Dr Artur Romaszewski
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems
Dr hab. Wojciech Trąbka
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems

Protection of personal data in health care entities and IT systems – the impact of new, national and EU legal regulations

Introduction

The security and confidentiality of personal data that is processed in the health care system is one of the most significant responsibilitries faced by health service in the time of comprehensive digitization.

In health care systems mainly data concerning patients' health are processed. Thus, their security and confidentiality must be ensured with the respect to patient's rights, including the right to the access to medical records. Health data are processed both with and without the agreement of the data subject. The latter case results from legal provisions that authorize several institutions to process health data. Such a situation is justified by public interest. That is the case with several data concerning the health condition of population[1] which make it possible to analyze morbidities and disabilities, the factors that influence health condition, the needs concerning health care, health care resources, services offered and their availability, the expenditure on health care and the methods of its financing, and the causes of deaths.

Issues related to new technologies

[1] *public health* should be interpreted in line with the definition given in the Regulation (EC) No. 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work,

As a result of technological development, the new computing capacities and cyberspace offer a whole range of services related to data processing, including data concerning health that are generated and managed by commercial entities which are not entitled directly to process them. The problem is associated with cloud computing. The processing may occur only after an agreement concerning personal data processing has been signed. The agreement of that type leads to several problems that are mainly related with data security and with the monitoring of the data flow between the delegating party and the recipient of the tasks, which is often established out of the EU borders.

It is worth mentioning that there is also a problem of personal data (which include data concerning health) that are processed in the scope that is considered appropriate by individuals that the data refer to. Some patients started processing their data in the cloud[2]. Under the current provisions of law, such data are not protected. The draft Regulation of EU, which is analyzed below, takes a different approach. It adopts the principle that the regulations will not apply to processing conducted by individuals as regards personal, family or domestic data such as private correspondence, the holding of addresses or a private sale that have no connection with a professional or commercial activity. However, the Regulation will apply to controllers and entities that provide the opportunities to process personal data for the needs of such personal or domestic activities[3]. That refers – for example – to cloud computing, which provides the measures for individuals to store their health data. So far, such data have not been protected.

It should be pointed out that along with the advancing digitization there is a change of the basic medical data carrier, i.e. paper files, into electronic databases where health data of patients are stored. The visualization and integration of the data is conducted only when necessary. In other words, complex medical records are generated from the resources stored frequently in the data bases belonging to different entities only if desired. That process will cause substantial changes in health data processing

[2] See more in: Zeszyty Naukowe No.33, A.Romaszewski, W. Trąbka Legal Issues of Data Processing by Cloud Computing, Procedures of Medical Data Processing by Cloud Computing.

[3] Amendment 2, Proposal for a regulation , Recital 15 - European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

The need for new legal regulations

Law must face the presented above challenges that are involved with the global change in information processing. Both Polish and European legal regulations on the protection of personal data were formed many years ago, when most of the problems mentioned above were nonexistent. In EU for years there has been in force the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[4] while in Poland there has been the Act of 29 August 1997 on personal data protection[5], which was largely based on the assumptions of the Directive. The Directive includes basic terms that refer to personal data protection and it defines the principles of personal data collection, storage and sharing. The assumptions of the Directive were implemented by EU member-states to their legal systems as it was done in the case of the Polish act on personal data protection[6]. The fact that EU member-states implemented the provisions of the Directive in their own ways resulted in the diversification of regulations regarding personal data in their legal systems. Thus, a decision was made to change the situation and to adopt one legal act that would regulate comprehensively the issues of personal data protection in the whole area of EU and eliminate the differences resulting from adjusting the legal form of the Directive to national legal systems. In 2012, a draft was prepared of the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data[7] - referred to as General Data Protection Regulation). Regulation[8] is a legislative act that applies directly to the member-states. Thus Sejm, the Polish Parliament, will not have to adopt any additional acts – the new law will bind directly the entities which process the data.

There were two objectives of the project:

- to strengthen the right to privacy on the Internet,
- to give the momentum to the development of digitalization in Europe.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[5] Dz.U. (Journal of Laws) 1997, No. 133, item 883

[6] Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2014, No. 1182, item 883

[7] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

[8] http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm

The accepted principle is: One continent, one law – that is how the European Commission advertises the new rules in a press release that accompanies the draft regulation[9].

The assumption was that European companies could not follow standards that are more rigorous than those of their competitors that have their head offices out of the EU borders but are engaged in an economic activity within the EU. In order to meet this assumption, a unified regulation was provided for the protection of data within EU institutions and bodies.

Figure 1 presents the most important issues concerning personal data protection that will be regulated in EU after the Regulation comes into force. The authors will make an attempt to discuss the ones that will have a significant impact on the health care area.

Separate articles will discuss the new responsibilities of database controllers and the issues related to the introduction of Information Security Controllers to health care institutions[10.]

[9]European Commission Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm

[10]A. Romaszewski W. Trąbka Administrator Bezpieczeństwa Informacji w podmiotach leczniczych w świetle ustawy o ochronie danych i Rozporządzenia Parlamentu Europejskiego I Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych

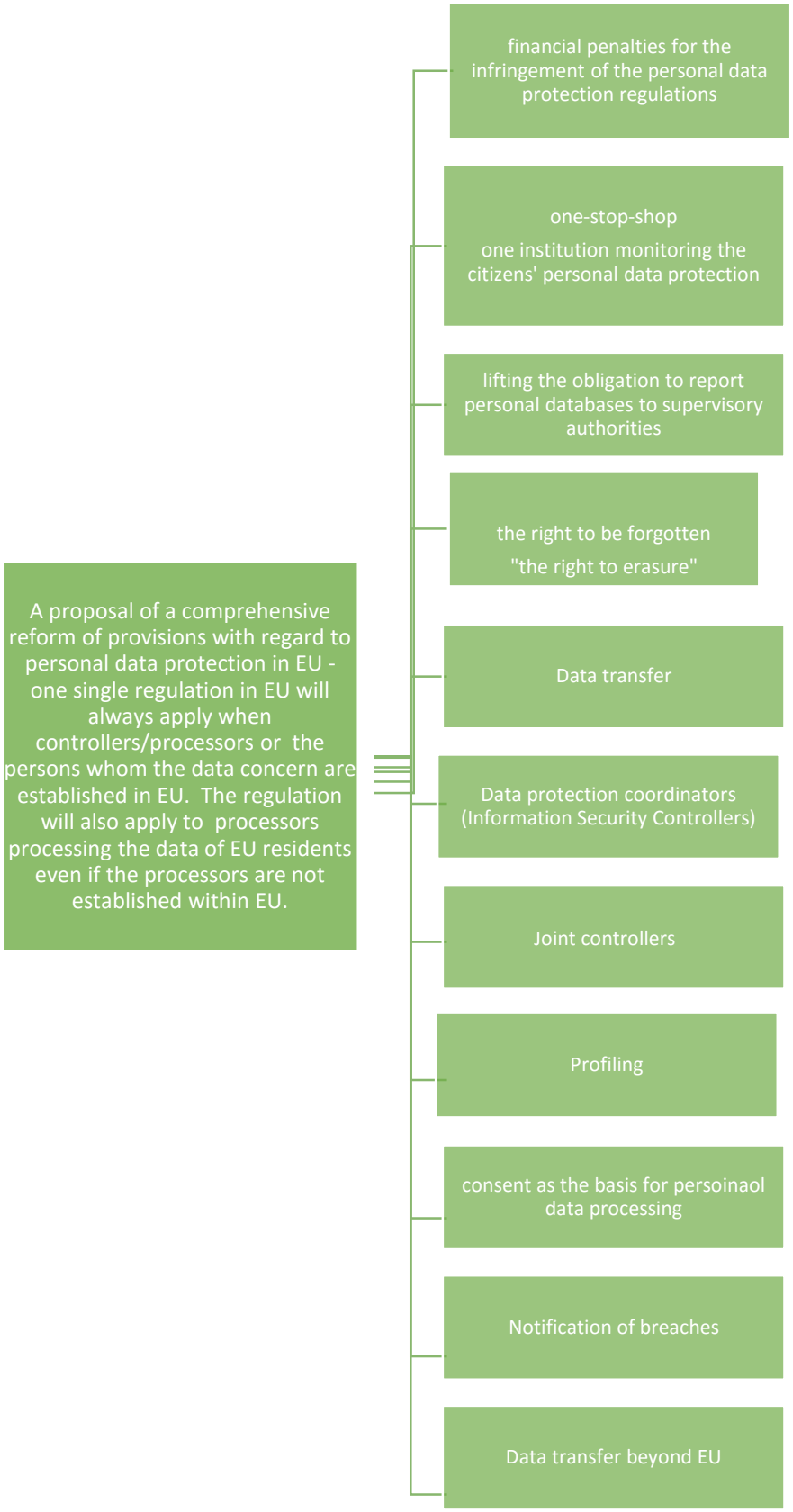

Figure 1. The most important issues related to personal data protection as regulated by the EU Regulation

Health care is a crucial aspect of the socio-economic life in every country. This is the area where a substantial amount of personal data is processed; the data do not concern only health care services but also the personal data of employees, service providers who work under civil contracts and the suppliers of materials and goods. Thus, some attention should be paid to the general aspects of the regulation. One should start here with the definition of personal data.

Personal data and data concerning health

The definition of personal data which is applied by the regulation is close to the one in the current Polish act on data protection. *Personal data* means any information related to an identified natural person or natural person who can be identified (data subject); *person who can be identified* is an individual whose identity can be determined directly or indirectly, particularly with the use of such identifying data as the name and the surname, identification number, place of residence , unique identifier or at least one factor specific to the physical, physiological, mental, economic, cultural , social and sexual identity of that person.

Thus, personal data are the data referring both to

- an identified natural person and
- and the data that can be applied to identify a natural person either directly or indirectly by measures reasonably likely to be used by a controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Natural persons can be identified when they use online services provided by their devices, applications, tools and protocols, such as Internet Protocol addresses or cookie identifiers. This may leave traces which, combined with unique identifiers and other information received by the servers, may be used to create profiles of the individuals and identify them. Consequently, it should be taken into consideration – separately for particular cases and with regard to the technological development – whether identification numbers, location data, online identifiers or other specific factors as such should be considered as personal data in all circumstances.

The Regulation provides the definitions of the following notions related to medical data:

- *data concerning health* mean any personal information which relates to the physical or mental health of an individual, or to the provision of health services to the individual;
- *genetic data* mean personal data, concerning the genetic characteristics of an individual which are inherited or acquired and can be inferred from sample bio-analyses, particularly from the chromosome, DNA or RNA analyses or the analysis of other elements that enable the acquisition of similar information;
- *pseudonymous data* mean personal data that cannot be attributed to a specific data subject without the use of additional information as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution;

The Regulation differentiated categories of data that are broadly applied in health care:

encrypted data mean personal data, which through technological protection measures are rendered unintelligible to any person who is not authorized to access it;

biometric data mean any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data[11];

Data concerning health belong to the group of the so called sensitive data and they should not be processed, unless the data subject gives his explicit consent. Derogating from the prohibition on processing such data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data of individuals they concern and in the cases when it is justified by public interest.

The Regulation defines the scope of personal data concerning health. It is important as the Polish law lacks that kind of definition (table 1)

[11] Amendment 98, Proposal for a regulation Article 4 - European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

Scope of personal data concerning health
• all data pertaining to the health of a data subject;
• information about the registration of the individual for the provision of health services;
• information about payments or eligibility for health care with respect to the individual;
• a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes ;
• any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples;
• identification of a person as provider of health care to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic[12.]

Table 1. The scope of personal data concerning health
Source: Authors' research based on the text of the Regulation

Conditions for processing personal data concerning health

Processing of personal data concerning health must be on the basis of Union law or Member State law which shall provide for suitable and specific measures to safeguard the data subject's legitimate interests, and be necessary for:

a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under member state law or rules established by national competent bodies; or

[12] Item 26 , Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

b) 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, inter alia for medicinal products or medical devices and when the data are processed by a person subject to the obligation of confidentiality; or

c) other reasons of public interest in areas such as social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance and health care systems .

The processing of personal data concerning health for the reasons of public interest should not imply the processing of personal data for other reasons unless the controller obtains the consent of the data subject or there is legitimate ground provided by Union law or the law of a member state.

In the cases when the above objectives can be obtained without the use of personal data, the data cannot be applied without the consent of the data subject or the law of a member state.

The principle was accepted that the processing of personal data concerning health necessary for historical, statistical and scientific purposes is acceptable solely under the consent of the data subject.

If the data subject's consent is required for processing medical data solely for public or scientific purposes, the consent may be granted for one or more particular and similar investigations. However, the data subject can withdraw the consent at any moment.

The regulations of member states can provide for the derogation from the obligation of the consent to process personal data for scientific purposes with regard to scientific research that is conducted for significant reasons of public interest and the research cannot be conducted otherwise.

If the data subject is required to grant the consent for processing medical data solely for public health purposes, he/she can have the opportunity to grant a general consent for epidemiological, translational or clinical purposes.

Personal data processed for scientific research purposes should be rendered anonymous or, if impossible, given an identifier with the application of the highest technical standards to prevent unwarranted re-identification of the data subjects. However, the data subject has always the right to withdraw the consent.

Personal data can be processed for historical, statistical and scientific research purposes only if:

- these purposes cannot be otherwise fulfilled by processing data which do not permit or not any longer permit the identification of the data subject;
- data enabling the attribution of information to an identified or identifiable data subject are kept separately from the other information under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects.[13]

The decision was also made that the Commission will be empowered to adopt delegated acts for the purpose of specifying other criteria of public interest in the area of public health[14].

General principles of personal data processing

Moreover,general principles of personal data processing were adopted. They are presented in table 2.

Principles of personal data processing[15]	
lawfulness, fairness and transparency uczciwość i przejrzystość	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject,
purpose limitation	collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes,
data minimization	adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the

[13] Amendment 194, proposal regarding resolution, Article 83, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

[14] The acts entered into force on 1 December 2009. Their aim was to supplement the provisions included in legislative acts (regulations, directives, decisions). Legislators are entitled to delegate to the European Commission the rights to detail or improve – which means decision making – some less significant elements of EU law or framework law. Delegated acts are superior to national acts and constitutions although they are adopted in an institution where not all member states are represented. http://pl.euabc.com/word/271 http://pl.euabc.com/word/271;
https://www.mir.gov.pl/rozwoj_regionalny/Polityka_regionalna/Documents/Akty_delegowane.pdf

[15] Amendment 99, proposal for resolution, Article 5, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

	purposes could not be fulfilled by processing information that does not involve personal data,
accuracy	accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay,
storage minimization	- kept in a form which permits *direct or indirect* identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, - stored for longer periods insofar as the data will be processed solely for historical, statistical or scientific research or for archive purposes and if a periodic review is carried out to assess the necessity to continue the storage, and if appropriate technical and organizational measures are put in place to limit access to the data only for these purposes,
effectiveness	processed in a way that effectively allows the data subject to exercise his or her rights,
integrity	processed in a way that protects against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures,
accountability	processed under the responsibility and liability of the controller, who shall ensure and be able to demonstrate the compliance with the provisions of this Regulation

Source: Authors' research based on the text of the Regulation

Table 2. Principles of personal data processing.

Processing of personal data is lawful only if at least one of the following conditions applies Amendment 100, proposal for resolution, Article 6, European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data

and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))

- ✓ the data subject has given consent to the processing of their personal data for one or more specific purposes;
- ✓ processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- ✓ processing is necessary for compliance with a legal obligation to which the controller is subject - that must be implied by the law of a particular member state;
- ✓ processing is necessary in order to protect the vital interests of the data subject;
- ✓ processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller - that must be implied by the law of a particular member state;
- ✓ processing is necessary for the purposes of the legitimate interests pursued by the controller.

The law of the Member State must meet an objective of public interest or must be necessary to protect the rights and freedoms of others, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued.

Within the limits of this Regulation, the law of the Member State may provide details of the lawfulness of processing, particularly as regards data controllers, the purpose of processing and purpose limitation, the nature of the data and the data subjects, processing measures and procedures, recipients, and the duration of storage.

Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

Bibliography

1. Regulation (EC) No. 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work,
2. Zeszyty Naukowe No 33 Wyższa Szkoła Zarządzania i Bankowości A. Romaszewski, W. Trąbka Legal Issues of Medical Data Processing by Cloud Computing, Procedures of Medical Data Processing in Cloud Computing,
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
4. Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
5. European Parliament legislative resolution of 12 March 2014 on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and the free movement of such data (general data protection regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
6. A.Romaszewski W. Trąbka, Administrator Bezpieczeństwa Informacji w podmiotach leczniczych w świetle ustawy o ochronie danych i Rozporządzenia Parlamentu Europejskiego I Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (Information Security Controller in health care entities in the light of the act on data protection and the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data)
7. Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883, EU website http://europa.eu/eu-law/decision-making/legal-acts/index_pl.htm
8. European Commission Memo http://europa.eu/rapid/press-release_MEMO-14-186_pl.htm
9. J.Bardadyn, Kiedy (ostatecznie!) i jak UE zreformuje prawo ochrony danych osobowych? http://blog-daneosobowe.pl/ue-ostatecznie-zreformuje-prawo-ochronie-danych-osobowych-beda-kluczowe-zalozenia/
10. M. Chmielecki, Unijna reforma przepisów o ochronie danych osobowych - informacje ogólne e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
11. M. Cwener, Propozycje zmian w zakresie przepisów dotyczących ochrony danych osobowych – cz. i; ii ogólne e-ochronadanych.pl http://www.e-ochronadanych.pl/regulamin.php
12. K. Szymielewicz, Półprzepuszczalny standard ochrony danych https://panoptykon.org/wiadomosc/polprzepuszczalny-standard-ochrony-danych
13. K.Witkowska, Reforma ochrony danych osobowych - nowe obowiązki, nowe korzyści https://www.portalodo.com/entry/reforma-ochrony-danych-osobowych-nowe-obowiazki-nowe-korzysci.
14. P. Wierzbicki, Jest szansa na unijne rozporządzenie o ochronie danych (2014.02.11) Obserwator Konstytucyjny http://www.obserwatorkonstytucyjny.pl/debaty/jest-szansa-na-unijne-

rozporzadzenie-o-ochronie-danych/

Abstract

In health care systems, mainly data concerning patients' health are processed. Their security and confidentiality must be ensured with the respect to patient's rights, including the right to the access to medical records. The implementation of new technologies, e-archives, teletransmissions, cloud computing and the globalization of the access to the data resulted in the necessity to introduce new legal regulations regarding personal data protection both on national and EU levels. The article presents the most crucial issues in the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The regulation, which introduces significant changes particularly as regards the protection of personal data (health data including) will come into force in EU countries in January 2016.