Personal Data Protection and Patient Rights in E-Health: legal issues

Maria S. Ablameyko, Nadzeya S. Shakel

***Abstract*—**The development and implementation of E-Health systems today is an important part of the activities of many states. In this paper, we analyze the main conceptual and strategic legal acts that determine personal data protection and patient rights in E-Health systems. E-Health systems expand the ability of patients to access health information. Nevertheless, a number of organizational and legal measures are required, including with a view to regulating issues of control over access to the Electronic Health Record.

Keywords— E-Health, electronic healthcare, electronic health record, medical professional, patient rights, personal data protection

I. INTRODUCTION

The progress in the development of Information and Communication Technologies (ICTs) in recent decades has led to qualitative changes in the health sector, creating new opportunities in the field of medicine. Today, an increasing number of states entered into Electronic Healthcare stage and create E-Health systems. The central part of E-Health is Hospital Information System (HIS) and Electronic Health Record (EHR).

The main impact of the introduction of E-Health is seen in the qualitative change of relations between the medical practitioner and the patient. It is obvious that they often have different views on what, when and how should be inserted in HIS and EHR systems.

The use of information and communication technologies in medicine drastically changed healthcare in many countries. For example, important figures are given in the study of European region on eHealth issues which was performed by the World Health Organization Regional Office for Europe (47 out of 53 countries in the region participated in the study) [1]. According to the study, as of 2015, the majority of States (28 countries) had national universal health coverage policy or strategy, that specifically referred to E-Health. As for the specific areas of implementation of health information systems, 27 countries reported on the availability of a national EHR system, and 38 countries reported on the use of teleradiology in telehealth programs. In 19 countries EHRs are connected to a pharmacy information system, such as electronic prescriptions. There is no doubt that these indicators have become even higher today.

For any medical officer, accuracy and proper detailing of health data is important. To see the picture of one's health and to establish valid medical treatment scheme, they often require wide range of information. If information that doctors obtain is inadequate, it can cause incorrect diagnoses, wrong prescriptions and sometime cause grave consequences. This poses specific risks, where doctors need to rely heavily on medical documents and patient's descriptions. For patients, on the other side, this all might seem less relevant, as they are reluctant to provide doctors with information that they consider as irrelevant to his sphere of expertise (e.g. information on leg surgery for eye specialist). Another important aspect here becomes the protection of personal data of a patient.

As one can see from the information above, the trend to enhance data protection, especially with regard to health care domain, is obvious. Countries use different methods and take diverse

M. A. Ablameyko, Belarusian State University, Minsk, Belarus (e-mail: m.ablameyko@mail.ru).
N. S. Shakel, Belarusian State University, Minsk, Belarus (e-mail: nshakel@tut.by).

paths in order to achieve the effective and efficient systems of healthcare, which at the same time should be able to ensure protection of patient's rights.

In this paper, we analyze legal aspects of patient rights in E-Health systems. The special attention is given to protection of patient personal data. Thus, this work focuses on the assessment for the development of the E-Health system from the point of view of human rights. As a result, based on the analysis and taking into account the human rights-based approach, we have developed a conceptual framework for the relationship between a medical professional and a patient in the context of E-Health system. Patient rights are considered and proposals for development of legislation in this area are given.

II. HOSPITAL INFORMATION SYSTEMS AND ELECTRONIC HEALTH RECORDS

Modern hospitals heavily rely on Hospital information systems (HIS), that are based on full informatization of a hospital activity and include a number of diverse system components. Such systems today are moving away from the monolithic centralized systems of earlier days and now accumulate medical information in Electronic Health Records, support networked interaction among heterogeneous components, with broad conventions and policies governing communication and interactions with other hospital responsibilities.

Functional features of HIS and its use depend on the territorial level of healthcare, as well as the special features of a particular healthcare organization. The main objectives of HIS implementation are enhancement of efficiency of treatment (reducing of medical errors), and optimization of diagnosis and treatment expenses. The main application fields and functions of HIS consist of:

Patient management: patient registry, scheduling of appointments, admittance and bed control; emergency care; in-patient/out-patient system;

Clinical management: hospital releases; medical reports, electronic prescriptions; surgery appointments;

Diagnostics and treatment: laboratory examinations; medical image analysis, computer-aided diagnosis.

Supplies management: stockroom; ordering of supplies; pharmacy; current assets;

Financial management: accounts payable and receivable; banking control;

Support services: hospital infection controls; assets maintenance; vaccine control;

Research and education: library; convention center scheduling, recruiting and personnel.

Architecture of HIS corresponds to a hospital structure with the same departments. From other side, Hospital Information Systems usually include the following components [2]:

- Laboratory information systems (LIS);
- Radiology information systems (RIS);
- Pharmacy information system (PIS);
- Pathology information system;
- Blood bank system;
- Picture archiving and communication systems (PACS);
- Research information system and others.

There are the following types of data in HIS [2]:

- Clinical and administrative patient data (e.g. electronic health records, including tests results, contact details, etc.);
- Financial, organisational and other hospital data;
- Research data (e.g. clinical trial reports) and data intended for secondary use;
- Staff data;
- Tracking logs;

- Vendor details (e.g. contact details, products used).

The central component of HIS is Electronic Health Record, which is usually created when a patient visits a hospital. Access to the EHR is usually open when patient stays in a hospital (depending on the country, such an access can be open to all medical staff, or only to the doctors that interact with the patient).

Electronic Health Record is an essential tool for the integration of medical data about patient. The purpose of EHR is to store the information about patient that is generated by physicians, nurses, hospital administrators, etc. Thus, EHRs may include medical history, current medications, laboratory test results, etc. This compound of data, in case it is duly organized and managed (clear structure, accurate and full records) can positively impact patient care in several ways. Some advantages involve increased efficiency and higher quality documentation while others involve automated checks and reminders to assist a physician in providing optimum care. It should also be noted that the use of this data can be performed in a variety of ways, which are not always directly connected with better medical treatment of the patient. Thus, from the practical point it is important to ensure that EHRs do not become merely automated forms of today's paper-based medical records; a contemplation of possible new ways and options that digital format can offer, and to ensure that the entire scope of health information in all media forms is used adequately.

The EHR has several advantages over the conventional paper-based medical record, which includes the following elements:

- Patient information is available at several working places at the same time.
- Information can be easily and quickly accessed (e.g. in case of emergency).
- Data can be better comprehended due to use of advanced user interfaces.
- Reuse of results of medical operations is supported, even over the lifetime of a patient. No need to pass same medical tests at various institutions or periods.
- Medical research is performed on a more accurate data (in case data are transferred to computer from a regular paper-based form, some mistakes are almost inevitable; in case data is entered directly into the system the chances of mistakes exist, of course, but they are not doubled by the situation of copying).

Thus, the creation of EHR is generally seen as a positive step both by medical professionals, who want to perform their functions in the most efficient way, and by patients, who see this system as an important way to ensure they get proper medical help, and have additional control over their medical history.

However, as any other system, especially at the initial stages of its implementation, the EHR has its disadvantages:

- It requires a larger initial investment than its paper counterpart because of hardware, software and training costs for the personnel. Moreover, many doctors, especially those close to the retirement and/or not very well familiar with modern IT gadgets and technical advancements might feel it burdensome and unnecessary to study new systems. This becomes especially stressful for all these professional when the system is structured in a counter-intuitive way or in a way that is otherwise not comfortable (e.g. very small fonts, large number of fields to be filled in, low efficiency of systems, when documents, especially image files, are opened very slowly). Another important issue here also lies with the overall great pressure on medical professional, who often work in a very tight time-limits; studying any new system requires time and efforts, that cannot be always available.
- A lot of medical information can be needed to make a decision. Capturing the collected data for an EHR can require a lot of time and efforts. However

sometimes important information can be skipped or overlooked namely because of the great amount of the data in the systems, which can be put in different folders.

- Data security. Easy and expedient access to person's data poses risks as to their integrity and possible future uses.

Thus, it is desirable to consider and wage these positive and negative elements at the early period of implementation on EHR, so as to be able to mitigate any threats.

Current development of E-Health is largely connected with the active use of could technologies, web-services, telehealth (remote interaction between a doctor and a patient with the use of technical means, such as computer, and specific software) and even mHealth (i.e., mobile healthcare, which ensures interaction via tablets, phones that are using medical applications, social networks, etc); electronic health records; medical analytics and big data. As the key trend in medical information technology of today is data integration (Connected Health), many countries see as the central part of their E-Health system an integrated EHR, that collects information (structured electronic medical documents) from distributed databases [15]. An interesting trend is a possible transformation of the concept of E-Health into the iHealth, where "i" at the moment has no established meaning, but, reflecting the growing role of the patient in the current era, can mean an individual, information, informatization, and innovation.

III. LEGISLATION IN MEDICAL DATA PROTECTION AND PATIENT RIGHTS: INTERNATIONAL EXPERIENCE

Data protection issues are increasingly important, as many countries tend to adopt or supplement data protection legislation in order to ensure high level protection of personal data. Special laws regulating the protection of personal data have already been adopted in more than 100 countries [5]. Data protection specific rules are often in place when it comes to the specific provisions on medical data protection.

Important developments take place in Americas. For example, in 2018, the law on data protection was enacted in Brazil. It was followed by further regulations, such as Decree No. 9637 of 2018 on National Information Security Policy; Law No. 13787 of 2018 on computerised systems for the storage of patient records; and Provisional Measure No. 869 of 2018, which created the National Data Protection Authority in Brazil [7]-[8]. In US, data protection issues in medicine are governed by the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996. HIPAA, though enacted in 1996, has important rules on privacy and security of health-related information.

Japanese regulation, namely, the Act on the Protection of Personal Information (enacted in 2003) have borrowed a lot of American concepts of privacy laws [9].

In China, the Network Security Law of the People's Republic of China, which was formally put into effect on June 1, 2017, regulates that network providers must not disclose, falsify, or destroy any personal information they have collected. The Information Security Technology and Personal Information Security Specification (enacted on December 29, 2017) followed soon, were privacy-related terms were clearly defined and many important data protection rules were introduced [6].

In the European Union, the right to a private life and associated freedoms are considered as fundamental rights. In 1995, Directive 95/46/EC was enacted by the EU with the purpose of creating a set of rules for its Member States on the protection of individuals with regard to the processing of personal data and on the free movement of that data between Member States, which was further complemented by other rules and regulations. General Data Protection Regulation (GDPR), which entered into force 25.05.2018, created a specific and quite elaborate regime of protection of personal data, giving specific emphasis to the sensitive data, which also

covers data on health issues [3,4]. However, the way these norms are applied in practice with regard to data protection activities in HIS systems can have variations. Some countries, for example, pay considerable attention to the possibility of tracking all actions committed with the EHR. For example, in Estonia, every access of a healthcare professional to these patients is registered by the system. E-Health system stores data about who specifically requested what data of a particular citizen. The patient can identify those who had access to his EHR, including online, and also has the right to specify the purpose for which this access was carried out.

Russian Federation has a comprehensive data protection law, which include quite specific norm, for example, that the personal data of Russian citizens are to be stored in databases and information systems that are located on the territory of Russia. Only in case the localization requirement is fulfilled, the data can be transferred abroad. There is also a set of rules which cover E-Health systems and data protection issues. Namely, medical workers are obliged to respect patients' rights with regard to circulation of undisclosed information and personal data in general; specific rules on liability are also in place [10].

In Australia, the patients also have broad rights of control over their personal data and privacy in the sphere of healthcare. Any patient has the right to get acquainted with the following information: the time and date of access; who got access; actions that were performed during access (receiving information, entering information, etc.). It is possible to set a notification via email or SMS to be immediately informed about the fact that the EHR was accessed. If the patient is concerned about someone else's access to their EHR, they can contact the EHR support service, which will conduct an appropriate investigation [11].

Belarusian law "On Healthcare" stipulates that the patient has the right to receive information about his own health in an accessible form (Article 41); the main source of information about the patient's health is his attending physician (Article 17); the information should be provided in compliance with the requirements of medical ethics and deontology (Article 46) [12]. However, at the moment, as there's no general data protection law, personal data protection is governed by the general rules on privacy, thus the legal regime in this sphere is quite fragmented.

As you can see from the information above, the trend to enhance data protection, especially with regard to healthcare domain, can be traced in many countries of the world. Countries use different methods and take diverse paths in order to achieve the effective and efficient system of healthcare, having due consideration to the necessity of protection of patient's rights.

Thus, the implementation of the EHR is to encompass a varied set of measures. Legislative acts are to provide necessary rules, standards and guarantees. Training and helpdesks are to be operating in order to ensure that all necessary information is available both to the patient and to the medical official when they are starting work with a new system. To ensure maximum transparency and usability it is important to ensure that patient can have various options of accessing his EHR and analyzing the information contained therein. The patient should be able to track all actions performed with his EHR. To do this, when viewing or making an entry in the EHR, the possibility of tracking the date, time and author of the medical record in automatic mode can be installed.

As EHR systems are complex and involve various applications, it is almost inevitable that conflicts, disputes and similar events will arise. Thus it is highly important to implement the security systems, with relevant units that will have appropriate duties and powers with regard to the security incidents and other negative event.

IV. HIS DATA PROTECTION

One of the main purposes of HIS is to automate and facilitate the decision-making process of medical and managerial personnel. The system as a whole is complex and its structure should properly reflect and cover all the activities of the medical institution (hospital).

The structure of HIS can be represented as a set of specialized workplaces of medical personnel that exchange data with each other. Ideally, the workplace of each employee is formed in accordance with their direct professional and job responsibilities and provides all the necessary tools for automation, collection, transmission and processing of information, enabling the medical staff to organize the processes of diagnosis and treatment in an efficient way. The implementation of HIS in a medical institution should provide reliable storage and prompt access to the data of patients.

All information collected during the patient's lifetime is shared in terms of access to it by the medical staff. HIS are distinguished primarily by the fact that they store and process information that comprehensively determines a person's social status, and this determines a special form of relations between those who form it and those who use it. This means that, along with increased requirements for the reliability of information, moral restrictions must be imposed on access to it, as well as the legal responsibility of the persons providing it. Any medical professional is fully responsible (morally, administratively, and criminally) for the confidentiality of the information that he or she has access to in the course of his or her professional activities.

Availability, completeness and quality of the records and data in HIS are also important as they can form a basis for a subsequent analysis of the healthcare provision, especially in a conflict situation. Paper documents can be easily modified or forged. In cases when any assessment of the quality of medical care takes place, the quality of medical records is of paramount importance. The completeness of the data in HIS, the ability to track all changes in it allows one to analyze the activities of medical professionals, including in the event of conflict or dispute situations [13]. However, the system has to be designed in a way that will not discourage medical workers from inserting all the information they consider as necessary. The problem which is seen today is that doctors, especially on the early stages of their career, are reluctant to include specific and / details information into the EHR, as they do not want to be seen as making mistakes. A paper-based format allows more flexibility, and thus doctors feel that they are less at risk.

Another important issue with regard to the protection of privacy and personal data in HIS is the delineation on access to its resources (databases), in order to ensure the required level of confidentiality, integrity and availability of information. The decision on how and to what extent to have this delineation depends on the function on the appropriate medical unit. For example, emergency care unit is usually interested in immediate and quick access to patient’s data, as emergency situation can be caused or can influence any part of the body. Whether such access should be granted to the professionals in the less urgent cases – is less clear. In many cases, countries decide that it is a patient who is to grant a specific medical practitioner a permission to access his data, for example, by using a one-time access code.

The core of any HIS is the Database management system (DBMS). The choice of a DBMS is of key importance, since most of the specified IT security functions are implemented by standard DBMS tools. As the studies [13] show, the most serious reasons for using a powerful security system are:

1. Accidental or intentional actions of registered users. As many IT professionals say, the major threat to any IT system is its user, who does not generally know modern threats and / or thinks that his actions do not pose threat to the security. Thus, for example, medical documents can be opened by a doctor and left on screen for an infinite period of time, where anyone can get access to them. Sometimes information about the dismissal of a doctor, nurse or any other

worker of a medical institution that has access to HIS is not given to the IT department, and they can enter the system and see the information for a long time after they seize working. Various means are used in order to mitigate this risks, for example, electronic cards, automatic blocking of workstations, a limit on the working time during which the user can gain access to the system, regular password changes.

2. Computer viruses. Viruses can cause serious harm, as they can destroy information, block access to it, or transfer personal medical data to unauthorized people. Thus, it is necessary to combat this problem, which can possibly include: a complete ban on the use of unverified CDs or other media, a ban on the use of the Internet or unverified e-mail on the workstations of the system, the use of modern antivirus programs and their constant updating.

3. Third-party actions. This can include interception and modification of data, filling the network with false information packets, and other actions aimed at disabling network equipment or servers.

Thus, to sum up, the creation of HIS infrastructure call for specific attention to ensure that all territories where IT infrastructure is located have appropriate security measures, and that only authorized personnel can enter such premises. Timely update of anti-virus software can also eliminate some of the issues.

Most of the information that circulates within the information space of a medical institution falls under the definition of medical secrecy. The content of medical secrecy includes data on the fact of seeking medical help, on diagnosis and treatment, on treatment methods, on the state of health of the person who sought help (his physical and mental disabilities, intimate relationships, etc.). The protection of this data is attained by provision of specific rules and sanctions, in order to ensure that only authorized parties can have access to this information. For example, in Belarus unlawful dissemination of the medical data described immediately above can cause criminal liability.

Taking into consideration all of the above, we think that is important to turn attention to the certain principles of security system’s operation:

1. The system must implement a procedure for establishing the identity of users (identification, authentication, etc.). The DBMS administrator assigns each employee of the medical institution a unique login/password pair, which is used to uniquely identify the user of the system.

2. The system must be audited. To this end, the following key events must be strictly recorded: the user's entry into the system, changes in the data on the medical institution's contingent, the completion of appointments and referrals, working with the patient's outpatient card, and the end of the user's work with the HIS.

3. The HIS administrator must be able to assign and restrict access rights to users of the system. The workplace of an employee of a medical institution consists of a set of functional software modules, the composition of which is determined in accordance with the official duties of the user. Each user of the system should only have access to their workstations in the HIS.

4. For patients of a medical institution, it should be possible to allocate a group of privileged (VIP) patients and close general access to their medical and personal data.

5. The possibility of verifying the authenticity of electronic documents should be implemented. When the user approves medical documents, the electronic digital signature technology must be used with additional authentication at the time of signing the document.

V. PERSONAL DATA PROTECTION IN EHR

In a modern democratic society, human rights, and in particular the right to privacy, are of paramount importance. The protection of personal data of the individual must be carried out

not only at the national level, but also the adoption of international instruments to ensure respect for human rights and fundamental freedoms in all countries, regardless of nationality or place of residence, and especially the right to privacy in connection with the processing of personal data. This is primarily due to the fact that today personal data is present on the Internet, most of which is distributed and used in social networks.

Changes related to the regulation of personal data (information about a person's personal life) are now taking place in many states. Special laws regulating the protection of personal data have already been adopted in more than 100 countries. As we wrote, in 25.05.2018, the General Data Protection Regulation (GDPR) came into force in the European Union.

The GDPR provides more rights to citizens to be better informed about the use made of their personal data, and gives clearer responsibilities to people and entities using personal data. The definition of personal data processing provided by Article 4(2) of the GDPR is extremely broad, as it includes any operation or set of operations carried out on personal data, with or without automated means, which encompasses all processes from the collection to the destruction of the personal data. Furthermore, personal data processing is only allowed if at least one of the hypotheses as provided in Articles 6(1) or 9(2) of the GDPR is present. These include (1) when the data subject has given consent to the processing of his or her personal data for one or more specific purposes, (2) for compliance with a legal obligation to which the controller is subject, (3) to protect the vital interests of the data subject or of another natural person and (4) for the purposes of legitimate interest [3].

In E-Health systems, creation of electronic health records is essentially an action that initiates the beginning of the processing of personal data of a person. In the EU, countries are divided into three groups with respect to obtaining consent for the creation of her: 1) requires to express consent of the patient in the EHR, and the inclusion of data from EHR in a centralized information system of public health (Germany, Norway, France); 2) do not require to express consent for the creation of EHR, but it is necessary for inclusion of data in a centralized information system of healthcare (Belgium, Denmark, Sweden, Estonia); 3) do not require to express consent for the creation of EHRs and the inclusion of data from the EHR into a centralized information system health (Finland) [14].

Every person must have right to access health information. This right takes on a new meaning within the framework of the introduction of E-Health systems, since new systems must be designed in such a way as to allow the exercise of this right at the highest possible and acceptable level for the patient. Access to health information with the help of EHRs is in many aspects faster and more convenient than obtaining such information by visiting a medical institution, which often leads to problems such as the need to wait in line for a medical worker, limited time to receive information from him, the possibility of illness due to contact with persons who may be infected, etc.

VI. Rights to Access Medical Information

EHR provides important opportunities for patients, compared to the “regular” way of accessing information about one’s health, which could include making appointment with a medical official, visiting a medical facility, requesting your medical card and trying to remember or obtain the copy of the information.

Introduction of a remote access to EHR provides quicker and easier option, which requires only present of a computer (or any other device that can be connected to the Internet, including regular mobile phone), logging and choosing the information that is of interest. As a whole, it seems to be an important way of the realization of the right to access health information, which is an important component of the right to health.

Let's take a closer look at the technical process of realization of these rights and describe the basic steps that a user needs to take in order to access her information [13].

The first step is authentication. In this case, the user account is used, which is defined by an open user name and an encrypted password. Each user's account is stored in a specific form in HIS. When performing the identification procedure, the user enters her name and password, which are then checked by the system for correctness.

If the first step is completed, the user opens a session with the server. All subsequent actions are performed on behalf of the account for which she successfully entered the password.

When accessing the database, the server checks whether the current user has the rights to the information that it requests. In case of a positive decision, the information is provided to the user. In case of a negative decision, the user is denied access.

So, for each HIS object a list must be set, according to which the HIS itself will check whether this user has the right to access this object or not. Such list is usually called Access Control List (ACL). The main objects of the HIS, for which an ACL must be set, are:

- information stored in the database;
- applications included in the system software package;
- commands and functions in applications that can be used with different access levels.

In this case, the order of verification should be carried out from large to small, i.e. first it is needed to pass a check for permission to access the patient card, then to its documents, etc.

VII. PATIENT RIGHTS

Obtaining health information is an important part of realizing the right to health. Today, the availability of complete, reliable and understandable information is the basis for making further decisions about how and to what extent to receive treatment, how to plan your life taking into account the state of health, etc.

The importance of health data for any patient determines the fact that the information should appear in the EHR promptly and in a sufficient volume (in particular, this applies to the results of tests, data on past appointments, records of information provided to the patient during a personal visit to the doctor, data on manipulations, procedures, medical measures taken in relation to the patient).

Patient’s right to access and control his health information (by using EHR functionality) can be attained exercising a number of rights, which include:

- right to read all material in EHR;
- right to refuse to process his data in EHR,
- right to make decisions about his health (including within the framework of digital technologies such as electronic prescriptions),
- the right to remove information about himself and his health from E-Health systems.

Patient’s right to health information is an important part of States’ efforts to improve public health literacy, as it enhances overall effectiveness of healthcare efforts (this can be explained, among other things, by the fact that when people understand the essence of the proposed treatment, they are more likely to follow the doctor's prescriptions). The problem is that, though the advent of EHR gives the patient additional opportunities to access medical information, the question rises as to whether patients can understand the medical terms, slang and abbreviations, and come to the right conclusions about their diagnosis and conditions. The important of this issue rises, as patients tend to take a more and more active role in determining what and how should be treated. Sometimes, “pure” medical information, which is not accompanied by any

comments and explanations, can be wrongly perceived by the patient. There are instances of people who thought of committing suicide after seeing in their EHR diagnose or test result that they consider as fatal to them. Thus, in some specific cases as we've just described, patient's right to information can be ensured by providing him of the said data, but only with necessary explanation, and with personal contact with a medical professional (it is obvious that in today's COVID situations, when certain restrictions on movement are in place, face-to-face contact might not always be appropriate; however there are now many technical ways that allow doctor to contact his patient and remotely discuss the details of his condition).

Let us now turn to the aspect of patient's control of access to her personal data. When EHR system is implemented, such access becomes widely possible for a virtually unlimited number of medical professionals. In this regard, the rights of the patient to determine the boundaries of access to information about their health deserve special attention.

This issue can be considered from two aspects: access to relevant information by the attending physician (or other medical professional who directly interacts with the patient) or by any third party.

The right of the patient to determine the limits of access to information about his health gives him the opportunity to independently decide whether he wants a particular medical professional to be able to see certain information about him. As we've discussed above, this can be achieved by using one-time access codes, generated by the patient who is willing to show his medical details to a specific person.

The right to control access to information about one's health may be restricted, in particular to ensure the vital interests of the person, if their consent cannot be obtained. In Finland, the law provides that consent is not required if the patient is unconscious. In France, if a person is unable to express their will and if circumstances require it, the emergency doctor may, in the best interests of the patient, decide to access the EHR without obtaining prior consent.

In recent years, the prevailing position is that it gives the patient even broader rights, namely, the right to remove information about themselves and their health from Electronic Health Records (or not to create an EHR in the digital environment at all). In order to answer this need, many states today have implemented the provision of citizens with the opportunity to quickly and easily "exit" from EH system.

Part of the patient's right to participate in making decisions about their health is the ability to independently enter additional information about their health into the EHR (assessment of the dynamics (improvement or deterioration) of their condition, assessment of the impact of medicines, data on pressure, the amount of exercise performed, certain pain sensations, etc.).

Thus, EHR system shall be construed in a way that ensures patient's right to control her information. This can be achieved by implementing all or any of the options described below:

1. Currently, the creation of E-Health system envisages a personal account of a patient, through which it will be possible to make an appointment, call a doctor at home, get an extract from medical documents, a reminder of vaccinations and an electronic prescription, view the results of tests, etc. Implementation of many HIS is accompanied by creation or linking to it a call service or support services, where all medical information and details, i.e. on the work of medical institutions, cost of their services and other relevant data, can be accessed in one call. In order to expand the possibility to control medical information, the capabilities of such services can be extended. For example, they can operate to ensure the need of blind people to access information about their health.

2. In order to exercise the right to choose the attending physician and the healthcare organization, a single information space can be created, with integrated IP and HER in both public and private medical institutions.

3. Step are to be taken to ensure fixation of the information in EHR in an accessible and

understandable form to human perception (i.e. decoding of diagnosis). It is important in order to ensure clarity of information about one's health and methods of medical care. Further steps can include the creation of information support services (patient support services): descriptions of diseases, basic treatment methods, descriptions of medicines, etc.

4. Due to various circumstances in life, patients sometimes have special interest in selecting persons that can be informed about their health status. Thus, EHR should individually reflect the information about who the person is ready to inform about their health, as well as make decisions about patient's health if her health condition makes it impossible for the person to decide herself. It should be noted that sometime the legislation defines people that can make decision related to person's health, however this approach is not always perfect. It is obvious that one can have quite tense relations with her relatives, and thus their decisions might not be relevant. Thus, a patient might consider that other people are his "close" one, and should be able to define them, and specify this information in EHR so that medical professional are aware of this information.

5. EHR should also include and maybe even specifically mark some of the patient's decision, especially those connected with his desire not have certain medical care, including medical interventions (namely, consent to donation, blood transfusion, etc.).

Thus, the analysis of the above and the "doctor-patient" interaction in general allows to conclude that the purpose of E-Health development is primarily the availability of services and quality of care provided by healthcare institutions through the use of ICT, as well as the awareness of the population about their health, the timely application of ICT in the diagnosis and treatment of diseases.

To further improve the legal framework of E-Health, it is necessary to focus on the following aspects of the legislation development:

- the right to access information about their health that affects the freedoms, rights, duties, interests of the patient, including the use of mobile applications;
- use of web services, remote interaction between the doctor and the patient through a variety of means: social networks, smartphone, tablet, etc. (mHealth);
- increasing the role of the patient in HIS, as a condition for the development of personalized medicine, with the right to "oblivion", etc.
- protection of personal data and legislation of certain secrets.

VIII. Conclusion

Medical informatics is the rapidly evolving field that allows to significantly improve work of hospitals. Electronic Health Record is a core of Hospital Information System and it allows to collect and to store all information about patient. The application of these systems in hospitals will contribute greatly to improve quality of healthcare in a community.

Every country pays considerable attention to issues related to the development of E-Health. As the analysis has shown, the practical implementation of the measures planned for further implementation, taking into account international obligations, foreign experience and national characteristics, should take into account the need to ensure human rights at the same time. It seems that only in this case, the interaction of medical worker and patient in a new electronic environment will be carried out as effectively as possible, which in general will become an important aspect of the realization of the right to health and other human rights.

Acknowledgment

The article is based in part on the study "Medical worker and patient: interaction in e-health" conducted in 2019 under the auspices of the Center for Human Rights at the Faculty of International Relations of the Belarusian State University in cooperation with the Ministry of

Health of the Republic of Belarus and with the support of the Raoul Wallenberg Institute of Human Rights and Humanitarian Law. The authors want to thank these organizations for their support and valuable contribution to the development of the research.

REFERENCES

[1] "From innovation to implementation: E-Health in the WHO European Region". World Health Organization. URL: http://www.euro.who.int/__data/assets/pdf_file/0018/310455/From-Innovation-to-Implementation-eHealth-Report-EU-ru.pdf.
[2] Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures. European Union Agency For Network And Information Security. November 2016, 55 p. URL: www.enisa.europa.eu
[3] I. Deguara, "Protecting patients' medical records under the GDPR". URL https://www.um.edu.mt/library/oar/bitstream/123456789/40287/1/The_Synapse%2c_17%282%29_-_A1.pdf.
[4] Recommendation CM/Rec(2019)2 of the Committee of Ministers to Member States on the protection of health-related data: adop. 27 March 2019, Council of Europe. URL: https://search.coe.int/cm/pages/result_details.aspx?objectid=090000168093b26e. (accessed: 10.04.2020).
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. (accessed: 01.05.2020)
[6] M. Gong, S. Wang, L. Wang, C. Liu, J. Wang, Q. Guo, H. Zheng, K. Xie, C. Wang, and Z. Hui, "Evaluation of Privacy Risks of Patients' Data in China: Case Study". *JMIR Med Inform* 2020;8(2):e13046/ doi: 10.2196/13046
[7] F. A.Vieira and C. B. Cunha Costa, Data Privacy and Protection Relating to Healthcare in Europe, the United States and Brazil. *Latin Lawyer*, April 30 2020, URL: https://www.lexology.com/library/detail.aspx?g=99b83b76-3f2f-4b23-a5c3-30ad576af369
[8] J. J Kim Marshall, "Japanese and American Privacy Laws, Comparative Analysis", *J Info Tech & Privacy* L. 2015. URL: https://repository.jmls.edu/cgi/viewcontent.cgi?article=1782&context=jitpl.
[9] H. Yamamoto, "Use of personal information in medical research in Japan". *The Lancet.* 2016 Oct;388(10055):1981–1982. doi: 10.1016/s0140-6736(16)31867-0.
[10] A.N. Pishchita (2013) "Legal Maintenance of Patient Data Confidentiality in the Russian Federation". In: Beran R. (eds) *Legal and Forensic Medicine.* Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32338-6_128
[11] See who has accessed your record. My Health Record. Australia. URL: https://www.myhealthrecord.gov.au/for-you-your-family/howtos/see-who-has-accessed-your-record. (accessed: 20.05.2019)
[12] S. V. Ablameyko, M. S. Ablameyko. "Legal issues of the development of E-Health in the Republic of Belarus". *Management Problems* No. 4, series A and B / Academy of Management under the President of the Republic of Belarus. Minsk, 2014. p. 33-40.
[13] S. V. Ablameyko, V. V. Anishchanka, V. A. Lapitsky, A. V. Tuzikov. *Medical information technologies and systems*, Minsk. UIIP NAS Belarus, 2007, 121p.
[14] N. V. Shakel, M. S. Ablameyko. *Medical worker and patient: interaction in the conditions of electronic health care.* Minsk: Ecoperspektiva, 2020. 120 p
[15] E-Health as a factor in improving the quality and availability of medical services for the population [Elektronnoe zdravooxranenie kak factor povysheniya kachestva I dostupnosti medicinskogo obsluzhivaniya-naseleniya]. 2014. URL: http://www.dompressy.by/2014/11/20/elektronnoe-zdravooxranenie-kak-faktor-povysheniya-kachestva-i-dostupnosti-medicinskogo-obsluzhivaniya-naseleniya/. accessed: 15.08.2019. (in Rus.)