal days	no	
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).

Annex 2.12 Data of emergency call submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Datetime of the call	yes	
Caller data	yes	
Datetime of the emergency service	yes	
Preliminary diagnosis	yes	
Implemented event	yes	May contain one of the following values: • On-site service • Transfer Based on the selected version, the description of the fields is given below.

On-site service

Fields	Required	Description
Conclusion	yes	
Attached files	no	

Transfer

Fields	Required	Description
Purpose	yes	May contain one of the following values: • Examination • Consultation • Treatment In case of choosing any option, the user should be able to fill in the data of transfers (Annex 2.13) and data in the sub-modules of the In-hospital module (2.2.3) for examination, additional consultation or treatment data processing for selected patient. The data processed in these sub-modules must have a reference to each other.

Annex 2.13 Data of transfers

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date of transfer	yes	
Diagnosis at transfer	yes	
Transferred medical institution	yes	Selected from the available data processed in the catalogues.
Form of transfer	yes	May contain one of two values: • Urgent • Planned
Means of transfer		May contain one of following values: • By emergency call • Other (all possible options should be clarified at the initial study)
Type of transfer	yes	May contain one of two values: • By government procurement referral • On a paid basis
Purpose of the transfer	no	May contain one of three values: • Consultation • Diagnose • Treatment
Government procurement referral number	no	
Doctor's (FLM) of transferred medical institution	no	
Contacts of transferred medical institution doctor	no	
Document substantiating the money transfer to the account of the transferred medical institution	no	
Document substantiating the transfer of escort and protection costs of the PI guard	no	

Annex 2.14 Data of internal inpatient service submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Purpose	yes	May contain one of the following values: • Examination • Consultation • Treatment Based on the selected version, the description of the fields is given below.

Examination

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Laboratory • Instrumental
Examination	yes	Selected from the available data processed in the catalogues by type. Laboratory • General blood test • Biochemical analysis of blood • Others Instrumental • ECG • Ultrasound • Others
Conclusion	yes	
Attached files	no	

Consultation

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Surgical • Neurological • Others
Conclusion	yes	
Attached files	no	
Referral	no	May contain one of the following values:

		• Examination • Consultation • Treatment In case of choosing any option, the user should be able to fill in the data in the sub-modules of the In-hospital module (2.2.3) for examination, additional consultation or treatment data processing for selected patient. The data processed in these sub-modules must have a reference to each other.

Treatment

Fields	Required	Description
Date and time of hospitalization	yes	
Disease history number	yes	
Sending PI	no	Selected from the available data processed in the catalogues
Subdivision	no	Selected from the available data processed in the catalogues
Diagnosis upon admission	no	Selected from the available data processed in the catalogues
Diagnosis at discharge	no	Selected from the available data processed in the catalogues
Outcome of the disease	no	Selected from the available data processed in the catalogues
Date of discharge	no	
Bed/days count	no	
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Consultations	no	Each in-hospital case can have one or more consultations. The consultation data match the data presented in the visits submodule (Annex 2.6).
Additional notice	no	

Annex 2.15 Data of external inpatient service submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Purpose	yes	May contain one of the following values: • Examination • Consultation • Treatment Based on the selected version, the description of the fields is given below.

Examination

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Laboratory • Instrumental
Examination	yes	Selected from the available data processed in the catalogues by type. Laboratory • General blood test • Biochemical analysis of blood • Others Instrumental • ECG • Ultrasound • Others
Conclusion	yes	
Attached files	no	

Consultation

Fields	Required	Description
Type	yes	Selected from the available data processed in the catalogues. • Surgical • Neurological • Others
Conclusion	yes	
Attached files	no	
Referral	no	May contain one of the following values:

		• Examination • Consultation • Treatment In case of choosing any option, the user should be able to fill in the data in the sub-modules of the In-hospital module (2.2.3) for examination, additional consultation or treatment data processing for selected patient. The data processed in these sub-modules must have a reference to each other.

Treatment

Fields	Required	Description
Type	yes	May contain one of the following values: • Conservative • Surgical
Indication	yes	
Realization	yes	
Description	no	
Attached files	yes	It can be an epicrisis or other documents

Annex 2.16 Data of disability management service module

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • And other necessary personal data
Group / Category	yes	May contain one of three values: • 1st • 2nd • 3rd
Date of issue	yes	
Date of re-examination	no	
Completion date	no	
First time	yes	May contain one of two values - yes or no
Diagnosis	yes	

Annex 2.17 Data of the submodule of patients with psychological problems

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Date of initial screening	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Conclusion of initial screening	yes	
Result of initial screening	yes	May contain one of the following values: 1. norm 2. referral to psychologist 3. referral to psychiatrist If the “norm” option selected the next fields must be ignored. If the “referral to a psychiatrist” option selected the next fields must be ignored also and the system must move to the submodule of “patients with psychiatric problems” and link to this case.
Date of psychologist consultation	yes	
Psychologist	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues or is filled in manually if the doctor's data is not in the system (doctor from external institution).
Conclusion of psychologist	yes	
Result of psychologist	yes	May contain one of two values: 1. norm 2. referral to psychiatrist If the “referral to a psychiatrist” option selected the system must move to the submodule of “patients with psychiatric problems” and link to this case.

Annex 2.18 Data of the submodule of patients with psychiatric problems

Consultation of psychiatrist

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Date	yes	
Psychiatrist	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues or is filled in manually if the doctor's data is not in the system (doctor from external institution).
Conclusion of psychiatrist	yes	
Result of psychiatrist	yes	May contain one of two values: 1. registration 2. short-term situational psychiatric treatment Based on the selected version, the description of the fields is given below.

Registration of the patient with mental disorders

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Registration date	yes	
Diagnosis	yes	Selected from the available data processed in the catalogues.
Previously registered	yes	It can contain one of two values – “yes” or “no”.
Need for treatment	yes	It can contain one of two values – “yes” or “no”. If “no” option selected the system must ignore the next fields and move to the submodule of “dispensary control” and link to this case.
Treatment start date	yes	
Treatment end date	yes	
Treatment regimen	yes	Selected from the available data processed in the catalogues.

Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Treatment outcome	no	

Short-term situational psychiatric treatment

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Treatment start date	yes	
Treatment end date	yes	
Diagnosis	yes	Selected from the available data processed in the catalogues.
Conclusion	no	
Treatment regimen	yes	Selected from the available data processed in the catalogues.
Medicine	no	Each case can have one or more record regarding receipt of medicine. The medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Treatment outcome	no	

Annex 2.19 Data of dispensary registration submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Registration start date	yes	
Registration end date	no	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Name and code of the disease	yes	Selected from the available data processed in the catalogues.
Dispensary registration group	yes	Selected from the available data processed in the catalogues: • Psychiatric • Oncology • Narcological • Anti-tuberculosis • Infectious • Dermatological • Endocrinology
Disability group/category	no	Selected from the available data processed in the catalogues.
Examinations	no	In one case of dispensary registration can be one or more examinations. The examinations data must be processed in internal and/or external inpatient service submodules (Annexes 2.14 and/or 2.5, Purpose- Examination) and link to the corresponding case of dispensary registration.
Additional notice	no	
Conclusion	no	
Result	yes	May contain one of the following values: • Norm • Treatment If selected “Treatment” option, the treatment data must be processed in internal and/or external inpatient service submodules (Annexes 2.14 and/or 2.5, Purpose- Treatment) and link to the corresponding case of dispensary registration.
Previously registered (may contain one or more similar data)		
Place of registration	no	The type of data should be clarified during the initial study
Duration	no	

Annex 2.20 Data of dispensary control submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Registration start date	yes	
Registration end date	no	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Name and code of the disease	yes	Selected from the available data processed in the catalogues.
Dispensary control group	yes	Selected from the available data processed in the catalogues: • Cardiovascular • Gastrointestinal • Neurological • Urogenital • others
Disability group/category	no	Selected from the available data processed in the catalogues.
Examinations	no	In one case of dispensary registration can be one or more examinations. The examinations data must be processed in internal and/or external inpatient service submodules (Annexes 2.14 and/or 2.5, Purpose- Examination) and link to the corresponding case of dispensary control.
Additional notice	no	
Conclusion	no	
Result	yes	May contain one of the following values: • Norm • Treatment If selected “Treatment” option, the treatment data must be processed in internal and/or external inpatient service submodules (Annexes 2.14 and/or 2.5, Purpose- Treatment) and link to the corresponding case of dispensary registration.
Previously registered (may contain one or more similar data)		
Place of registration	no	The type of data should be clarified during the initial study
Duration	no	

Annex 2.21 Data of drug-addicted patients submodule

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Date	yes	
Doctor	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Diagnosis	no	Selected from the available data processed in the catalogues.
Complaint	no	
Registration	yes	May contain one of two values - registered or removed
Additional notice	no	

Annex 2.22 Data of the submodule of management of a drug addiction treatment program

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Criminal article • Punishment • Beginning of detention
Application of patient	yes	Attached file
Date of application	yes	
Narcologist	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Previously involved	no	May contain one or more records for the separate case. The fields can me filled manually if there are not any data of the patient regarding involvement to the program in the system or must be auto filled in opposite case. The description of the fields is given below.
Urine toxicochemical examination		
Date of sampling	no	
Date of Result	no	
Result	no	
Result file	no	Attached file
Consultation of narcologist		
Conclusion	yes	May contain one of the following values: • Need a treatment. • Don't need a treatment If selected the “Don't need a treatment” option “Conclusion file” filed must be filled only. The “Treatment” section must be available only when the “Need a treatment” option is selected.
Conclusion file	yes	Attached file
Additional notice	no	
Treatment		
Start date	yes	
End date	no	
Involved by priority	yes	May contain one of two values – “yes” or “no” If selected option “yes” the “Reason of priority” fields (file also) are required.
Reason of priority	no	
Reason of priority - file	no	Attached file
Treatment regime	yes	

Medicine	yes	Selected from the available data processed in the catalogues:
Initial dosage	yes	
Provision of medicine	yes	May contain one or more records for the separate case. The provisioned medicine data match the data presented in the submodule of accounting for the provision and receipt of drugs (Annex 2.25).
Status	yes	May contain one of the following values: • Interrupted • Normal process • Ended If selected the "interrupted" option the reason and file fields are required. After changing status to "interrupted" or "ended", the treatment end date must be filled and the case must be unavailable to change.
Interruption reason	no	Selected from the available data processed in the catalogues: • on doctor's instructions, • at the will of the patient, • others
Interruption reason file	no	Attached file

Previously involved

Fields	Required	Description
Start date	yes	
End date	yes	
Interrupted	yes	May contain one of two values – "yes" or "no" If selected option "yes" the next fields are required.
Interruption reason	yes	Selected from the available data processed in the catalogues: • on doctor's instructions, • at the will of the patient, • others
Interruption reason file	yes	Attached file

Annex 2.23 Data of the submodule of quantitative accounting of medicines and medical supplies

Fields	Required	Description
Medicine	yes	Selected from the available data processed in the catalogues (name, dosage, form, package).
	In	
Date of receipt	yes	
Invoice number	yes	
Quantity	yes	
Unit price	no	
Sum	no	
	Out	
Quantity	no	
Unit price	no	
Sum	no	
	Balance	
Quantity	no	
Sum	no	

Annex 2.24 Data of the submodule of accounting of distributed medicines and other medical supplies

Fields	Required	Description
Medicine	yes	Selected from the available data processed in the catalogues (name, dosage, form, package).
	In	
Date	yes	
Claim number	yes	
Quantity	yes	
	Out	
Date	no	
Quantity	no	
Number of disease history, medical card or outpatient registration	no	
	Balance	
Quantity	no	

Annex 2.25 Data of the submodule of accounting for the provision and receipt of drugs

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate • Number of medical card (disease history)
Datetime	yes	
Medicine	yes	Selected from the available data processed in the catalogues (name, dosage, form, package).
Provider	yes	Autofill - depending of the data of the logged in user or is selected from the available data processed in the catalogues.
Date of issue:	yes	
Notes on receiving the medicine	no	
Additional notice	no	

Annex 2.26 Data of the submodule of accounting of drugs brought by relatives

Fields	Required	Description
Patient	yes	Selected from the data processed in the patient management module. The selection can be made by searching with any identifier. As displayed data, from the patient data should be used: • First name, Last name, Middle name • Birthdate
Date	yes	
Brought medicine	yes	Selected from the available data processed in the catalogues (name, dosage, form, package).
Type of medicine	yes	Selected from the available data processed in the catalogues.
Quantity	yes	
Note	no	

Annex 2.27 User data

Fields	Required	Description
Username	yes	
E-mail	yes	
SSN	yes	Will be used for eID and mID authentication
First name	no	
Last name	no	
Middle name	no	
Photo	no	file URL
Type	yes	Selected from catalogues (doctor, nurse, operator end etc.)
Subdivision	yes	Selected from catalogues (PMC subdivisions)
Description	no	

Annex 2.28 Required and provided interfaces

Interfaces provided by E-penitentiary system

Personal data of the patient	
Input parameters	**Output parameters**
SSN or Id document number of imprisoned people	Personal data • SSN • First name • Last name • Middle name • Birth date • Sex • Nationality • Registration address • Living place
	Data regarding education
	Data regarding type of imprisonment (detainee, convict)

Sync of catalogues data	
Input parameters	**Output parameters**
	List of PIs (with the sub data)
	List of regions
	List of communities (with the region data)

Interfaces provided by EMS

Patient medical data	
Input parameters	**Output parameters**
SSN or Id document number of imprisoned people	Status data • Disability • Dispensary registration • Registration of drug-addicted • Including in drug addiction treatment program • Mental illness
	Treatment data • Data regarding internal inpatient services • Data regarding external inpatient services
	Others (must be found out at the initial study phase)

Annex 2.29 Data processed in catalogues

PI (this is synchronized with the e-penitntiary system)

Fields	Required	Description
Institution identifier	yes	
Name of institution	yes	
Region	yes	
Community	yes	

Region (this is synchronized with the e-penitntiary system)

Fields	Required	Description
Region identifier	yes	
Name of region	yes	

Community (this is synchronized with the e-penitntiary system)

Fields	Required	Description
Community identifier	yes	
Name of community	yes	
Region	yes	Selected from pre-processed Region data

PMC subdivision

Fields	Required	Description
Subdivision identifier	yes	
Name of subdivision	yes	
PI	no	Selected from pre-processed PI data (The need should be clarified at the initial study)
Region	yes	Selected from pre-processed Region data
Community	yes	The value depends on selected PI or selected from pre-processed Community data (which included in selected region)

Department

Fields	Required	Description
Department identifier	yes	
Name of department	yes	
PMC subdivision	no	Selected from pre-processed PMC subdivision data

Type of medical care

Fields	Required	Description
Identifier	yes	
Name	yes	

External medical institution

Fields	Required	Description
Medical institution identifier	yes	
Name of the medical institution	yes	

Code of the medical institution	yes	
Region	yes	Selected from pre-processed Region data
Community	yes	The value depends on selected PI or selected from pre-processed Community data (which included in selected region)
Address	yes	
Contacts	yes	

Purpose of mandatory situational examination performed by medical staff

Fields	Required	Description
Identifier	yes	
Name	yes	

Purpose of Polyclinic, Transportation, Hospital cases

Fields	Required	Description
Identifier	yes	
Name	yes	

Examination type

Fields	Required	Description
Identifier	yes	
Name	yes	

Examination

Fields	Required	Description
Identifier	yes	
Type	yes	Selected from pre-processed Examination type data
Name	yes	

Consultation type

Fields	Required	Description
Identifier	yes	
Name	yes	

Immunization type

Fields	Required	Description
Identifier	yes	
Name	yes	

Diagnosis

Fields	Required	Description
Identifier	yes	
Name	yes	

Medical intervention

Fields	Required	Description
Identifier	yes	
Name	yes	

Treatment regimen

Fields	Required	Description
Identifier	yes	
Name	yes	

Treatment Interruption reason

Fields	Required	Description
Identifier	yes	
Name	yes	

Outcome (disease/operation)

Fields	Required	Description
Identifier	yes	
Name	yes	May have one of several values: • recovery • improves • unchanged • deterioration • death

Cause of death

Fields	Required	Description
Identifier	yes	
Name	yes	May have one of several values: • suicide • due to illness • other

Name and code of the disease

Fields	Required	Description
Identifier	yes	
Name	yes	

Dispensary registration group

Fields	Required	Description
Identifier	yes	
Name	yes	

Dispensary control group

Fields	Required	Description
Identifier	yes	
Name	yes	

Disability group/category

Fields	Required	Description
Identifier	yes	
Name	yes	May have one of several values: • 1st • 2nd • 3rd

Medicine

Fields	Required	Description
Identifier	yes	
Name	yes	
Dosage	yes	
Form	yes	
Package	yes	

Type of medicine

Fields	Required	Description
Identifier	yes	
Name	yes	

User Type

Fields	Required	Description
Identifier	yes	
Name	yes	Possible values - doctor, nurse, operator, etc.

Annex 2.30 Functional requirements of the system

Mandatory requirements

F01 – Patient management module	
F01.01	Processing of patient data (data processing), especially: 1. Create a patient record via request by unique identifier: a. to e-penitentiary system in case patient doesn't exist in the system, b. to local database in case patient exist in the system 2. Update the patient info, 3. Archive the patient record 4. Remove the existing patient record.
F01.02	Inserting patients group data from the file (.xls, .xlsx, .csv).
F01.03	Saving patient medical history (accomplished in all subdivisions).
F02 – Outpatient module (Data processing[7])	
F02.01	Annual preventive examinations
F02.02	Preventive fluorographic examinations
F02.03	Visits
F02.04	Primary examinations
F02.05	Gynecological examinations
F02.06	Mandatory situational examinations performed by the medical staff
F02.07	Polyclinic visits
F02.08	Stomatological services
F02.09	Emergency calls
F02.10	Refer submodules data with each other and with other modules and submodules
F03 – In-hospital module (Data processing)	
F03.01	Internal inpatient services – provided by the subdivisions of PMC (prisoners' hospital, inpatient service provided by other subdivisions of PMC)
F03.02	External inpatient services – provided by the medical institutions of the healthcare bodies
F03.03	Refer submodules data with each other and with other modules and submodules
F04 - Disability management module (Data processing)	
F04.01	Disability data processing
F04.02	Refer module data with other modules and submodules
F05 - Mental health module (Data processing)	
F05.01	Patients with psychological problems
F05.02	Patients with psychiatric problems
F05.03	Registration and management of the patient with mental disorders
F05.04	Short-term situational psychiatric treatment of the patient
F05.05	Refer submodules data with each other and with other modules and submodules
F06 - Dispensary module (Data processing)	
F06.01	Dispensary registration
F06.02	Refer dispensary registration submodule data with internal and/or external inpatient submodules regarding examination and treatment data.
F06.03	Dispensary control

[7] Data processing – Create, Read, Update, Delete, Archive the record.

F06.04	Refer dispensary control submodule data with internal and/or external inpatient submodules regarding examination and treatment data.
F07 - Drug addiction module (Data processing)	
F07.01	Registrations of drug-addicted patients
F07.02	Management of a drug addiction treatment program
F08 - Medical books and registries module (Data processing)	
F08.01	Quantitative accounting of medicines and medical supplies - storage in subdivisions of the PMC
F08.02	Accounting of distributed medicines and other medical supplies - transfer from the subdivision storage to the residential area
F08.03	Accounting for the provision and receipt of drugs - provision of a specific patient in the residential area
F08.04	Auto process the medicine/drug data in the submodule of "Accounting for the provision and receipt of drugs" in case when any medicine/drug data processed in any module or submodule.
F08.05	Accounting of drugs brought by relatives
F09 – Reporting module	
F09.01	Reports related to the PMC working activities, such as an annual activity report in a PIs or a prisoners' hospital etc.
F09.02	Reports that allow the user to obtain any combined and/or aggregated data from any area of activities without the intervention of developers (Ad hoc reporting)
F10 - Notifications and internal communication module	
F10.01	Notifications to relevant users regarding certain changes and/or events in various modules (submodules) of the system as well as in external systems
F10.02	Providing internal communication between system users in the following ways: 1. Instant messaging, 2. E-mail service (operated within the system)
F11 - User management and user access modules	
F11.01	Roles data processing, especially: 1. Create a role, assign permissions, 2. Update the existing role, add and/or remove permissions, 3. Remove the existing role if the latter is not assigned to any user, otherwise deny the removing, and generate the error message.
F11.02	User data processing, especially: 1. Create a user, assign roles, 2. Update the existing user - add and/or remove roles, update personal info (not username, password, email), 3. Remove the existing user.
F11.03	Creation of user password with email confirmation. Password requirements: • At least 8 characters. • A mixture of both uppercase and lowercase letters. • A mixture of letters and numbers. • Inclusion of at least one special character, e.g., ! @ # ?]
F11.04	Login to the system from the internal network without MFA.
F11.05	Login to the system from the external network by email based 2FA.

F11.06	Authentication with eID and mID
F11.07	Logout from the system
F12 - Interoperability module	
F12.01	Exchange data with e-penitentiary system via GIP.
F12.02	Discuss possible data exchange solutions with ARMED system, as well as with technical teams of other involved organizations.
F12.03	Development of data-providing interfaces of the patient information to external systems via GIP.
F13 - System support and management modules	
F13.01	Processing of catalogues data
F13.02	Secure and reliable usage of database by the modules
F13.03	Initial installation of the system
F13.04	Setting the connection string of database
F13.05	Setting interfaces URLs to interoperate with external systems
F13.06	Archiving the data at any time, as well as by scheduling (daily, weekly, monthly, yearly)
F13.07	Recovering system data from previously archived data
F13.08	Manual data entry functionality that ensures entry as separate data and as group of data from the file (.xls, .xlsx, .csv, etc.).

Conditional (non-mandatory) requirements

F12 - Interoperability module	
F12.04	Development and implementation of interoperability with ARMED system according GIP requirements, if there are no technical or legal restrictions..
F14 – Video module	
F14.01	Study the TOR of the video module to understand how that meet the requirements of the telemedicine (Bidding document - PSMP3-GO-2-2-8/1).
F14.02	Integration of the video module into the EMS in case of meeting the requirements and if there will not any technical restrictions.

Annex 3.1 Technical specifications of PC or laptop

Parameters		
1	CPU	2.10 GHz, 2 Cores, 4 Threads, 4 MB Cache or higher
2	RAM	8 GB DDR4
3	SSD	250 GB or higher
4	Graphics Card	Integrated 512 MB Video Memory or higher
5	Network Interface	Gigabit Ethernet
6	Wireless Interface	802.11b, IEEE 802.11g, IEEE 802.11n
7	Display	For PC – 22”, 1920 x 1080, 60 Hz, 16:9, HDMI For Notebook (built-in) – 15”, 1920 x 1080, 60 Hz, 16:9
8	Operating System	Windows 10 Pro
9	Warranty	3 years

Quantity	
For telemedicine	12
For EMS	12
Total	24

Annex 3.2 Technical specifications of camera

		Parameters	Quantity
1	Resolution	4K/30fps (up to 4096 x 2160 pixels) 1080p/30 or 60 fps (up to 1920 x 1080 pixels) 720p/30, 60, or 90 fps (up to 1280 x 720 pixels)	12
2	Focus type	Autofocus	
3	Microphone	Built-in, range – up to 1m	
4	Field of view	90°	
5	Digital zoom	5x	
6	USB connectivity	USB-A plug-and-play	
7	Compatible	Windows 10	
8	Warranty	2 years	

Annex 3.3 Technical specifications of the network router

	Parameters		Quantity
1	CPU frequency	600 MHz	12
2	RAM	256 MB	
3	Storage size	16 MB	
4	Ethernet	5 x 10/100/1000 Ethernet ports	
5	Warranty	1 year	

Annex 3.4 Response of EKENG

	Questions	Answers
1	Can EKENG provide a computing resource (virtual server - at least with the following parameters - 2 cores, 16 GB RAM) and data storage with 3-5 TB capacity?	The server can be provided, but providing of storage with more than 1TB is problematic. However, if it is possible to purchase storage within the project, it is advisable to purchase the following set of disks to ensure the neccary capacity: 2 x 3.8 TB for Netapp AFF A400 (MKTG. P/N: X357A, Spare P/N: SP-357A)
2	If more resources will be needed during the operation or development phase (in terms of virtual server) than is initially presented, will it be possible to increase the resources? If yes, please indicate the maximum amount that EKENG can provide.	We do not think that a more powerful server need for the product described, but we can increase the settings by 50% if absolutely necessary.
3	Will data be archived to recover data in case of an emergency?	The resources of the government backup data center located in the Ministry of Emergency Situations will be used.
4	Will it be possible to provide access from both - the Penitentiary Service network and the public internet network if solution be installed in EKENG environment?	All necessary access will be provided depending on the need.
	4.1 Will EKENG provide support in case of network access problems?	Yes
5	Due to security concerns, there may be some restrictions for the development company. e.g.: • Uploading certain types of files from external networks, • Make direct changes on any file or in database, • etc. In case of such problems, will EKENG provide support?	The development company under no circumstances will have access to a real database. All problems must be solved in a test environment, which will be accessible to the development company. EKENG is always ready to provide professional support.

Annex 3.5 Technical specifications of the disks

Parameters		Quantity
Capacity	• 3.8 TB	2
Device Type	• Solid state drive	
Interface	• SAS 12Gb/s	
Drive Transfer Rate	• 1.2 GBps (external)	
Form Factor	• 2.5”	
Compatible	• Netapp AFF A400	
Other	• Cage included	
Warranty	• 1 year	

Annex 3.6 Technical specifications of combined device (printer/scanner)

Parameters		Quantity
Printing Technology	• Laser - monochrome	12
Functions	• Printer, scanner, copier	
Paper Format	• A4	
Monthly Duty Cycle (max)	• 10000 pages	
Memory	• 256 MB	
Max Copying Speed	• Up to 23 ppm	
Max Copying Resolution	• Up to 600 x 400 dpi	
Max Printing Speed	• Up to 23 ppm	
Max Printing Resolution	• Up to 1200 dpi	
Document Feeder	• ADF	
Connectivity	• LAN, USB 2.0	
Warranty	• 1 year	

Annex 3.7 Technical specifications of barcode scanner

Parameters		Quantity
Connectivity Technology	• Wired, USB • 2.4G Wireless	21
Barcodes	• Code 93, Code 39, UCC/EAN-128, IATA, Code 39 Full ASCII, Discrete 2 of 5, Codabar, Code 128, Code 11, UPC, Interleaved 2 of 5, Code 128 Full ASCII, Code 39 Trioptic	
Scan Speed	• 100 scan / sec	
OS support	• Windows 7, 8.1, 10, • Mac • Linux (desktops) • Android • iOS	