Dr Artur Romaszewski
Department of Medical IT systems, Institute of Public Health, Jagiellonian University Medical College in Krakow
artur.romaszewski@uj.edu.pl

Mariusz Kielar
Department of Medical IT systems, Faculty of Health Science, Jagiellonian University Medical College in Krakow
mariusz.kielar@uj.edu.pl

Dr Wojciech Trąbka
Department of Bioinformatics and Public Health, Faculty of Medicine and Health Science, Krakow Andrzej Frycz Modrzewski University
wojciech.trabka@uj.edu.pl

Krzysztof Gajda
Department of Medical IT systems, Faculty of Health Science, Jagiellonian University Medical College in Krakow
krzysztof.gajda@uj.edu.pl

NEW GDPR-RELATED PATIENT RIGHTS IN THE ACTIVITIES OF HEALTHCARE ENTITIES

Introduction

The 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) [1], below referred to as GDPR, granted several rights to data subjects irrespectively of the fact whether the processing is conducted pursuant to legal regulations, a consent or a contract. This is due to the fact that some of the rights are common to all persons whose data are processed. In the cases of processing that is based on consent, the catalogue of rights is wider (see Figure 1).

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A32016R0679 (accessed: 06.2018).

1. New rights in GDPR

A patient whose data is processed in relation to a visit to a medical service entity has several rights that are provided by the regulations that are in force in healthcare, as well as GDPR, with regard to the permissions to their data. As a patient, the data subject is granted the right to health information and the access to medical documentation. As a person whose data is processed, the data subject has defined rights resulting from the regulations on data protection. The rights to access one's own data and to rectify it are known from the previous regulation. They concern personal data that is processed both on the basis of legal regulations, consent or contracts.

However, some new rights emerged and their implementation involves adequate preparation. This concerns particularly the right to data portability, to be forgotten and to restriction of processing. The eligibility to these rights depends on the fact whether the data is processed under consent or a legal regulation. The execution of the above rights is possible only when data processing is conducted by a healthcare entity under consent. A catalogue of patient rights with regard to data processing under GDPR is given below in Figure 1.

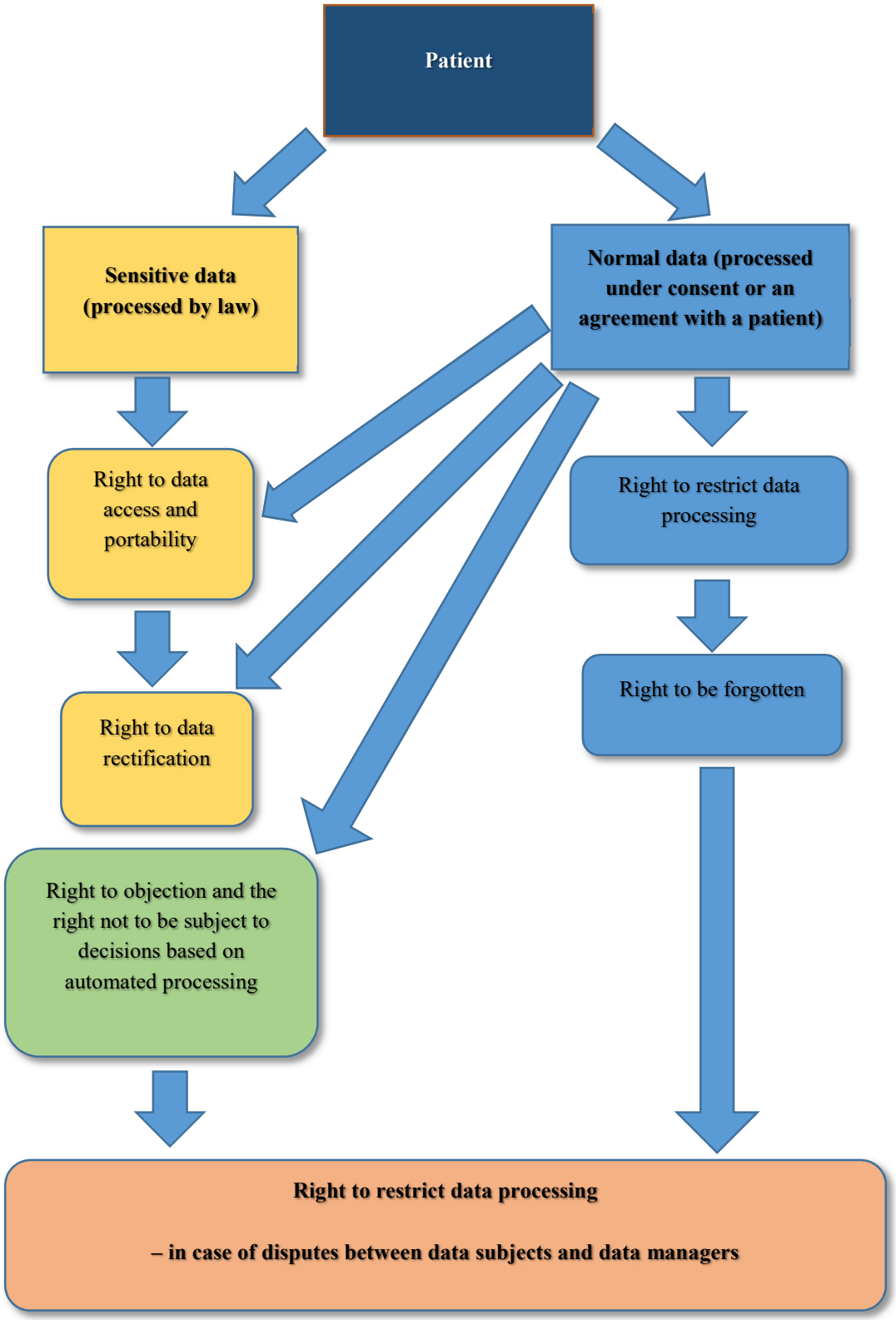
The consent to process patient data is required in the following cases:

- marketing purposes,
- clinical research,
- other research purposes,
- automated individual decision-making,
- transfer of personal data to third countries unless there is a different legal basis for the data manager to process patient personal data under GDPR.

There is no necessity to obtain patient consent when the processing is indispensable for the purposes of health prevention or occupational medicine, work ability assessment, medical diagnosis, the assurance of healthcare or social insurance, treatment, healthcare system and services management or social security on the basis of EU or member-state law or pursuant to a contract with a healthcare professional and subject to the GDPR-based conditions and safeguards[2].

[2] A. Plichta, *RODO: Czy zgoda pacjenta na przetwarzanie danych musi być na piśmie?,* https://www.zdrowie.abc.com.pl/artykuly/rodo-czy-zgoda-pacjenta-na-przetwarzanie-danych-musi-byc-na-pismie,119293.html (data dostępu: 06.2018).

Figure 1. GDPR- based catalogue of patient rights with regard to data processing



Source: Author's research.

2. Implementation of the right to information in healthcare entities

The right that will obviously be difficult to implement in health care is the right to information. Data subject should have the right of access to the collected personal data that concern them, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data[3].

Information obligation can be fulfilled in an electronic form, e.g. through a website[4]. This should concern particularly the cases when a significant number of actors and technological complexity make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected. When the data have been obtained from a source different than the data subject, the data subject should be informed about it at the latest within one month[5]. If the personal data are to be used for communication with the data subject, the obligation should be fulfilled the latest at the time of the first communication to that data subject[6]. The information obligation is required when the purpose of processing has been changed. The data subject should be informed about it prior to further processing[7].

It is not necessary to inform the data subject (irrespectively of the information source) when he or she already has the information[8]. The information obligation does not apply when:

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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), Recital 63
[4] GDPR, Recital 58
[5] GDPR Art. 14 item 3 (a) and Preamble Recital 61
[6] GDPR Art. 14 item 3 (b)
[7] GDPR Art. 13 item 4 and Art 14 item 5 (a)
[8] GDPR Art. 13 item 3 and Art. 14 item 4.

- the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as this obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing[9];
- obtaining or disclosure is expressly laid down by EU or member-state law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests[10];
- personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or member-state law, including a statutory obligation of secrecy[11].

The assurance of rights frequently involves several organization and technical operations. From among the rights of healthcare beneficiaries, significant problems involve the assurance of the right to information. Healthcare is the area where the fulfilment of this obligation is extremely complicated. This is because a question arises how to fulfil the information obligation to the millions of healthcare beneficiaries. Every person whose data are in the database should be appropriately informed both about the fact that their data is processed and about the resulting rights.

Some entities are exempt from the information obligation under legal regulations; for example

- the regulations allow ZUS (the Polish Social Insurance Institution) not to inform the persons whose data was obtained with reference to the insurance application and the payment of contributions (including healthcare providers, ZUS and the KRUS Agricultural Social Insurance Fund) about every case of data processing if personal data was obtained from sources other than data subjects. The exemption from the obligation to inform people whose data are processed by ZUS is possible insofar the national regulations that were issued pursuant to Regulation 2016/679, Art. 23 provide for it and the data processing is in the public interest with regard to public health and social security;
- the information obligation that was imposed on entities running medical registries[12] and processing data was removed. The entities, i.e. healthcare units that run medical

[9] GDPR Art. 15 item 5 (b).
[10] GDPR Art. 15 item 5 (c).
[11] GDPR Art. 15 item 5 (d).
[12] Act of 28 April 2011 on the information system in healthcare, Journal of Laws 2011 No. 113 item 657.

registries, contain frequently tens of thousands or more of personal data and are not able to inform data subjects about the processing of their data in the registries. This is because they do not possess updated addresses of the patients and the costs of such operation – with databases having as many as hundreds of thousands of records – would be disproportionate to potential benefits.

3. Medical data transfer and archiving

Patient records are both paper- and computer-based. Until quite recently, this differentiation was significant as regards their protection. The paper-based data were protected only when they were a part of files, records, etc. Currently, the differentiation is crucial mainly as regards the execution of some rights. The right to data transfer applies only to electronic files.

In the case of records that include medical data, paper-based documentation will be used until the statutory retention periods expire. Then, the records will be destroyed or transferred to an authorized person[13].

The scope of the records is regulated by law. As regards medical records and other patient data files, legal basis for the records can be indicated. Moreover, the regulations that concern other areas indicate precisely what data can be stored. For example, the Labour Code defines in detail the scope of employee data that can be stored by the employer. In comparison to the previous regulations, the scope has been restricted, e.g. - among other things - it does not include the employee's address or the parents' names[14].

Due to the fact that the personal data controller (PDC) is responsible for the implementation of the GDPR principles, including the storage limitation principle, a continuous monitoring of paper-based documentation is the obligation that requires systematic work. The procedure is more convenient with electronic files where systems automatically indicate the records whose retention periods is close to expiry. Also documents other than patient records are subject to reviewing, shredding[15] and archiving. Pursuant to the Act on National Archives

[13] Introduced in 2008 to the Act on patient rights.
[14] Draft Act of 12 September 2017, Art. 5.
https://legislacja.rcl.gov.pl/docs//2/12302951/12457706/12457707/dokument308373.pdf (accessed: 06.2018).
[15] Shredding/Destroying non-archival documents is the selection for destruction of this part of non-archival records whose retention period (as defined in a consolidated list of files or a documentation qualifier that are mentioned in the Archival Act, Art.6 item 2 (2) expired or when an entity or organizational unit decided that the non-archival documentation is no more of value for them (including their probative value) - Brakowanie

Resources and Archives, the documents that constitute archival material are transferred after 25 years of their creation to a relevant state archive unless the entity or organizational unit had transferred the archival materials earlier to the state archive (applicable to paper-based documents) [16]. Electronic documents that are qualified as archival material are subject to archiving and must be transferred to a relevant archive within 10 years of their creation (however, there are derogations from this rule) [17]. It should be pointed out here that there are provisions that regulate the procedures for the preparation of archival documentation to be transferred to a relevant archive.

Healthcare is a system which applies both the regulations of general law and lex specialis that concern proceedings with patient health data. The GDPR and Polish regulations on medical data transfer are a good example. For example, when a contract is signed between a healthcare service provider and an employee who is responsible for the assurance of medical tests for the employees and job applicants, apart from the main agreement, an employee data entrustment agreement is made. In the cases when the employer changes the service provider, he/she can apply for the transfer of the data to the new service provider. However, the personal data of employees who were subject to periodic medical examinations and whose medical documentation was established is to be processed for 20 years by the entity that originally obtained the data[18].

It can be concluded from the above example that a healthcare entity will frequently act as a personal data controller despite the fact that initially (before the patient's visit) it obtained the personal data as a processor. This is due to the fact that depending on their roles, the entities (their data controllers), although they will be obliged to follow the principle of the scope of data processing, will practically have to complete more tasks: for example when keeping various documents (e.g. the records of processing activities or processing categories) or the ones that are related to their obligations to data subjects. One of the key issues that a data controller in healthcare entity has to face when preparing a data processing model is the organization of data

dokumentacji niearchiwalnej w archiwum zakładowym (składnicy akt) –*Archiwum Narodowe w Krakowie*, http://www.ank.gov.pl/nadzor-a .ive rchiwalny/glowne-zadania-nadzoru-archiwalnego/brakowanie-dokumentacji-niearchiwalnej-w-archi (accessed: 06.2018).

[16] Act of 14 July 1983 on National Archives Resources and Archives, Art. 5; Journal of Laws 1983, No. 38 item 173

[17] *Przekazywanie dokumentów elektronicznych do archiwum państwowego*. Archiwista 24, https://archiwista24.wordpress.com/2014/07/03/przekazywanie-dokumentow-elektronicznych-do-archiwum-panstwowego/ (accessed: 06.2018).

[18] Ordinance of the Minister of Health of 29 July 2010 concerning the types of medical documentation used by occupational medical service, the way it is kept and stored and the templates of documents used, par. 21.1, Journal of Laws, 2010, No. 149 item 1002

with respect to the legal basis for the processing. Generally, data in healthcare entities are processed when, among other cases:

- the processing is stipulated law,
- the processing is justified by health objectives that are related to healthcare service management,
- the processing is necessary for reasons of public interest in the area of public health,
- the (potential) patient has given consent[19].

4. Sensitive data processing

The prohibition of processing sensitive data is not absolute. This means that there are cases where the processing is possible.

GDPR is a regulation that authorizes entities to process health data. This is important as the processing of sensitive data, including the data on health, genetic code, sexuality or sexual orientation, is generally banned.

Pursuant to GDPR, sensitive data on health can be processed for the purposes of health prevention, occupational medicine (to assess an employee's ability to work), treatment, health care system and services management or social security assurance under EU or member-state law or pursuant to a contract with a healthcare professional.

Processing is also possible when necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare and of medicinal products or medical devices, on the basis of EU or member-state law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

The division of persona data to general and sensitive data is crucial as regards the assurance of appropriate measures and methods of securing data in the course of their processing (including sanctions or the appointment of controllers). The data that are processed under consent include general data and sensitive data. One should keep in mind that health care – as it was mentioned above – has a very specific quality. This concerns the purpose of health data processing. When an individual is subject to some examination or an experiment he/she becomes a patient. Some of the data concerning the individual will be used to describe the examination itself; it will become a part of medical documentation and for a defined period of

[19] GDPR, Article 9

time will be subject to lex specialis while some of it may be used for a different reason, for example for marketing purposes. The data sets for such purposes are developed under a consent or agreement that involves informing the patient about, for example, new treatment methods or drugs.

There are cases when a patient sells or transfers his/her health data to business entities that analyze data. Then, the processor that acquires this data for commercial or scientific research purposes is obliged to comply with the GDPR regulations on data transfer or erasure. It is important to note that these regulations do not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. However, it applies to controllers or processors that provide means for processing personal data for such personal or household activities[20]. (e.g. they share the software in the cloud which enables the retention and processing of health data). This provision expressly excludes situations in which health data was acquired by providing ” free” space for data on cloud platforms.

5. Secrecy and data protection

Secret is a message defined by law whose recognition or disclosure is forbidden by law[21]. Healthcare is the operation area of individuals that are subject to various kinds of secrets. The purpose is to ensure the security of patient data that is processed in healthcare entities. It is the right of the patient that medical professionals, including the ones that provide healthcare services, keep patient data secret. The secrets are regulated by provisions of law that apply to medical professionals, i.e. physicians, dentists, nurses and midwives, diagnosticians, physiotherapists, chemists, feldshers and psychologists[22].

The secrecy also applies to data and information that is included in medical documentation. The following persons are authorized to process the data in medical documentation for healthcare purposes, to provide and manage healthcare services, to keep IT system in which medical documentation is processed and to ensure the security of the system:

1) medical professionals;

[20] GDPR, Recital 18.
[21] *Słownik PWN*, https://sjp.pwn.pl/slowniki/tajemnica.html (accessed: 06.2018).
[22] physician and dentist – Act of 5 December 1996 on professions of doctor and dentist, Art. 40; nurse and midwife – Act of 15 July 2011 on professions of nurse and midwife, Art. 17; Act of 20 July 1950 on the profession of feldsher, Art. 7; laboratory diagnostician – Act of 27 July 2001 on laboratory diagnostics, Art. 29; pharmacist – Act of 19 April 1991 on Pharmaceutical Chambers, Art. 21 item 2; psychologist – Act of 8 June 2001 on the profession of psychologist and professional self-government of psychologists, Art 14.

2) other healthcare support workers who perform, apart from healthcare services, tasks related to the maintenance and security assurance of IT systems in which medical documentation is processed when authorized by data controllers. The professionals in question are obliged to secrecy also after the patient's death.

Thus, apart from medical professionals, some other persons are also allowed to process data; this, however requires a consent of a data controller. It is one of the security requirements that the access to personal data should be given solely to natural persons that operate under the authorization of a controller of processor.

6. Access to medical documentation

With regard to the access to patient medical documentation in entities that employ numerous persons subject to the obligation of professional secrecy, a practical problem may emerge in the case of persons who provide services to "their own patients". When the access concerns the patients who are registered in an entity that employs several doctors (specialists), the documentation is completed by various people and there is no problem with the access for all service providers in the entity. However, the situation is different as regards the access to data that is included in the documentation of a healthcare entity other than the one that employs the doctor or other service provider. In such cases, the access has to be justified either by therapeutic reasons or obligations that are not connected with the treatment, e.g. the analysis that is conducted by an authorized worker with regard to the legal requirements of the documentation. The authorization must be granted from a data controller. This is also the case when someone – as a part of their job (e.g. presidents for medical affairs in healthcare entities) – needs the access to other patients' data). The authorization is also necessary in the case of the access to data on persons who provide healthcare service, e.g. for the heads of entities that employ or have civil law contracts with healthcare providers.

When health data is transferred to external entities, the entity that obtains the data is obliged to secrecy. Both the GDPR provisions and acts on patient rights regulate the issue of secrecy on the part of persons responsible for processing under a contract with the data controller.

The processor processes personal data only when requested in writing by a data controller. Apart from other requirements that are provided by the provisions, the processor makes sure that persons authorized to process personal data are committed to secrecy or are subject to

appropriate statutory obligation to secrecy. Healthcare provider may outsource data processing to a data processor under a contract. The contract should comply with the GDPR regulations[23].

Pursuant to the Act of 28 April 2011 on information system in health care [24] the entities that specialize in the provision of IT technical support in the cases of health data transfer (including all system modules and registries) are committed to secrecy. The secrecy applies to the information on service beneficiaries that is obtained as a result of the entrustment of data processing in the systems. The entities in question are obliged to secrecy also after the beneficiary's death.

Until recently, the concept of the so called digital secrecy[25] was used – the persons that were authorized to process data were obliged to keep secret the data and their security tools.

At present, pursuant to GDPR, personal data should be processed in a way that ensures adequate security and confidentiality. Persons that are authorized to process the data are obliged to maintain confidentiality even if they have not made an appropriate statement as this obligation results directly from GDPR. Every person that acts under the authority of a controller or processor and has the access to personal data is allowed to process it solely by the order of the data controller[26].

The issue of the employee's obligation to confidentiality is regulated by the Labour Code. An employee is obliged to keep confidential any information that could cause damage to the employer if disclosed[27]. The obligation is formulated in a fairly general way but it is assumed that it applies to the information that is accessible to the employee and its disclosure could result in, even potential, damage to the employer. The secrecy binds the employee from the moment of signing the labour contract and it is not necessary for the employer to undertake any additional measures (such as confidentiality agreements) with regard to this issue. However, this does not mean that the parties of the contract of employment cannot make such an agreement. It is in the interest of the employer that the employee should know what particular data and information are crucial to the employer to the extent that their disclosure could cause a damage. Consequently, the employer should indicate (e.g. in the contract of agreement or in

[23] GDPR, Art. 24, item 4.
[24] Act of 28 April 2011 on information system in health care, Journal of Laws 2011, No.113 item 657.
[25] The repealed Act of 20 August 1997 on personal data protection, Art. 39, item 2.
[26] A. Kręcisz-Sarna, *Oświadczenia o zachowaniu danych osobowych w tajemnicy – czy aktualizować je w związku z RODO*?, https://www.poradyodo.pl/administracja-publiczna/oswiadczenia-o-zachowaniu-danych-osobowych-w-tajemnicy-czy-aktualizowac-je-w-zwiazku-z-rodo-8332.html# (accessed: 06.2018).
[27] Labour Code, Art. 100, par. 2 item 4.

work regulations) the type (scope) of information that should not be disclosed[28]. Thus, the employer should be informed that the security measures taken by the company are crucial to the employer and their disclosure could lead to a damage.

Because of the expiry of the regulation that made it possible to commit all authorized processors in an entity to secrecy and also to maintain the confidentiality of the security measures and technical solutions, it is possible now to refer to business secret.

Conclusions

GDPR granted several rights to every data subject. The rights to access one's own data and to rectify it are known from the previous regulation. They concern personal data that is processed both on the basis of legal regulations, consent or contracts. However, some new rights emerged and their implementation involves appropriate preparation. This concerns particularly the right to data portability, to be forgotten and to restriction of processing.

From among the rights of healthcare beneficiaries, significant problems concern the assurance of the right to information. Healthcare is the area where the fulfilment of this obligation is extremely complicated. This is because a question arises how to fulfil the information obligation to the millions of healthcare beneficiaries. Every person whose data are in the database should be appropriately informed both about the fact that their data is processed and the resulting rights.

The GDPR regulations on sensitive data processing are extremely important to the healthcare system. The processing of sensitive data, including the data on health, genetic code, sexuality or sexual orientation, is generally prohibited. Pursuant to GDPR, sensitive data on health can be processed under specific conditions, for example when it is necessary for the purposes of health prevention, occupational medicine, the assessment of an employee's ability to work, medical diagnosis, the provision of health care and social security assurance, treatment and healthcare system and services management.

[28] M. Szuszczyński, *Jak zobowiązać pracownika do zachowania poufności?*, Biuletyn Prawo Pracy i HR, https://www.bdo.pl/pl-pl/publikacje/biuletyn-prawo-pracy-i-hr/2017/jak-zobowiazac-pracownika-do-zachowania-poufnosci (accessed: 06.2018).

Bibliography

[1] *Archiwum Narodowe w Krakowie*, http://www.ank.gov.pl/nadzor-archiwalny/glowne-zadania-nadzoru-archiwalnego/brakowanie-dokumentacji-niearchiwalnej-w-archi
[2] Kręcisz-Sarna A., *Oświadczenia o zachowaniu danych osobowych w tajemnicy – czy aktualizować je w związku z RODO*?, https://www.poradyodo.pl/administracja-publiczna/oswiadczenia-o-zachowaniu-danych-osobowych-w-tajemnicy-czy-aktualizowac-je-w-zwiazku-z-rodo-8332.html#
[3] Plichta A., *RODO: Czy zgoda pacjenta na przetwarzanie danych musi być na piśmie?*, https://www.zdrowie.abc.com.pl/artykuly/rodo-czy-zgoda-pacjenta-na-przetwarzanie-danych-musi-byc-na-pismie,119293.html
[4] Draft act of 12 September 2017 on personal data protection (Provisions introducing the act on personal data protection, https://legislacja.rcl.gov.pl/docs//2/12302951/12457706/12457707/dokument308373.pdf
[5] Ordinance of the Minister of Health of 29 July 2010 concerning the types of medical documentation used by occupational medical service, the way it is kept and stored and the templates of documents used, Journal of Laws, 2010, No. 149 item 1002
[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016on 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, GDPR)
[7] *Słownik PWN*, https://sjp.pwn.pl/slowniki/tajemnica.html
[8] Szuszczyński M., *Jak zobowiązać pracownika do zachowania poufności?*, Biuletyn Prawo Pracy i HR, https://www.bdo.pl/pl-pl/publikacje/biuletyn-prawo-pracy-i-hr/2017/jak-zobowiazac-pracownika-do-zachowania-poufnosci
[9] Act of 14 July 1983 on National Archives Resources and Archives, Journal of Laws 1983, No. 38 item 173
[10] Act of 26 June 1974, Labour Code, Journal of Laws 1974, No.24 item 141
[11] Act of 28 April 2011 on information system in health care, Journal of Laws 2011, No.113 item 657
[12] *Przekazywanie dokumentów elektronicznych do archiwum państwowego*, Archiwista 24, https://archiwista24.wordpress.com/2014/07/03/przekazywanie-dokumentow-elektronicznych-do-archiwum-panstwowego/

Abstract

The patient whose data is processed in relation to a visit to a medical service entity, has several rights that are guaranteed by the regulations that are in force in healthcare, as well as GDPR, with regard to the permissions to their data.

The rights to access one's own data and to rectify it are known from the previous regulation. They concern personal data that is processed both on the basis of legal regulations, consent or contracts. However, some new rights emerged and their implementation involves

preparation. This concerns particularly the right to data portability, to be forgotten and to restriction of processing.

From among the rights of healthcare beneficiaries, significant problems concern the assurance of the right to information. Healthcare is the area where the fulfilment of this obligation is extremely complicated.

The GDPR regulations on sensitive data processing are extremely important to the healthcare system. The processing of sensitive data, including the data on health, genetic code, sexuality or sexual orientation, is generally prohibited.

Pursuant to GDPR, sensitive data on health can be processed for the purposes of health prevention, occupational medicine, the assessment of an employee's ability to work, medical diagnosis, the provision of health care and social security assurance, treatment and healthcare system and services management.

Key words

GDPR, catalogue of the rights of data subjects, sensitive data, medical documentation, professional secrecy