Malwina Edyta Kowalska, Szczepan Jakubowski, Artur Romaszewski
Information Systems Department, Institute of Public Health, Faculty of Health Sciences, Jagiellonian University Medical College
malwina.kowalska89@gmail.com

PATIENTS AND THEIR DATA – PART 1 – THE RIGHT TO HEALTH DATA IN THE LIGHT OF IMPLEMENTATION PLANS REGARDNG ELECTRONIC MEDICAL RECORDS DOCUMENTATION AND GDPR

Introduction

After several years of preparation and debates in Poland, a decision was made to change radically the form of medical documentation that is required from healthcare entities. Pursuant to the draft regulation that changes current provisions on medical documentation[1], a digital form is considered to be the basis. Paper-based records will be acceptable only in exceptional situations such as a lack of organizational and technical conditions to run computer-based records and the cases defined by law (e.g. areas with poor Internet connections or power failures).

In order to eliminate the practices of using both computer- and paper-based documents, a uniform form of medical records is to be applied in particular healthcare entities. Thus, the documentation must be conducted either electronically or in paper form. In time, it will be forbidden to have documentation in both forms in one entity and, consequently duplicating patient data will be avoided.

Due to the implementation of new IT solutions, the scope was changed of data that are indispensable for the electronic medical records to operate. The catalogue of data that is included in medical records was extended by unique e-prescription numbers - as they became increasingly more common, numbers of e-referrals and the identification numbers of healthcare assistants.

Record keeping is expected to be easier as the number of data entered into the documentation system will be limited. A possibility of a follow-up of medical history will be provided in the cases of patient's several hospitalizations in the same hospital.

The objective of the implementation of electronic medical records documentation is to facilitate the information sharing processes regarding the treatment of a particular patient

[1] Draft regulation of the Minister of Health of 10 November 2019 on the types, scope and templates of medical records and methods of their processing, https://legislacja.rcl.gov.pl/projekt/12326010/katalog/12634203#12634203 (Accessed:17 November 2019).

among various healthcare entities. Patient data can be transferred via ICT by the information producer to the person that referred the patient for diagnostics, consultation or treatment or to a primary care physician. Sharing the information in a paper-based form will be acceptable only when organizational and technical conditions make electronic methods impossible.

After recording the data that was transferred and that is crucial to the diagnostic, therapeutic or treatment process, the paper-based documentation provided by the patient should be returned or destroyed in the way that prevents the identification of the patient. This procedure aims at a gradual elimination of paper-based documentation and it also solves the problem of the storage of the growing amount of paper-based medical records.

The implementation of electronic documentation and the development of an IT system that in indispensable in the creation and processing of documents require several operations on the part of healthcare entities. This regards both the development of a system from the very beginning or the adaptation of the existing ones.

1. Ownership of medical records and the right to data in medical records

Polish regulations do not define clearly who has the ownership of medical records, whether it is the healthcare entity or the patient. The *Regulation of the Minister of Health of 29 July 2010 on the types of medical records in occupational medicine service, the methods of keeping and storing the records and on the document templates* states that the records are owned by a healthcare unit but this is restricted only to a particular type of documentation[2].

It seems justified that medical records should be owned by the institution that produced them. The healthcare entity cannot simply get rid of medical documentation. Keeping, storing and sharing medical records is an inseparable element of healthcare activity. These issues are regulated by The Act of 6 November 2008 on Patient Rights and the Patient Ombudsman[3] and the Act of 28 April 2011 on healthcare information system[4].

[2] Regulation of the Minister of Health of 29 July 2010 on the types of medical records in occupational medicine service, the methods of keeping and storing the records and on the document templates, Journal of Laws 2010, No.149, item 1002, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20101491002/O/D20101002.pdf (Accessed: 17 November 2019).
[3] Act of 6 November 2008 on Patient Rights and the Patient Ombudsman http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20090520417/T/D20090417L.pdf (Accessed: 17 November 2019).
[4] Act of 28 April 2011 on healthcare information system (http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20111130657/U/D20110657Lj.pdf (Accessed: 17 November 2019).

The patient has the right of access to medical records in the forms that are defined in The Act of 6 November 2008 on Patient Rights and the Patient Ombudsman. This refers to medical records that concern patient's health and the services provided. Moreover, patients have the right to authorize other persons to access their medical records[5].

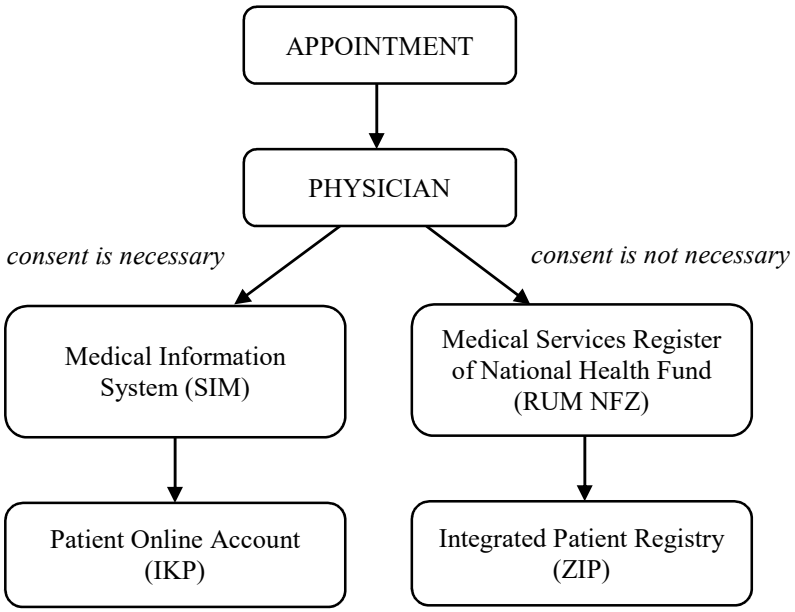
Patients' right to access to their own medical records does not interfere with the right of a healthcare entity to own medical records. This is due to that fact that the patient is never entitled – with some exceptions – to possess the whole records in their full (original) version. Patients have the right to see their medical records, to their excerpts, certified copies or copies. The original copy can be given out only on the request of an authorized body or entity. In such cases medical records can be made available on the receipt of the documents and must be returned in due time[6]. Thus, it means that patients never have the ownership of their medical records; they only come into their possession.

Moreover, The Act of 6 November 2008 on Patient Rights and the Patient Ombudsman[7] regulates the restrictions for physicians and hospitals as regards the transfer of medical records and it gives patients the right to share their medical records with anybody – even to publish them in media. Thus, it seems appropriate to define in the above act who is and who is not entitled to medical records.

As regards the processing of patient data, patients' consent or its lack expressed in the course of the first (or subsequent) visit at the specialist is crucial. Figure 1 presents in a simplified way when the consent is or is not required and where patient data is transferred in the next stages.

[5] Act of 6 November 2008 on Patient Rights and the Patient Ombudsman http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20090520417/T/D20090417L.pdf (Accessed: 17 November 2019).
[6] Act of 6 November 2008 on Patient Rights and the Patient Ombudsman http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20090520417/T/D20090417L.pdf (Accessed: 17 November 2019).
[7] Act of 6 November 2008 on Patient Rights and the Patient Ombudsman http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20090520417/T/D20090417L.pdf (Accessed: 17 November 2019).

Figure 1. Patient medical data collection



Key to Fig.1:
Medical Information System (SIM) is an ICT system for processing data that concerns healthcare services that are being, have been and are going to be provided, and are shared by IT systems of service providers.
Patient Online Account (IKP) – is an electronic application where every patient can log in in order to have a free access to their medical records, historic prescriptions and other data.
Integrated Patient Registry (ZIP) – a national service that shares with registered patients the history of the provided healthcare services and their financing that was stored by the National Health Fund since 2008
Medical Services Register of National Health Fund (RUM NFZ) – an ICT system to process the information on healthcare services financed from public funds that were provided and are planned to be provided as well as to account the services.

Source: Author's research based on: Act of 28 April 2011 on healthcare information system, , http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20111130657/U/D20110657Lj.pdf (Accessed:17 November 2019), *O IKP - Internetowe Konto Pacjenta*, https://pacjent.gov.pl/ikp (Accessed:17 November 2019), *ZIP*, https://zip.nfz.gov.pl/ap-portal/user/menu/open@info?view=001 (Accessed:17 November 2019), Act of 28 April 2011 on healthcare information system (Journal of Laws, 2019.0.408, Art.10), https://www.lexlege.pl/ustawa-o-systemie-informacji-w-ochronie-zdrowia/ (Accessed:17 November 2019).

The issue of patient medical data processing without a consent was regulated by GDPR (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)[8]. The data of service recipients (patients) can be processed without their consent when it is justified by the protection of their

[8] 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) https://giodo.gov.pl/234/id_art/9276/j/pl (Accessed: 17 November 2019).

other fundamental rights or for the purposes other than medical. Table 1 presents situations where patient medical data processing is possible without consent of data subject.

Table 1. Catalogue of situations where healthcare data processing without consent of data subject is lawful

Patient health-related purposes	
Category	**Example**
Health prevention	- Invitations to screening programmes and innoculations - Dissemination of educational materials
Employment medicine	- Work capability assessment – preliminary, periodical medical examinations and check-ups
Medical diagnosis and treatment	- Provision of healthcare services (diagnostic and therapeutic)
Provision of healthcare	- Patient registration in healthcare entitites; - Healthcare service management: confirmation and cancelation of appointments
Social protection	- Issue of medical certificates; - Tasks of certifying doctors
Patient nonhealth-related purposes	
Category	**Example**
Public health	- Protection against cross-border health threat - Provision of healthcare quality and security standards
Public interest	- Scientific or historical research - Statistics
Protection of person's vital interests	- Monitoring epidemics
Legal obligations	- Job recruitment

Source: Authors' research based on: Act of 29 August 1997 on personal data protection and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) https://giodo.gov.pl/234/id_art/9276/j/pl (Accessed: 17 November 2019).

2. Increasing the autonomy of data user

GDPR includes regulations which give data subjects the right to delete their data, including the right to be forgotten. Data subjects whose data are processed may require the data controller to erase their data and the controller[9] is obliged to delete the indicated data without undue delay.

When the controller has made the personal data public and is obliged to erase it (and there are no reasons that the request should be rejected), the controller – taking into account the available technology and the cost of implementation - should take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data

[9] GDPR, Art.4, item 7, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-4-definicje (Accessed: 17 November 2019).

subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data[10].

The controller is also obliged to provide adequate organizational and technical means that are necessary for a complete erasure of data of the data subject that exercises the right to be forgotten. All personal data must be erased from all locations such as mailboxes, discs, paper copies, text files, spreadsheets, backup copies and event logs. Table 2 presents cases where data controllers are obliged to erase personal data or may not comply with this obligation.

Table 2. Circumstances under which erasure obligation applies or does not apply

Data erasure obligation under the right to be forgotten	Exemptions to the right to be forgotten
Personal data are no longer necessary in relation to the purposes for which they were collected	Data processing is required by EU or national law
The data subject withdraws consent for data processing	Processing is necessary to establish, exercise or defend legal claims
The data subject objects to data processing	Archiving purposes in the public interest
The personal data have been unlawfully processed	Exercising the right of freedom of expression and information
The personal data have to be erased for compliance with a legal obligation	Exercising scientific or historical research purposes

Source: Authors' research based on: Act of 29 August 1997 on personal data protection; 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): https://giodo.gov.pl/234/id_art/9276/j/pl (Accessed: 17 November 2019).

Another patient's right that was introduced by GDPR is the right to data portability. Pursuant to the regulations, the data subject has the right[11]:

- to receive their personal data in a readable format and to transmit it to another controller;
- to have the personal data transmitted directly from one controller's IT systems to another, where technically feasible.

The above right applies to personal data that was provided to the controller based on consent or agreement and the processing is carried out by automated means. However, the right of data portability does not apply to the so called derived and inferred data such as algorithmic

[10] 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) https://giodo.gov.pl/234/id_art/9276/j/pl (Accessed: 17 November 2019)

[11] 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) https://giodo.gov.pl/234/id_art/9276/j/pl (Accessed: 17 November 2019).

results that are obtained by the controller through the analysis of personal data. In other words, these are the data that are developed by a physician after the analysis of patient's personal data that was obtained by a healthcare entity from the patient.

Conclusions

IT and organizational solutions that were discussed above result in an effective provision to patients of their health data and the opportunity of free decision as regards sharing the information with other actors. The development of patient's electronic portal is a substantial step in this direction. The characteristics of the portal is presented in the next article.

Bibliography

[1] GDPR, Art.4, item 7, https://gdpr.pl/baza-wiedzy/akty-prawne/interaktywny-tekst-gdpr/artykul-4-definicje.
[2] *O IKP - Internetowe Konto Pacjenta*, https://pacjent.gov.pl/ikp.
[3] Draft regulation of the Minister of Health of 10 November 2019 on the types, scope and templates of medical records and methods of their processing, https://legislacja.rcl.gov.pl/projekt/12326010/katalog/12634203#12634203.
[4] Regulation of the Minister of Health of 29 July 2010 on the types of medical records in occupational medicine service, the methods of keeping and storing the records and on the document templates, Journal of Laws 2010, No.149, item 1002. http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20101491002/O/D20101002.pdf.
[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), https://giodo.gov.pl/234/id_art/9276/j/pl
[6] Act of 6 November 2008 on patient Rights and the Patient Ombudsman, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20090520417/T/D20090417L.pdf.
[7] Act of 28 April 2011 on healthcare information system, http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20111130657/U/D20110657Lj.pdf
[8] Act of 28 April 2011 on healthcare information system, (Journal of Laws 2019.0.408, Art.10), https://www.lexlege.pl/ustawa-o-systemie-informacji-w-ochronie-zdrowia/
[9] *ZIP*, https://zip.nfz.gov.pl/ap-portal/user/menu/open@info?view=001.

Abstract

Electronic medical records documentation became a fundamental application to store health data that is processed by medical IT in health care entities in Poland. Its implementation and the adaptation of the IT solutions that are used in particular entities require a set of activities

that involve changes in the current IT structure and the development of an architecture that is functional with regard to the new information processing processes that apply modern IT solutions. The article discusses key legal, regulatory as well as technical and organizational aspects to these issues.