Problem of Cybersecurity in Context of Medical Information System «Register of Palliative Patients»

Ekaterina Menshikova, Gennady Sigovtsev, Marina Charuta
Petrozavodsk State University
Russia, Petrozavodsk
menshiko@cs.karelia.ru, sigovtsev@petrsu.ru, charuta@cs.karelia.ru

Abstract **The project of a special purpose medical information system for use in the field of palliative care "Register of palliative patients" is proposed. The project provides that the system should have the following basic functionality: providing system administration; maintaining a patient register; searching for patient data by specified parameters; maintaining a patient's medical record including information about prescriptions; searching for prescriptions by specified parameters; generating summary reports and reports for a group of prescriptions. The prototype of the system, presented by its structural-functional and informational models, and its implementation are described. The cybersecurity issues of MISs are analyzed in terms of meeting regulatory requirements. An initial protection level of the «Palliative Patient Register» system was assessed, and the most relevant threats were identified to build a threat model. A scheme for ensuring information security was proposed. A model of data protection in the system based on the exchange of only anonymized personal data between the client and the server is proposed. To do this, we suggest using cryptographic security tools. The General scheme of interaction between the client and server using the REST architecture is described. The possibilities of the Yii framework for implementing the RestFull API are considered.**

I. Introduction

Nowadays information systems are widely obtained in many spheres of life, including healthcare. In modern medicine, information systems are used in all its most important areas, while much attention is paid to the collection and systematization of the versatile information.

In the Russian Federation, in 2011, the Concept of creating a unified state information system in the field of healthcare was approved [1]. The main structural elements of the unified system are medical information systems (MIS) at the Federal, regional, and health facility levels.

MIS of a medical organization (in English, it is also customary to use the term Hospital Information System - HIS) is software product for integrated management of all major processes related to the work of medical institutions. These include: the work of the registry (registration of patients and management of their applications for doctors appointments and medical care), ensuring electronic document flow (electronic medical records of patients, medical research data, medicinal prescriptions, etc.), the functioning of the workplaces of doctors and nurses, managing the resources of the institution (financial, personnel, staff planning. The Russian Ministry of health has developed guidelines for ensuring the functionality of medical information systems [2].

Specific modules can be added to the MIS, such as RIS (Radiology Information System), a radiological information system, or PACS (Picture Archiving and Communication System), a system for storing medical images. Another kind of MIS is laboratory information system (LIS). LIS can be partially or completely implemented as separate components of a complex MIS.

Currently, in our country, there is growing attention to such a specific area of health care as palliative care. Palliative care is provided to the seriously ill, including incurable citizens, in order to maximize their quality of life through medical manipulations and medications. Palliative care should include: medical procedures, relieving the patient from pain, and care for the seriously ill.

The most important (though not the only) category of palliative care patients are cancer patients. This is evidenced by the growing worldwide number of cancer patients in General, and the number of patients dying for this reason, in particular. According to the World Health Organization [3] cancer is the second leading cause of death worldwide (about 1 in 6 deaths is due to cancer).

In Oncology, palliative care should address a wide range of issues related to medical interventions for inoperable neoplasms. A goal of palliative care is the maximum possible recovery with life extension and positive quality. [4]

To provide high-quality palliative care, specialists monitor and evaluate many parameters, which today, as a rule, are recorded on paper. Conventional MIS, on the one hand, are not focused on taking into account the specifics of information processes of this kind. On the other hand, they have obviously excessive functionality for use in palliative care institutions.Thus, in hospices, it is necessary to use an information system that would reduce staff labor and improve the quality and speed of processing the information necessary for organizing palliative care, including that used for maintaining case histories of palliative patients, providing them with medicines and medical services.

Today in Russia there is no unified system for recording patients who need palliative care. For this reason, there are no high-quality statistical data for conducting analytics and

calculating the need for medicines and medical services for this category of patients.

The above circumstances make the task of developing a specialized MIS for palliative care institutions relevant.

Medical information systems (MIS) are one of the most sensitive types of information systems to information security problems, since a number of data entered, processed and stored during the operation of the MIS are personal data or may constitute a medical secret. The consequences of the realization of information security threats can be criminal acts of a selfish nature, as well as actions that have direct negative consequences for the health and life of patients.

As it mentions in [5] «Healthcare cybersecurity has become one of the significant threats in the healthcare industry». The reviews of trends threats and ways forward to cybersecurity in healthcare are publishing annually [6].

In the Russian Federation, MIS refers to the type of information systems for processing personal data (ISPD). Such personal data also include a special category on the patient's health status - sensitive personal data [7]. The Decree of the Government of the Russian Federation establishes the requirements for the protection of personal data during their processing in ISPD [8]. The same decree establishes the levels of security of personal data that ISPD should provide, depending on the significance of this data and its volume.

II. Goals and objectives

The information system "Register of Palliative Patients" is intended for storing and processing data of patients in need of palliative care in the Republic of Karelia, Russia. The system under development, while ensuring information security requirements at the demanded level, should have the following basic functionality:

1. System administration, which includes:
   - Input, Editing and Deleting data about system users;
   - Input, Editing and Deleting records in the system reference books (for example, medicaments reference book);
2. Patient registry management, which includes:
   - Input, Editing and Display of information about the patient;
   - Search for patient data by specified parameters;
   - Input, Editing and Display of prescriptions to the patient;
   - Search for patient prescriptions by specified parameters;
3. Reports generation, which includes:
   - Report generation in PDF format on a group of patient prescriptions for a specified period of time;
   - Summary report generation in PDF format on the status and needs of patients for a certain period of time on the specified parameters in one or more medical institutions.

Among the users of the information system identified the following categories and their rights are defined:

- User - a user who has passed the authorization procedure and does not have the rights of a system administrator: has access to the limited functions of the system, can carry out operations to work with information about the patient and his prescriptions and reporting.
- Administrator - a user with system administrator rights: has unlimited access to the information system functionality.

The above goals and objectives of the development of the system indicate that this system should be focused on satisfying the informational needs of medical personnel related to their professional activities. As noted in [9, 10], this is typical of such systems. Maintaining informational interaction between staff and patients is not one of their primary tasks.

III. Models of the system

A context diagram of structural-functional model of the system is shown at Fig. 1.

The input data streams in the context diagram are divided by external entities that are their sources.

The administrator registers user doctors and accompanies various system reference books used for maintaining medical records and generating reports.

The doctor registers patients and saves their medical records.

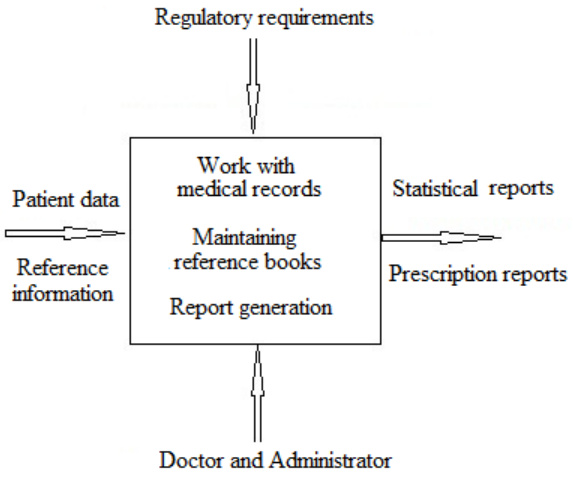

Fig. 1. Context diagram

Information in the form of regulatory requirements defines the structures and formats of data when they are entered and stored in the database and displayed in reports.

The external entities to which the reports are generated by the system are:

- for statistical (summary) reports - the Ministry of Health of the Republic of Karelia;
- for prescription reports - medical users.

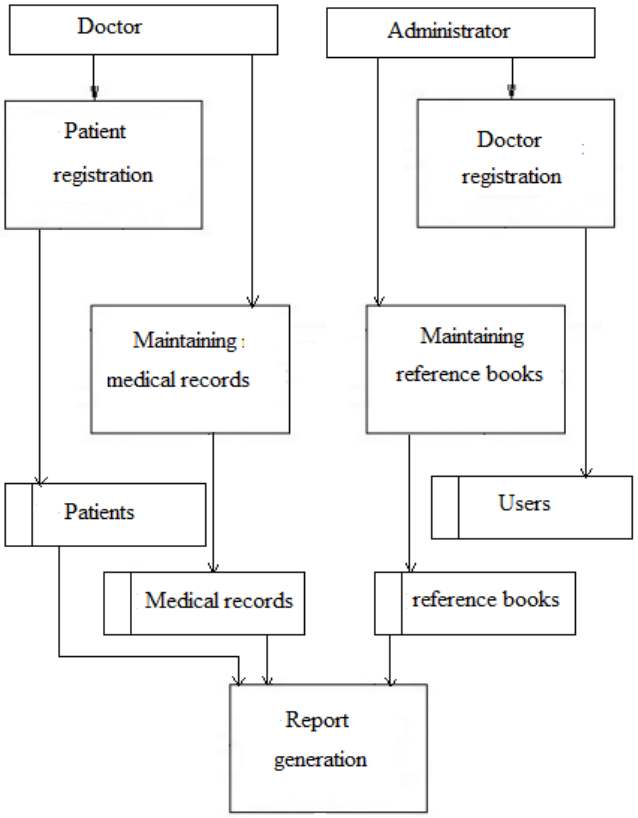

Fig. 2. Context diagram decomposition

The decomposition of the context diagram by functions performed by system users is shown in the Fig. 2. This diagram contains five functions with corresponding relationships in the form of data flows between them and their corresponding storage devices.

The storages presented in Figure 2 are a model of the information content of the system with which its users work. A general view of the information model of the system in the form of an entity-relationship diagram is presented in Figure 3.

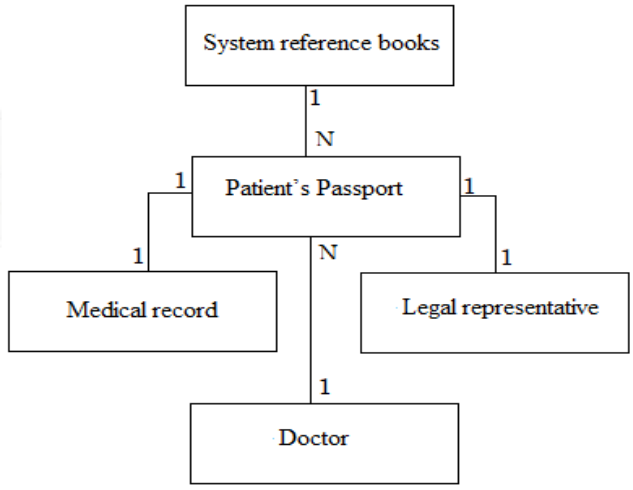

Fig. 3. Entity-Relationship Diagram

IV. The prototype of the system

The prototype of information system «Register of palliative patients» has a classic client-server application architecture.

Currently, a local prototype of the system has been developed, which implements the model shown in Fig. 2.

The diagram presented in Fig. 4 shows the main software modules that compose the system, and the relationships between them. Each of these modules provides an interactive HTML page to authorized users, interacting with which users can carry out the actions assured by their roles.

Also the lines on Fg. 4 shows a set of possible user transitions between system modules that the user can exist while working with it.

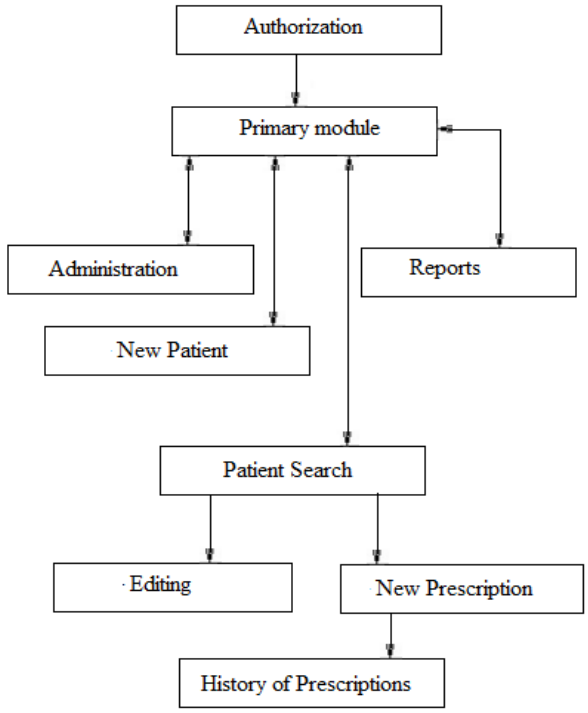

Fig. 4. Architecture of the system prototype

1. The user enters the domain name of the site in the address bar. After that, the system checks for the presence of cookies and session parameters.
   - If there is an active session or the correct cookie data, then the user does not need to be identified and will be redirected to the "Home" page.
   - If the above data are not present or it is incorrect, then the user will see the «Authorization» page to enter a login and password. After successful identification, user will go to the «Home» page.
2. Depending on the rights of the user (Administrator or User), various system functionality is provided. So, the Administrator has access to the «Administration» page using the navigation bar.

3. The transitions between the «New Patient», «Patient Search» and «Reports» can be performed by all authorized users using the navigation bar.
4. After receiving the list of patients according to the specified parameters on the "Patient Search" page, the user can go to the «New Prescription» or «Patient Editing» page. After completing the editing of patient data, the user can also proceed to fill out prescriptions.
5. From the page «New Prescription», the user can go to the «History of Prescriptions» page to view previously created prescriptions and generate reporting.

The system was recognized as fulfilling the specified requirements during clinical testing at the Center for Palliative Care in Petrozavodsk. The prototype of the system was accepted for consideration as one of the variants for the register of patients in need of palliative care, recommended as a standard form of recording in all relevant medical institutions [11].

As a method of user authorization, role-based access control (RBAC) was used with the associated allocation of the necessary resources to store information in the database. At least one role must be assigned to each user, and the total number of roles, permissions, and rules unlimited. For the information system «Register of Palliative Patients» two roles were created (administrator and user) and four permissions (for administration, work with patients data, work with medical records and reporting).

V. CYBERSECURITY ISSUES IN HEALTHCARE

One of the most important tasks in the development of MIS is to ensure information security. At the same time, it is necessary to protect both personal data of patients, their status of health, the course of the treatment and diagnostic process, and information about the MIS itself: its program codes, the organization of storage and work with data, etc. [3]. The speed of development and the breadth of information technology coverage of the healthcare system in our country is in line with global trends. Consequently, the information security problems of domestic MIS will also become more acute.

As noted in [12], there are two important reasons why MISs are becoming increasingly attractive to cybercriminals: «For those conducting cyberattacks the healthcare sector is an attractive target for two simple reasons: it is a rich source of valuable data, and it is a soft target».

Most common cyber threats in healthcare is given in [10], the following are included in the list:

- Theft of personal data for financial gain, such as names, addresses, social security details, and financial information;
- Theft and publication of confidential medical information of certain categories of individuals; for example, celebrities, politicians, or others;
- Use of malicious software for extortion under the threat of blocking data or systems or deleting them;
- Deliberate misrepresentation of data, such as changing test results, for political or personal purposes;
- Denial of service attacks;
- System failure or data loss due to unintentional actions of personnel.

As a rule, they named four properties of information, the violation of which it is necessary to implement such types of threats as [11]:

- confidentiality;
- reliability;
- integrity;
- availability.

For MIS, violations of all four types are possible, but the most dangerous is a violation of reliability, since this can threaten the health and even life of the patient. With regard to confidentiality, its violations occur most often and entail a wide range of undesirable consequences.

Since in Russia MISs have the status of information systems for processing personal data, it is imperative for them to fulfill the information security requirements defined by a special decree of the Government of the Russian Federation [8]. The decree establishes the levels of security of personal data that the ISPD should provide, depending on the significance of this data and its volume.

The rules for determining the required level of security for ISPD are contained in the recommendations of the Federal Service for Technical and Export Control [15]. In accordance with them, the third level includes systems in which:

- there are special categories of personal data;
- the number of personal data subjects who are not employees of the system operator is less than 100,000;
- threats that are not related to undocumented software capabilities are relevant (3rd type).

According to the listed characteristics, the developing system belongs to ISPD of the third level of security.

The general scheme of information security in MISs is based on the following features [14]:

• user identification and authentication;

• organization of authorized access to data;

• control over the rights and actions of users;

• use of cryptographic means of protection;

• control over the life cycle of data in the system.

VI. THREAT MODEL

The first step in the analysis of information security threats is to determine the level of initial security of the ISPD, which consists in its assessment by the following parameters [16]:

1) The territorial distribution;
2) The availability of connection to public networks;

3) Built-in operations with records of personal data databases;
4) The differentiation of access to personal data:
5) The presence of connections with other personal data databases of other ISPD;
6) The level of generalization (depersonalization) of personal data;
7) The amount of personal data that is provided to third-party users of the personal data information system without prior processing.

According to this assessment methodology, the information system «Register of Palliative Patients» has a low level of initial protection, since parameters with a level of protection not lower than average are less than 70 percent (Table I).

TABLE I. CHARACTERISTIC OF INITIAL PROTECTION LEVEL OF THE INFORMATION SYSTEM «REGISTER OF PALLIATIVE PATIENTS».

Technical and operational characteristics of ISPD	Security level
City ISPD, covering not more than one settlement (city, village)	Low
ISPD having multi-point access to the public network	Low
ISPD supporting operations of recording, deleting and sorting records of personal data databases	Middle
ISPD to which access is determined by the list of employees of the organization that is the owner of ISPD	Middle
ISPD, in which one personal data database is used, owned by the organization - the owner of this ISPD	High
ISPD, in which the data provided to the user is not anonymized (i.e. there is information that allows identifying the subject of personal data)	Low
ISPD that does not provide any information to third-party systems	High

Based on parameters with a low level of security, as well as the fact that the system does not use a secure data communication channel, we can conclude that for the information system "Register of Palliative Patients" an actual information security threat is the possibility of interception of protected information by an external perpetrator during its transmission via communication channels.

VII. PROTECTION MODEL

Localization or elimination of the identified actual threat is possible by organizing the transfer between the client and the server of exclusively anonymized personal data.

As noted earlier, special categories of personal data are processed in the information system, which are stored in the «Patient's Passport» and «Medical Record». At the same time, the «Medical Record» without communication with the «Patient's Passport» cannot be identified with a specific patient, i.e. contains anonymized personal data. Anonymization of the personal data of the «Patient's Passport» can be achieved through the use of cryptographic protection - encryption.

The following general scheme for working with anonymous personal data is proposed:

- The client part of the information system requests the necessary data from the server and receives it in anonymous form;
- Prior to displaying to the user, the data to which cryptographic protection tools have been applied are decrypted using local encryption keys;
- At the end of the processing of personal data by the user, the information constituting the “Patient's Passport” is encrypted using local keys and only after that anonymous data is sent to the server.

The use of local encryption keys is justified by the fact that the information from the "Patient's Passport" is processed directly in institutions and does not participate in the compilation of summary reports at higher levels (city or region). These reports are based on data from the prescriptions of the «Medical Record», to which cryptographic means of protection are not applied, that is why it can be freely processed.

In implementing the scheme described above two new challenges may appear: an attempt to access the local encryption keys and the encryption algorithms. The first threat can be localized by using user parameters stored on the server as a key (for example, a unique user token), or by storing the key on removable media designed for this purpose only. The second threat can be eliminated through the use of technology encapsulation of the code, in which access to the source code of the page in the browser will be limited.

The following technologies can be used as particular solutions for implementing the proposed scheme:

- localStorage or IndexedDB for storing data in the browser during encryption;
- Electron framework for encapsulating code;
- REST architecture for the interaction between the client and server.

To determine the possibility of implementing the REST architecture in the existing prototype, the opportunities of creating a RESTful API of the Yii framework, on the basis of which the information system "Register of Palliative Patients" was implemented, were studied. The RESTful API applies to web services that correspond to the requirements of a REST architectural style.

Among these requirements, the following can be distinguished: an explicit separation of the needs of the client requesting data and the server that stores data (the client-server model) and the lack of information about the status of users on the server. The simplest RESTful API for working with user data was developed in the prototype of information system. As a result of the study, it is worth noting that it is advisable to design the RESTful API on Yii as a separate module, for which can set own configuration and at the same time not violate the logic of the system.

VIII. CONCLUSION

Currently, in the Russian Federation, MISs are actively being introduced in the field of healthcare and solve a wide range of tasks related to information support of the activities

of medical facilities at the polyclinic or hospital level. But such systems are not sufficiently effective in narrower areas.

Presented in this article MIS «Register of palliative patients» is focused on the information support for the work of doctors involved in palliative care. It can improve the effectiveness of use of information technologies in this area. The development of a full-scale information security module that implements the model of ensuring cybersecurity for this system proposed in the article will allow to offer this system for practical use in the field of palliative care.

As a prospect for the further development of this project, it can be pointed out that the system «Register of palliative patients» can serve as the core for creating a distributed information system such as «electronic hospice».

One of the tasks facing the national project "Healthcare" is the formation of digital medicine, within which it is planned to develop such an option of Telemedicine as consultations in the format of "doctor – doctor" and "doctor – patient". This format can be used for dynamic monitoring of the patient's condition and treatment adjustments.

Increasing the system "Register of palliative patients" with this kind of functionality, which implements the main principles laid down in the concept of Telemedicine in the field of palliative care, will allow providing a qualitatively new level of care and care for palliative patients.

REFERENCES

[1] Concept of Creating a Unified State Information System in the Field of Healthcare. Ministry of health and social development of the Russian Federation. The order of April 28, 2011 г. N 364. Web: http://docs.cntd.ru/document/902276660

[2] Methodological Recommendations for Ensuring the Functionality of Medical Information Systems of Medical Organizations. Moscow: 2016. Web*:* https://portal.egisz.rosminzdrav.ru/materials/351

[3] *Cfncer*. Key facts. Web: https://www.who.int/news-room/fact-sheets/detail/cancer

[4] On the basics of health protection of citizens in the Russian Federation Federal law of 21 Nov. 2011 ќ 323-ФЗ. Collection of legislation of the Russian Federation. 2019. Web: https: //fzrf.su/zakon/ob-ohrane-zdorovya-grazhdan-323-fz/st-36.php.

[5] Security Threats in HealthCare Systems March 18, 2019. Web: https://consoltech.com/blog/security-threats-healthcare-systems/

[6] L. Coventry and D. Branley, Development Cybersecurity in healthcare: a narrative review of trends, threats and ways forward Web: http://ifets.ieee.org/russian/depository/v16_i2/pdf/13.pdf.

[7] Guliev Y. I., Tsvetkov A. A. Ensuring Information Security in Healthcare Organizations. *Doctor and Information Technology* 2016, № 6, pp. 49-62.

[8] Resolution of the Government of the Russian Federation dated 01.11.2012 No. 1119 " On Approval of Requirements for the Protection of Personal Data when Processing Them in Personal Data Information Systems» Web: http://www.consultant.ru/document/cons_doc_LAW_137356

[9] V. A. Alvarez-Tobyna, I. F. Luna-Gymezb, E. A. Torres-Silvab, J. F. Florez–Arangob,P. T. Rivera-Mejia A. Higuita Usugab, Design of an Information System for Palliative Care: User Analysis *Nursing Informatics,* 2018.

[10] A. Reisa, A. Pedrosab, M. Douradoc, C. Reisd, Information and Communication Technologies in Long-term and Palliative Care *Procedia Technology* 2013, № 9, pp. 1303–1312.

[11] G. P. Tichova, M. A. Charuta, E.A. Menshikova, Information System Register of Patients in Need of Palliative Care. XIII All-Russian Scientific and Practical Conference " Digital Technologies in Education, Science, Society"Petrozavodsk, 2019, pp. 176-178.

[12] Cybersecurity and Healthcare: How Safe are We? bmj 2017; 358 :j3179; (published 06 july 2017).

[13] S.N.Semkin, E.V.Beliakov, S.V.Grebenev, V.I.Kozachok . *Fundamentals of Organizational Provision of Information Security of Informatization Objects*. Moscow: Helios APB, 2005.

[14] G.I.Nazarenko, A.E.Mikheev, P.A.Gorbunov, Ia.I.Guliev, I.A.Fokht, O.A.Fokht Features of Solving Information Security Problems in Medical Information Systems. *Doctor and Information Technology,* 2007, № 4, pp. 39-43.

[15] Methods for Determining Current Threats to Personal Data Security when Processing Them in Personal Data Information Systems FSTEC OF RUSSIA. — 2008. WEB: https://fstec.ru/component/attachments/download/290

[16] J.K.Alhassan, E.Abba, O.M.Olaniyi,and V.O.Wazir Threat Modeling ofElectronic Health Systems and Mitigating Countermeasures // Int. Conference on Information and Communication Technology and Its Applications , Nigeria 2016.