Dr Artur Romaszewski
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
artur.romaszewski@uj.edu.pl

Dr Wojciech Trąbka
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda
Jagiellonian University Medical College

Faculty of Health Sciences

Medical Information Systems Department
krzysztof.gajda@uj.edu.pl

CLUD COMPUTING AND PROCESSING MEDICAL DATA IN ELECTRONIC FORM

Introduction

The implementation of modern IT solutions in a health care system requires the compliance to the standards of secure data processing in health care entities. Cloud computing is an available technology that may serve this function. As regards the application of cloud solutions in the processing of data in health care, one can see some enthusiasm resulting from numerous benefits of this technology on the one hand but on the other hand several problems emerge concerning:

- diversified interpretation of legal regulations, including different approaches of various state authorities as regards the interpretation of the acceptability of the application of cloud computing,

- protection of privacy, including the protection of personal data, health data in particular,
- the consequences of processing the data abroad as the Internet crosses state borders and the regulations of personal data processing differ in various countries,
- the lack of information about cloud service subcontractors,
- ownership changes as regards cloud computing suppliers,
- the protection of the continuity of operation, the compliance with international standards, etc.

Numerous publications on cloud computing include the division of clouds by the groups of users that have the access to particular clouds. Thus, there are public, private, community, hybrid and personal clouds[1]. It is crucial that every type of a cloud should provide conditions that are indispensable for the functioning of a public cloud:

- resource pooling– available to every registered user
- virtualization – effective sue of the hardware
- elasticity – dynamic scaling without investment costs
- automation – development, implementation, configuration, protection and transfers without hand-on intervention
- pricing – business model depends on actual use: you do not pay for the resources that you do not use.

In the case of private clouds three conditions are required: virtualization, elasticity and automation. The remaining two, i.e. resource pooling and pricing, are related to the business attributes of public clouds and do not refer directly to private clouds. Private clouds by definition are not a pool of computing resources that are available on demand to all registered users.

Private clouds are a type where internal resources of a company, i.e. its data centre, are not available publicly. The resource pool is controlled by a particular organization and is available only to its members. The difference between a private and a public cloud is that its

[1] Reczek E., Implementation of Cloud Computing in health Care Sector, Scientific Journal of WSZiB in Krakow 2014 No 33

computing resources are not available to external users (i..e. to the bodies external to the company that owns the data centre and its available computing capacity)[2].

A hybrid cloud is a combination of two models of cloud computing: an efficient and effective external cloud and the company's own network. Thus, this is the cloud computing environment in which a company provides and manages the resources within the organization while other services are provided by an external provider. Practically it means that the company uses the public cloud but it stores the data (e.g. the data of its patients) in its own database. Cloud computing is considered to be the future of companies and the hybrid model is to be the most popular. Major corporation have already made significant investments in the infrastructure that is necessary for the management of resources within the organization. Moreover, numerous organizations prefer storing special data by themselves for security reasons.

Through the integration of several cloud services the users can more easily go to the services of external cloud as they avoid frequent compatibility or authorization issues. A hybrid cloud is administered parallelly by the internal and external provider in line with their competencies[3].

The document of the European Parliament's Committee on Internal Market and Consumer protection *Cloud Computing – Study* includes the definitions of both private and personal clouds[4] . The latter may practically be a small server in a home or small business network that can be accessed over the Internet. Designed for storing and sharing personal content, personal clouds enable viewing and streaming from any Internet-connected personal computer and quite often from smartphones. Although personal clouds function in a similar manner to any private cloud that is set up in a company, their primary feature is the easy installation for an average personal computer user. A question arises, however, whether a small or medium-sized health care entity will be capable of updating the security tools that were installed at the moment of the system was installation.

Which cloud?

The publications on the implementation of cloud computing in health care entities frequently suggest that private cloud is the only acceptable form as regards this type of health

[2] Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*. Wydawnictwo Helion
[3] http://computingcloud.pl/pl/cloud-przewodnik/219-chmura-prywatna-publiczna-a-moze-hybrydowa
[4] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf

data processing. Such approach is based on the fact that only private cloud computing makes it possible to take into consideration data processing area other than a private one. This area should be indicated in the security policy and it includes a list of buildings, rooms or their parts where personal data are processed.[5] Obviously, one should not forget that an ordinance regulating these issues was introduced in the early days of the Internet in Poland[6]. Its literal interpretation does not allow for the use of laptops, tablets and other mobile tools to process data by health care service providers out of a strictly defined data processing area.

It has been emphasized since the beginning of cloud computing services in the health care system that health data should be processed in areas that are controlled by the entities which are entitled to process them. Thus, in practice private cloud computing (with the possibility to use servers outside the area of a health care entity) was acceptable. It was assumed that public clouds are vulnerable to any attacks or errors resulting in an unauthorized access to the data or their loss. Despite that, health care entities lack adequate internal procedures aiming at the protection of IT systems and, consequently, the sensitive data of patients are protected insufficiently. A decision to transfer all or some of the data out of their IT systems – mainly to computing clouds – would be a solution to the problem. However, there is still the issue of the legal acceptability of the transfer of the data and health information to the resources that are out of direct control of controllers – i.e. mainly to computing clouds.

The choice of a cloud computing service provider is a comparatively complicated task. In Poland the principle of technological neutrality of the state is applied. That means that all entities can provide services while the role of the state is to prepare and publish technological solutions (mainly by indicating adequate standards and norms) so that the interoperability of the existing systems is ensured. In order to be effective in the provision of services in a cloud model the provider should not only have adequate competencies, products and infrastructure but also a suitable scale, i.e. organizational and financial potentials

That condition is met by companies that operate globally and due to the attractiveness of the potential market they are first in their endeavors to meet the requirements of the EC

[5]Ordinance of 29 April, 2004 of the Minister of Internal Affairs and Administration on personal data processing documentation and technological and organizational conditions to be met by devices and computer systems used to process personal data, § 4.

[6] The first Internet portal developed by Poles started operating in 1995. It was *Wirtualna Polska*. In April 1996, Telekomunikacja Polska company offered anonymous access to the Internet via a modem. At first media in Poland considered the Internet as an unprofessional, unpromising and costly tool - https://pl.wikipedia.org/wiki/Internet_w_Polsce

guidelines. Microsoft is such a company. Inspectors for personal data protection from 28 EU countries – the so called Article 29 Data Protection Working Party (including Polish GIODO – General Inspector for Personal Data Protection) – i.e. the authorities that control companies operating in EU published their common position in which they express their support to the Microsoft correct contract solutions regarding cloud computing services for business. In short, in this particular case it means the service users are informed that the EU regulator accepts Microsoft's approach to the protection of privacy and the security of data of EU citizens.

The issues presented above became the subject to EU regulations and in 2016 Directive (EU) 2016/1148 of the European Parliament and of the Council was adopted concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). EU states were obliged to develop national strategies of cybersecurity, to identify the operators of the essential infrastructure (hospitals included) and to develop national cyberattack response networks based on Computer Security Incident Respond Teams (CSIRT). The NIS Directive is restricted to two types of entities: the so called essential service operators (power sector, transport, banking and financial market infrastructure, healthcare, water supply, digital infrastructure) and digital services providers (internet trade platforms, search engines, processing services in cloud computing).

The choice of the essential services providers depends only on the member-state and will be made either together with the implementation of the NIS Directive or directly after its implementation. It is not stated which services are in question – every country has to develop a list of essential services for each sector mentioned in the Directive.

The selected entities will have mainly two responsibilities. Firstly, to introduce security measures (both technical and organizational) that are adequate to the risk level that will probably be also defined by functionaries. Secondly, to report the incidents[7]. The Directive concerns three types of digital service providers: trade platforms, search engines and data processing in clouds. As the issue concerns international operators, the decision was made that they will be appointed by EU and – as in the case of essential services operators – they will have to ensure security levels adequate to identified risks[8]. Moreover, the general ordinance on

[7] The operating procedures for computer security incidents are given in NIST 800-61 standard which was developed by the National Institute of Standards and Technology at the US Trade Department

[8] Grzybowski M., *Dziewięć faktów o Dyrektywie NIS, które powinieneś znać*, https://www.cybsecurity.org/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/

data protection provides for stricter respopnsibilities of the entities which administer and process the data (e.g. hospitals) as regards the protection of personal data that are stored. The lack of security measures adequate to the risk level may result in severe financial penalties imposed by GIODO of 10 or 20 million Euro depending on the degree of infringement or – in the case of companies – 2% or 4% of the total annual revenue in the previous fiscal year. EU countries have to implement the NIS Directive by 2018.

The use of cloud computing services may involve some risk concerning, for example, the security of data. The ISO/IEC 27018:2014 standard, which is based on the older version ISO 27001 may be here of some help. These standardizing regulations (ISO/IEC 27018:2014 and the original standard ISO 27001) concern mainly the following issues:

- security policy
- organization of information security
- HR security
- asset management
- access control
- cryptography and sensitive data encryption
- physical and environmental security
- operational management
- management of information security incidents
- information security issues in operational continuity management
- compliance with national standards.

The above mentioned standard includes the following assumptions for the user of cloud computing: service transparency for the user, clear standards as regards the rights and responsibilities of the provider and the user, the implementation of the core principles that make data processing possible in compliance with the existing legal regulations.

Providers who would like to implement the ISO/IEC 27018:2014 standard should first of all ensure the users (employees) the control over the processing of their data. It is also within the responsibilities of cloud computing providers to ensure restrictions as regards the disclosure of data and the access to the data by a third party, e.g. subcontractors (including the obligation to ensure confidentiality and to disclose the subcontractors to the users). It is required that the above standard should be transparent as regards the request of state authorities (e.g. the

prosecutor or the court) to disclose personal data. The registered data of users can be disclosed to such authorities only when the provider is obliged by law to do so. On the basis of publication[9], GIODO developed a document entitled *Dekalog chmuroluba* (Cloudfan decalogue) [10] which includes the guidelines that concern the security of data stored in clouds. The data recording format in cloud computing is another issue.

Legal standards for all entities that carry out public tasks are included in the Regulation of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, the minimum requirements for public records and exchange of information in electronic form and minimum requirements for ICT systems[11]. Pursuant to the regulation all data generated by an IT system (including the systems of healthcare entities) should be recorded in XML format. Consequently, the data sent to cloud computing and acquired from the cloud should be in XML format, which also involves the possibility to exchange medical data through – for example - HL7. However, no norm or standards include a precise indication on the format in which the data should be stored in clouds. The first entity to implement the ISO/IEC 27018:2014 standard officially was Microsoft.

Cross-border transfer of medical data

When signing a contract for data processing, especially in the case of cloud computing, the principles of personal data transfer should be taken into consideration. The general rule is that data transfer within the European Economic Area is treated in the same way as the transfer in Poland. The same applies to all EU member-states and the member states of the EEA which are not in the EU (Norway, Island and Lichtenstein at present). In other words, signing contracts with a service provider whose service systems are based in the EEA is legal and separate consents are not required.

Data can be transferred to the remaining countries if an adequate protection level is ensured. Due to a significant diversification of national personal data protection systems, the Article 29 Working Party pointed at three conditions that the systems should meet to be allowed to process personal data. Thus, the system should ensure a high level of compliance with the personal data processing principles (it should be effective and the data controllers should be

[9] Segalis B., *Cloud Computing Legal Risk and Liability,* InfoLawGroup 2011
[10] http://www.giodo.gov.pl/259/id_art/6271/j/pl
[11] http://dziennikustaw.gov.pl/du/2016/113/D2016000011301.pdf

well aware of their responsibilities). Moreover, the system should also provide the opportunity to exercise the rights by data subjects; this means that the system ensures the possibility to seek compensation in the cases of infringement. Finally, the system should make it possible to transfer personal data to a third country that does not ensure adequate protection only on the condition that one of the following prerequisites that are defined in the act should be fulfilled:[12]

- the data subject has given his/her written consent,
- the transfer is necessary for the performance of a contract between the data subject and the controller or takes place in response to the data subject's request,
- the transfer is necessary for the performance of a contract concluded in the interests of the data subject between the controller and another subject,
- the transfer is necessary or required by reasons of public interests or for the establishment of legal claims,
- the transfer is necessary in order to protect the vital interests of the data subject,
- the data are publicly available.

If the conditions of the Act are not fulfilled and the third country does not ensure adequate protection standards, the transfer of data may take place after a prior consent of GIODO, provided that the controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject.

It should be pointed out that the commencement of the personal data transfer to a third country that does not ensure adequate protection can take place only after the positive decision of GIODO as the decision does not legalize prior transfers of personal data.

However, the consent of GIODO is not required if the data controller ensures adequate safeguards with respect to the protection of privacy, rights and freedoms of the data subject through:

- standard contractual clauses on personal data protection as approved by European Commission[13]

[12] Act on data protection, Art.47 , section 2 and 3.
[13] under Art.26, section 4 of the Directive

- binding corporate rules that have been approved by the Inspector General[14]

There is no obligation to apply standard clauses. At present, the data controller who uses model contractual clauses approved by European Commission as an adequate instrument protecting the rights and freedoms of data subjects is exempt from the duty to apply to GIODO for the data transfer consent. So far, the Commission issued three decisions that include sets of standard clauses. The first two concern controller-to-controller data transfers. The clauses introduced by the third decision are applied in the cases of controller-to-processor data transfers. Model clauses can constitute a part of a wider transfer contract between a data controller and recipient or they may be included in the appendix to the agreement[15].

The consent of GIODO will not be required if the data transfer complies with legally binding rules of personal data protection that are approved by GIODO, the so called *binding corporate rules* (BCRs). BCRs are a private law instrument that aims at a high uniform protection level of rights of data subjects with respect to the data transfer within company groups in order to compensate the lack of personal data protection in particular countries. As a result of the adoption of such rules by a corporation, all data controllers belonging to this capital group will be able to share personal data without a separate consent of GIODO on the condition that they follow the rules. Moreover, the controller will also be allowed to transfer the data to the processor. This can be done on the basis of a written agreement between the controller and the "subcontractor". In this case, data processing can be performed only for purposes indicated in the agreement and one should not forget that the controller is still responsible for the protection of the data. At present, GIODO first approves corporate rules with respect to personal data protection and consequently there is no need to apply for the consent for a transfer[16].

Conclusions

It seems that the introduction of cloud computing as a common mechanism of health data processing is only a matter of time. Due to the fact that the majority of people who provide

[14] Under Art. 48, section 2 of the Act on personal data protection
[15] Wronka K., *Modelowe klauzule umowne, a ochrona danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/modelowe-klauzule-umowne-a-ochrona-danych-osobowych.html
[16] Wronka K., *Wiążące reguły korporacyjne w świetle nowelizacji ustawy o ochronie danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/wiazace-reguly-korporacyjne-w-swietle-nowelizacji-ustawy-o-ochronie-danych-osobowych.html

medical services lack the necessary technical and IT competences, the Authors think that it is the Minister of Health who should be involved in the assessment of the solutions that are offered by cloud computing providers. The Ministry should develop adequate regulations in a legal act that would indicate what requirements should be met by cloud computing providers to enable them to process health and other sensitive data such as genetic data.

On the other hand, the providers of cloud computing services should aim at maintaining the transparency as regards privacy, providing their clients with options of privacy protection and a responsible management of the data stored in the cloud. In order to guarantee such practices, service providers implement adequate procedures and security policy that are confirmed by independent certificates (such as the certificate of compliance with 27001/27002:2013, which is a commonly applied international standard of information security management, ISO/IEC 27018 as regards PII data protection or the *Cloud SecurityAlliance Cloud ControlsMatrix* [CCM] which describes the core protection principles that should be applied by service providers) and audit procedures that comply with global standards (e.g. SOC 1 and SOC 2 in the area of auditing) [17] .

Bibliography:

[1.] Gibas A., Gawroński M., Gajda R., *Czas na chmurę w sektorze finansowym w Polsce!,* https://it.projektekf.pl/sites/default/files/prezentacje/CloudComputingInFSIPoland_GAB_Article_online.pdf
[2.] Grzybowski M., Dziewięć faktów o Dyrektywie NIS, które powinieneś znać, https://www.cybsecurity.org/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/
[3.] http://computingcloud.pl/pl/cloud-przewodnik/219-chmura-prywatna-publiczna-a-moze-hybrydowa
[4.] http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/475104/IPOL-IMCO_ET(2012)475104_PL.pdf
[5.] Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*. Wydawnictwo Helion
[6.] Procedures for computer security incidents are given in NIST 800-61 standard which was developed by the National Institute of Standards and Technology at the US Trade Department
[7.] Reczek E., *Zastosowanie chmury obliczeniowej w sektorze ochrony zdrowia*. Zeszyt Naukowy - Wyższa Szkoła Zarządzania i Bankowości w Krakowie 2014 nr 33

[17] Gibas A., Gawroński M., Gajda R., *Czas na chmurę w sektorze finansowym w Polsce!,* https://it.projektekf.pl/sites/default/files/prezentacje/CloudComputingInFSIPoland_GAB_Article_online.pdf

[8.] Ordinance of 29 April, 2004 of the Minister of Internal Affairs and Administration on personal data processing documentation and technological and organizational conditions to be met by devices and computer systems used to process personal data
[9.] Segalis B., *Cloud Computing Legal Risk and Liability,* InfoLawGroup 2011
[10.] Wronka K., *Modelowe klauzule umowne, a ochrona danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/modelowe-klauzule-umowne-a-ochrona-danych-osobowych.html
[11.] Wronka K., *Wiążące reguły korporacyjne w świetle nowelizacji ustawy o ochronie danych* http://prawoitechnologia.pl/aktualnosci/dane-osobowe/wiazace-reguly-korporacyjne-w-swietle-nowelizacji-ustawy-o-ochronie-danych-osobowych.html

Abstract

The article presents practical issues regarding the implementation of cloud computing in processing medical data in electronic form. It discusses particular types of cloud services, the prerequisites for the choice of particular solutions from the point of view of healthcare entities and the concept of the contract for data processing with the application of cloud resources within the framework of the cross-border transfer of medical data.