Dr Artur Romaszewski
Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems

Dr hab. med. Wojciech Trąbka

Jagiellonian University Medical College
Faculty of Health Sciences
Department of Medical Information Systems

PROCEDURES OF MEDICAL DATA PROCESSING IN CLOUD COMPUTING

The article presents procedures related to the transfer of data and information on healthcare services to the healthcare information system, as well as the functioning of databases, electronic medical documentation and medical registers.

Loading data and information into the system within the scope defned by law.

Law regulates the scope of data that is stored by entities providing medical services (treatment and diagnosing) – that refers both to databases, registers, medical electronic documentation and the SIM (Medical Information System) document. The law also defines the responsibilities of health service providers as regards sharing the acquired data and information on patients' health. The provisions of law identify the entities that are authorized to process health data and information that is included in medical records as well as oblige practically all medical service providers and pharmacies to inform continuously the system on the completed service (i.e. the completion of a medical service or prescription)

There are two separate systems that process health data and information:

1. **Medical information in healthcare** – the system acquires the data free of charge in compliance with the obligation of all health service providers in Poland (except for the entities rendering such services to imprisoned persons) to transfer the information. The SIM (Medical Information System), which operates within that system, is a teleinformatic system that processes data concerning the past, current and scheduled healthcare services and is shared by the teleinformatic systems of service providers and pharmacies. Those entities process the SIM electronic documents in the scope defined by the act. The sharing of the messages on the referrals that are issued and

completed and of the prescriptions and referrals in the form of an electronic document that enables patients to obtain a particle healthcare service is conducted on an ongoing basis, at least once a day.

Sending the SIM electronic documents consists in:

- developing the message with the SIM electronic documents by the entity obliged to send such information to the SIM,
- signing the message with the use of a secure electronic signature or a signature authorized by trusted ePUAP profile;
- sending the message by the entity obliged to send such information to the SIM,
- receiving the message, verifying and sending back either the confirmation of its reception or a list of errors or deficiencies to the adequate entity[1].

2. **RUM-NFZ** (Medical Services Registry of the National Health Fund) information system – the obligation of all entities that have contracts with the NFZ (service providers[2], pharmacies[3]). The service providers and pharmacies transfer the data in an electronic form to the entities that are obliged to finance services from public means. The data within the scope defined by the provisions of law are transferred in the form of electronic messages that are developed by every entity obliged to finance the services from public means in accordance with the prescribed format. The data is transferred at the end of a reporting period, i.e. a month, not later than 10 days after the expiration of the period. The data can also be sent during the reporting period. At a justified request, the entity obliged to finance the services from public means can release the service provider from the obligation to collect and transfer data in an electronic form for a specified period.

[1] Ordinance of the Minister of Health of 23 March 2013 on the requirements regarding the SIM (Medical Information System, Dz.U. (Journal of Laws) 2013, item 463.

[2] Ordinance of the Minister of Health of 20 June 2008 on the scope of the indispensable data stored by service providers, precise methods of data registering and sharing with entities obliged to finance services from public means, Dz.U. (Journal of laws) 2008, No. 123, item 801

[3] Art.45, Act of 12 May 2011 on the reimbursement of medical products, special purpose dietary supplements and medical devices, Dz.U. (Journal of Laws) 2011, No. 122, item 696 , Proclamation of the Minister of Health of 23 July 2011 on the announcement of a uniform text of the Ordinance of the Minister of Health on the information collected by pharmacies and the information transferred to the National Health Fund, Dz.U. (Journal of Laws) 2014, item 122.

Databases

Database is a set of data or any other materials and elements stored on the basis of a specified scheme or method that are individually accessible in any way – electronic access including – and one that requires a substantial investment , both as regards quality and quantity, in order to develop , verify or present its contents[4].

All entities operating within the healthcare information system are obliged to run databases. Thus, the system includes databases that are developed by entities that are obliged to run databases with the following information :

- the past, current and scheduled healthcare services;
- service providers and medical workers;
- service recipients.

The entities that run databases are entitled to process the stored data within the scope essential to fulfill their tasks. They are obliged to transfer and share the data along the principles defined by legal provisions. Their responsibilities include checking the completeness, correctness and accuracy of the data being stored and shared

The transfer and update of the data sent to the information system is carried out electronically.

The entities obliged to conduct healthcare databases will have to deal with several problems, including the issues related to the possible application of cloud computing. First of all, the security and confidentiality of the data will have to be ensured. Moreover, there is the necessity to define – within the law regulations – the principles of applying their own databases as well as the ones belonging to other entities.

The entities that run healthcare databases are obliged to provide organizational and technological infrastructure that would ensure the protection of data being processed; particularly to protect the data against unauthorized access, their illegal disclosure or acquisition as well as modification, damage or loss.

[4] Art.2, item 1, Act of 27 July 2001 on database protection. Dz.U.(Journal of Laws) 2001 No. 128, item 1402

Healthcare databases are subject to supervision. In the cases when the inspection procedures are related to the access to individual medical data[5] or medical records, they can be proceeded only by a person of a medical profession that is adequate to the kind and scope of the data under control or the range of medical record being accessed.

The inspectors are obliged to keep the confidentiality of the information on the patient, including the individual medical data, that is acquired in relation to the inspection procedures. The use of the data for the needs of the inspection is acceptable only in the way that makes the identification of the patient impossible. As regards the entities that administer healthcare databases, the minister competent for health has the right to:

- inspect the implementation of the health sector IT projects and teleinformatic systems that operate within the information system in order to ensure their coherent functioning and correctness as well as completeness of data transferred to the system[6];
- monitor the legality, purposefulness and reliability of running the healthcare databases and transferring the data to the information system;
- make recommendations as regards the removal of faults revealed by the inspection.

The protection of databases is regulated by the Act on database protection[7]. That is the so called *sui generis* protection, irrespective of the protection that some databases are entitled to in accordance with the Act on copyright and related rights[8]. The act protects first of all the economic interests of the entity that covered the costs of database development and functioning.

Unauthorized revealing or transferring the data from the database is the case of unfair competition conduct[9] that consists in the violation of business secret on the condition that the employer took necessary steps to maintain the confidentiality of data.

[5] Art. item 7, individual medical data – personal data and other concerning natural persons that regard their entitlement to healthcare services that were completed, are being provided or scheduled, their health and other data processed with regard to past, current and scheduled healthcare services, health prevention and accomplishment of healthcare programs;

[6] along the principles defined by the provisions of articles 25–35, Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565

[7] Act of 27 July 2001 on database protection. Dz.U.(Journal of Laws) 2001 No. 128, item 1402

[8] Act of 4 February 1994 on copyright and related rights, Dz.U. (Journal of Laws) 1994, No. 24, item 83

[9] Act of 16 April 1993 on combating unfair competition, Dz.U. (Journal of Laws) 1993, No.47, item 211

The Ministers of Health and the Minister responsible for computerization are obliged to develop and share free of charge the software for running electronic databases, including medical registers, that enables data set founding and updating, the development of healthcare databases and their integration within the information system with the consideration of the technological neutrality principle[10].

Registers

Medical registers[11] are a type of databases that is defined separately in the Act. They are mainly collections of records, lists and other sets of data, including personal data, that are organized in some order. Founding a medical register and its closing down is possible by means of an ordinance. They can be conducted by entities stipulated by law. The data is transferred to registers by:

- service providers and pharmacies;
- entities that keep public and medical registers.

The regulations concerning register oblige healthcare service providers to complete adequate electronic forms (sometimes also in a paper version) and to transfer them to the entities that conduct registers.

The provisions of several acts and ordinances regulate in detail the principles of the transfer of data and information to and from healthcare registers.

The data from the registers is shared free of charge with the healthcare information system by service providers and by entities that keep medical registers. Some of the registers are (or will be) conducted in the cloud. The data in medical registers can be shared for statistical scientific and research reasons only in the form that makes it impossible to assign it to a particular natural person.

The scope of data processed in the registers is defined by the provisions of law. Data other than the one referred to in the Act and the one that can be assigned to a particular natural

[10] according to the provisions of law, Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565

[11] medical register - a register, records, a list or any other set of personal data or individual medical data in an organized form that is developed under the law, Art. 2, item 12, Act of 28 April 2011 on healthcare information system , Dz.U. (Journal of Laws) 2011 No. 113, item 657

person can be processed in medical registers only in the cases when the source of the data is a document including personal data that cannot be separated when transferring or when the identification is essential to accomplish the tasks and objectives of the register.

Data processing in the register is legal on the condition that the individual concerned is informed about it. Within 30 days since the beginning of the processing procedures, the entities that keep a register are obliged to inform every individual in question to inform about the following :

- the address of the location and full name of the entity;
- the objectives, scope and form of processing the data of the individual;
- the right to have the access to the data and its correction;
- the optionality or obligation to provide the data that is being processed in the register and – in the latter case – the adequate legal provisions.

In the case of the individual's refusal, the administrator of the data is obliged to remove from the register any data that make the identification of the individual possible unless the processing is essential to save people's lives or health.

The minister competent for health conducts a list of medical register in the BIP (Public Information Bulletin). The list is updated immediately after founding or closing down a register.

The minister also plays the role of the administrator of the data stored in medical registers.

The procedure of sharing the information that is stored in registers has been regulated. The entity that keeps a public register[12], when revealing the information from the register in the form of data exchange, is obliged to give account of such operations.

The entity that keeps a register informs in a commonly accessible way (including the BIP) on the conditions, methods, scope and time of the register data sharing as well as the format in which the data is made accessible. In the cases when the provisions on the basis of which the register is kept do not define the time of data sharing, the data is shared not later

[12] Public register – a register, records, a list or any other form of keeping records that is applied to complement public tasks , kept by a public entity on the basis of separate statutory provisions; Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565

than within 14 days from the day when it was applied for. The data stored in the register is shared by the head of the unit where the register is kept or by a person authorized by the head.

The entity that receives the data from the register is obliged to protect it against unauthorized access or alterations as well as against its use that is inconsistent with the original purpose of its collection. The entity is responsible for the security and integrity of the data shared. The information on the technological and organizational security measures as regards the access to the register data is given in a commonly accessible way by the head of the entity keeping the register, the BIP including[13].

The exchange of data between public registers includes only the data that is essential to the correct functioning of the registers. The exchange is conducted through a direct reference to the data by the entity that initiates the exchange. Any other mode of data exchange (including the copying of data by the register that initiates the exchange) is acceptable only in justified cases.

Selection of the location of health data storage

The decision on the location of health data and information storage is one of the most significant decisions that have to be made when developing electronic medical record.

There are no legal provisions as regards the processing of data in medical records by cloud computing.

The decision on the location and method of storing the data that is included in records (also in an electronic form) is made by the head of a healthcare entity. The internal documentation is stored by the entity that developed it.

The location of the storage of current internal documentation is determined by the entity; in the case of a medical entity, the decision is made by the heads of particular organizational units of the entity in agreement with the head of the whole entity[14]. There is no requirement whether the electronic medical records should be stored on the location of the

[13] Ordinance of the Council of Ministers of 27 September 2005 on methods, scope and mode of sharing data stored in a public register ; Dz.U. (Journal of Laws) 2005, No. 205, item 1692

[14] Art. 74. Ordinance of the Minister of Health of 21 December 2010 on the types and scope of medical records and methods of their processing. Dz.U. (Journal of Laws) 2010 No. 252, item 1697

entity. The issue is regulated more precisely by the Minister of Internal Affairs. [15] The ordinance defines the location of the storage of internal documentation : it is the entity where the documentation was developed. However, it is also accepted that the documentation can be archived by another entity on the condition that it is protected against destruction, damage, loss or unauthorized access.

The requirements for electronic processing of medical records are as follows:

- the records should be kept in a teleinformatic system that ensures:
  1. the protection of the records against damage or loss;
  2. the maintenance of the integrity and reliability of the records;
  3. constant access to the records by authorized persons and protection against unauthorized access;
  4. the identification of the individual that provides healthcare services and registers the changes;
  5. sharing, also by the electronic exports of the records or its part constituting documentation as defined by the ordinance, in XML and PDF formats;
  6. the exports of the whole data in the XML format in the way that would enable the reproduction of the records in another teleinformatic system;
  7. printing the records in the forms defined by the ordinance.
- the records should be adequately protected. The provisions of law define precisely the conditions that have to be met systematically if the electronic form of the documentation is to be considered secure. The conditions are as follows:
  1) the records should be accessible only to authorized persons;
  2) they should be protected against unintended or unauthorized destruction;
  3) the effectiveness of the methods and means of protection should be commonly recognized.

In order to protect electronic medical records, the following measures are essential:

- systematic analysis of threats;
- development and implementation of the documentation and processing systems security procedures, including the procedures regarding the access and storage;
- implementation of security measures that are adequate to the threats;

[15] Art. 58. 1. Ordinance of the Minister of Internal Affairs and Administration of 18 May 2011 on the type, scope and method of processing medical records in healthcare entities founded by the minister competent for internal affairs, Dz.U. (Journal of Laws) 2011, No. 125, item 712

- current monitoring of all organizational, technological and computer security measures, including their regular effectiveness assessments;
- development and implementation of plans as regards long term documentation storage, including its transfer to new digital data carriers and new data formats if it is required to ensure the continuity of the access to the records.

Moreover, the regulations concerning electronic medical records refer to the provisions that provide for the protection of information that is included in the records and is protected by law. Those regulations regard mainly patient's rights, professional secrecy and personal data protection.

Several issues have to be considered when deciding on the location of health data processing and storing. In the analysis of the potentials of cloud computing in health data processing the attention is focused mainly on the regulations concerning personal data protection. That issue is a complex one and new regulations are expected soon, which will additionally force practically all healthcare service providers to take several further steps. This is the result of the scheduled entry into force of the European Parliament and the Council regulation concerning the processing of personal data. Regulation is an act that would directly apply in all member states without the need to pass national acts of law. After the implementation of the regulation, the European Union would reach a complete harmonization of substantive law and a free flow of data[16].

The Inspector General for Personal Data Protection expressed his views on health data processing: *Obviously, a significant number of healthcare entities is not ready to deal with the electronic form of such procedures as storing, processing or archiving medical data. The smaller healthcare entity that processes the data, the more problems will occur as regards its independent operations. That means that the market for outsourcing such services is going to boom. What is more, I expect that a substantial number of medical entities will be willing to use the cloud, which means that they will transfer the data to entities that will provide the infrastructure together with the software operating in the cloud. In other words, doctors will not have the software necessary to collect, process and record medical data in their computers. The software, and the infrastructure with the data, will be located off the doctor's room. It will not be located with a particular outsourcing entity in a particular computer but it will exist in the cloud. One has to be aware of that fact when considering the security of health data. The SIM (Medical Information System) is being implemented*

[16] General information – website of the GIODO (Inspector General for Personal Data Protection) http://www.giodo.gov.pl/1520143/j/pl/ (Accessed: 30.10.2014)

in Poland; it will be more active in using the resources, and possibly the resources that the doctors will wish to store in the cloud[17].

Entrustment of health data

The issue of entrusting the data[18] is one of the key elements related to the application of cloud computing.

A data administrator can process the data:

- on his/her own
- or delegate the processing to other entity.

In both cases the cloud can be used as a place of data processing. However, in the Polish conditions the first case would apply mainly to private or hybrid clouds, while the use of more significant resources and processing power is related to the clouds that are administered by external entities. The objective of the legislator was to separate the responsibilities of the administrator from the data managing entity.

The data administrator delegates data processing to other entity by means of a written agreement.

The entity that is entrusted the data:

- is allowed to process it only within the scope and purpose of the contract. However, in the case of cloud computing, it may happen that the entity possessing the cloud will decide on the means of data processing;
- is obliged to take appropriate measures to protect the data being processed. As regards the security requirements, the entity takes the responsibility to the same degree as the data administrator.

The responsibility for the compliance of the regulations of the Act on the protection of personal data lies on the data administrator, which does not exclude the responsibility of the entity that signed the agreement for processing the data in a manner inconsistent with the

[17] Complete record of the Commission for Innovation and New Technologies (No. 86) meeting on 11 September 2011, Inspector General for Personal Data Protection (GIODO), Wojciech Wiewiórowski, source: http://www.sejm.gov.pl/Sejm7.nsf/biuletyn.xsp?skrnr=INT-86, accessed: 30.10.2014

[18] Art. 31, Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2002, No. 101, item 926

agreement. The entity that was entrusted the data is subject to inspection as regards the compliance of data processing with the Act.

In the cases when personal data is processed by entities based in a third state, the data administrator is obliged to appoint a representative in the Republic of Poland.

Recently, in the preliminary views to the amendments to the act on patient's rights[19], suggestions emerged to introduce the institution of "entrusting data to other entity". There are also plans to introduce to the act the institution of "entrusting the storage of medical records".

Similarly, as in the Act on data protection, the entity providing healthcare services would operate as the data administrator. The entity dealing with the medical data storage would be obliged to protect it, i.e. to use technological and organizational means that would ensure the security of data being processed, adequately to the threats and category of the data under protection. The entity has to protect the data particularly against unauthorized access, processing it with the violation of the act, its alterations, loss, damage or destruction.

Moreover, the entity would be obliged – among other things – to run documentation (which includes the security policy and the procedures of IT system of personal data processing) on the method of data processing and the technological and organizational measures of data protection, to appoint an information security administrator, to allow data processing to be conducted only by individuals who are authorized by the data administrator and to keep the records of the individuals that are authorized to process the data. The individuals authorized to processing the data are obliged to the confidentiality of the data and methods of its protection. The entity that is entrusted data processing would be responsible for the violation of law in that respect and for any conduct in breach of the agreement with the data administrator. Such a solution would strengthen the guaranties of the security of data transferred by the data administrator.

According to preliminary views, a possibility to render „storage" services of paper documentation will be provided. A healthcare service provider could order the storage of paper medical documentation by means of an agreement with a medical entity whose statute would provide for such activity. The healthcare service provider would be obliged to arrange and describe the medical records to be stored. As the commission to store paper

[19] Preliminary views to the draft act on amendments to the Act on patient's rights and Patient's Rights Ombudsman and other acts., October 2013, source: http://legislacja.rcl.gov.pl/lista/1/projekt/185992, (accessed: 30.10.2014)

documentation is connected with its physical delivery – which limits a direct access to the data – it would be acceptable only on the condition of ensuring the access without undue delay. Despite commissioning the storage services to other entity, the healthcare service provider would still be obliged to share the documentation with authorized entities and authorities. The amendment would enable healthcare service providers to take advantage of the premises of another entity but would have no impact on the situation and rights of the patients who – as it is now the case – would apply for the access to medical documentation directly to the healthcare service provider and should receive it without undue delay[20].

It is a common conviction that every cloud computing service is connected, as a rule, with data entrustment[21]. However, such a position is not shared by everyone. It is particularly questionable when the cloud supplier does not have the access to data, e.g. when it is enciphered by the cloud recipient. The problem, however, is related to the definition of data processing.

According to the statutory definition, *data processing is perceived as any operation conducted on personal data such as collecting, recording, storing, developing, altering, sharing and removing, especially when done in IT systems*[22].

Consequently, data storing is one of the data processing operations and the commission of such operations to cloud providers will in fact constitute the entrustment of personal data processing. The GIODO[23] expressed the opinion that if the entity providing IT infrastructure possesses the knowledge on the character of the data being processed, it should adequately protect the data in compliance with the regulations on entrustment[24]. However, if the cloud provider does not have the knowledge on the character of the data being processed, it is not

[20] Preliminary views on the draft act on amendments to the Act on patient's rights and Patient's Rights Ombudsman and other acts., October 2013, source: http://legislacja.rcl.gov.pl/lista/1/projekt/185992, (Accessed: 30.10.2014)

[21] Art. 29 Working Party Opinion 1/2010 of 16 February 2010 on the concepts of „data controller" and „processor", hosting will be constituted, as a rule, by the entrustment of personal data processing to the entity processing the data.

[22] Art. 7, item 2, Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 1997, No. 133, item 883

[23] ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych (ABC of the security of personal data processed by IT systems, website of the GIODO (Inspector General for Personal Data Protection)
https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod_resource/content/15/INF1/INF_R05.html#

[24] Art. 31, Arts 36-39 as regards personal data protection

subject to the provisions on entrustment but to the regulations on the exclusion of liability of the provider of services by electronic means[25]. Practically, however, the excuse of the lack of knowledge on the character of data being processed will not be credible[26].

The presented above procedures of data processing and the solutions that exist in the healthcare service system must be taken into consideration when applying the cloud in medical data processing. It is particularly obvious that in the case of data entrustment, the procedures require adjustment and clarification as regards health data and their processing in cloud computing.

Bibliography

[1] ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych (ABC of the security of personal data processed by IT systems , website of the GIODO (Inspector General for Personal Data Protection) https://edugiodo.giodo.gov.pl/pluginfile.php/113/mod_resource/content/15/INF1/INF_R05.html#, (accessed: 30.10.2014)

[2] *Cloud Computing* w Sektorze Finansowym, Regulacje i Standardy (Cloud Computing in Finance Sector, Regulations and Standards), Maciej Gawroński (ed.), source: http://www.twobirds.com/~/media/PDFs/PolandPDFs/Cloud%20Computing%20w%20Sektorze%20Finansowym%20Regulacje%20i%20Standardy%202011.pdf, (accessed: 30.10.2014)

[3] Complete record of the Commission for Innovation and New Technologies (No. 86) meeting on 11 September 2011, Inspector General for Personal Data Protection (GIODO), Wojciech Wiewiórowski, source: http://www.sejm.gov.pl/Sejm7.nsf/biuletyn.xsp?skrnr=INT-86, accessed: 30.10.2014

[4] Ordinance of the Minister of Internal Affairs and Administration of 18 May 2011 on the type, scope and method of processing medical records in healthcare entities founded by the minister competent for internal affairs, Dz.U. (Journal of Laws) 2011, No. 125, item 712

[5] Ordinance of the Minister of Health of 20 June 2008 on the scope of the indispensable data stored by service providers, precise methods of data registering and sharing with entities obliged to finance services from public means, Dz.U. (Journal of laws) 2008, No. 123, item 801

[6] Ordinance of the Minister of Health of 21 December 2010 on the types and scope of medical records and methods of their processing. Dz.U. (Journal of Laws) 2010 No. 252, item 1697

[25] Arts 12-15, Act of 18 July 2002 on providing services by electronic means, Dz.U. (Journal of Laws) No. 122, item 1204

[26] *Cloud Computing* w Sektorze Finansowym, Regulacje i Standardy (Cloud Computing in Finance Sector, REgulations and Standards), Maciej Gawroński (ed.), http://www.twobirds.com/~/media/PDFs/PolandPDFs/Cloud%20Computing%20w%20Sektorze%20Finansowym%20Regulacje%20i%20Standardy%202011.pdf, (Acccessed: 30.10.2014)

[7] Ordinance of the Minister of Health of 23 march 2013 on the requirements regarding the SIM (Medical Information System, Dz.U. (Journal of Laws) 2013 item 463.
[8] Ordinance of the Council of Ministers of 27 September 2005 on methods, scope and mode of sharing data stored in a public register ; Dz.U. (Journal of Laws) 2005, No. 205, item 1692
[9] Act of 12 May 2011 on the reimbursement of medical products, special purpose dietary supplements and medical devices, Dz.U. (Journal of Laws) 2011, No. 122, item 696 , Proclamation of the Minister of Health of 23 July 2011 on the announcement of a uniform text of the Ordinance of the Minister of Health on the information collected by pharmacies and the information transferred to the National Health Fund, Dz.U. (Journal of Laws) 2014, item 122
[10] Act of 16 April 1993 on combating unfair competition, Dz.U. (Journal of Laws) 1993, No.47, item 211
[11] Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565
[12] Act of 18 July 2002 on providing services by electronic means, Dz.U. (Journal of Laws) No. 122, item 1204
[13] Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2002, No. 101, item 926 Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2002, No. 101, item 926
[14] Act of 4 February 1994 on copyright and related rights, Dz.U. (Journal of Laws) 1994, No. 24, item 83
[15] Preliminary views on the draft act on amendments to the Act on patient's rights and Patient's Rights Ombudsman and other acts., October 2013, source: http://legislacja.rcl.gov.pl/lista/1/projekt/185992, (accessed: 30.10.2014
[16] Source – website of the GIODO (Inspector General for Personal Data Protection) http://www.giodo.gov.pl/1520143/j/pl/ (Accessed: 30.10.2014)

Abstract

The article presents procedures related to the transfer of medical service data to healthcare information systems, the functioning of databases, medical electronic documentation and registers. It discusses the issues of loading the system with data and information, running databases and registers, storing and entrusting health data. The presented procedures of data processing and the solutions functioning in the healthcare system have to be considered if cloud computing is to be applied in medical data processing. As it has been presented, particularly in the case of data entrustment, the procedures require adjustment and clarification as regards health data and the application of cloud computing.