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

REQUIREMENTS AND STANDARDS IN MEDICAL DATA PROCESSING

The aim of the article is to present standards related to personal data security, the standards applied when developing and applying IT systems and registers that are developed and run by entities offering medical services. The standards must be considered when planning the implementation of cloud computing in health data processing.

Responsibilities resulting from the fact that health data being processed is considered as personal data

The provisions of the Act on data protection with implementing ordinances[1] oblige every entity that processes personal data to take several steps aiming at the assurance of personal data security, its confidentiality, integrity and accountability. The meaning of these concepts that are defined by adequate provisions of law is given in Table 1.

Table 1. Meaning of the selected legal terms that are applied in the area of personal data processing

Data confidentiality	is understood as a property that ensures that the data is not available to unauthorized entities;
Data integrity	is understood as a property that ensures that the data is not modified or destroyed by unauthorized party;
Data accountability	is understood as a property that ensures that the operations can be assigned explicitly only to the entity that performs them

Source: Authors' development based on the Act on data protection with implementing ordinances[1]

[1] Ordinance of the Minister of Internal Affairs and Administration of 29 April, 2004 on personal data processing documentation and technological and organizational conditions to be met by devices and computer systems used to process personal data Dz.U. (Journal of Laws) No. 100, item 1024)

In order to meet the above requirement, the cloud administrator is obliged to perform several operations as indicated by regulations[2]:

a) the obligation to develop and keep security documentation

Irrespectively of the fact whether the entity processing personal data is the data administrator or the entity that was entrusted the data, it has to make a record of the data in the data security policy document and determine the processing procedures in the management instructions of the IT system that is applied to process the data (e.g. regarding the assignment of permissions, the methods and means of authorization, archiving procedures, etc.). When processing the data, it is significant to determine the range of data processing, to make a list of personal data records with the indication of the software applied in the processing and to develop the descriptions of database structures and the methods of data flow between particular systems. Moreover, the entity has to indicate what technological and organizational measures were taken to ensure the confidentiality, integrity and accountability of data processing. The above operations are regulated by the security policy.

b) requirements regarding the system in which health data is processed

The administrator should see to the fact that the service provider has a system that operates in compliance with the provisions of law. The system that is applied to every individual whose personal data is processed should be capable of including:

- the date of the first load of data to the system;
- ID of the user that enters personal data to the system, unless the IT system and the data processed can be accessed by only one person;
- the data source in the case when it is not collected from the individual that the data refers to;
- the information on the data recipients;
- the refusal to process the data for marketing purposes or to transfer it to another administrator.

The above information should be provided automatically after the confirmation of the data entry by the user.

[2] Arts 36-39a, Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2002 No. 101, item 926; Ordinance of the Minister of Internal Affairs and Administration of 29 April, 2004 on personal data processing documentation and technological and organizational conditions to be met by devices and computer systems used to process personal data Dz.U. (Journal of Laws) No. 100, item 1024)

Moreover, the IT system provides the possibility for every individual whose personal data is processed to develop and print out a report with the above information in a commonly understandable form.

c) the requirement to introduce procedures that are adequate to the security level of the entity

Security levels of processing personal data in an IT system are introduced in relation to the category of data being processed and the threats that result mainly from connecting the devices of the data processing IT system with a public network:

Table 2. Security levels of personal data processed in an IT system

Level	Level application
basic	- sensitive data cannot be processed by the system, - none of the devices of the IT system applied in personal data processing is connected to a public network,
intermediate	- the system processes sensitive personal data, - none of the devices of the IT system applied in personal data processing is connected to a public network,
advanced	- applied when at least one device of the IT system that processes personal data is connected to a public network.

Source: Authors' development based on the 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

Adequate security measures that are provided by law are implemented in accordance to the security level of entity offering medical services. Due to the fact that the advanced level will always be applied in the case of the use of cloud computing in health data processing, all the requirements to that level must be implemented.

It is a rule that all requirements of lower levels must be applied if a higher level is introduced. Thus, in the case of the advanced level, several requirements of the basic and intermediate levels should be implemented.

The personal data processing IT system is protected against the threats from public networks through the implementation of physical or logical security measures that guard against unauthorized access.

Logical security measures include:

- the supervision of the data flow between the data administrator's IT system and the public network;

- the supervision of operations that are initiated from the public networks and the data administrator's IT system.

The advanced security level involves the administrator's obligation to implement cryptographic security measures in relation to the authorization data that is sent in the public network. Although there is no direct duty to cipher all personal data, one should emphasize the fact that the data administrator is obliged to implement technical and organizational measures in order to ensure the protection of personal data being processed that is adequate to the security threats and the category of the data and, particularly, to protect the data against an authorized access or theft, the violation of the provisions of law during data processing or any modification, loss, damage or destruction of the data[3].

Other requirements concerning cryptographic data security measures should also be mentioned.

- Cryptographic protection should cover personal data that is processed in portable computers outside the data processing area.
- Devices and personal data carriers that are moved out of the area are secured in a way that ensures the confidentiality and integrity of the data.

However, there is no obligation of cryptographic protection as regards the data that is transmitted through a network.

Responsibilities related to the implementation of the standards of ICT systems

The standards provided for ICT systems that are applied by medical service providers constitute a complex issue since the Act on the computerization of entities implementing public tasks includes an indication of entities that are obliged to fulfill the tasks that is contrary to the indication in the Act on medical activity[4]. That is caused by the fact that

[3] Art. 36, Act of 29 August 1997 on the protection of personal data, Dz.U. (Journal of Laws) 2002 No. 101, item 926

[4] Act of 15 April 2011 on medical activity , Dz.U. (Journal of Laws) 2011 No. 112 , item 654

- independent public healthcare centers and joint-stock companies providing healthcare services within the meaning of regulations on medical activity[5] and
- the National Health Fund (NFZ)

are considered by the Act as entities that are obliged to follow the standards regarding, among others, ICT systems, registers, procedures of sharing electronic documents and the application of the ePUAP (Electronic Platform of Public Administration Services).

Obviously the problem concerns the term of *joint-stock companies providing healthcare services*. The regulations[6] do not provide for such form of medical activity. A correct form is: entrepreneur in the meaning of the provisions of the Freedom of Economic Activity Act[7].

The standards are applied to a great extent in relation to entities that are commissioned a public task by a public entity if the tasks involves the obligation to transfer information to or from entities that are not the bodies of state administration[8]. That refers – among others – to doctor and nursing services contracted by the NFZ. The entities are obliged to implement standards regarding, among others, the minimal requirements for ICT systems.

The development of ICT systems consists mainly in the implementation of standards that are defined by the National Interoperability Framework[9] .

The ICT systems applied by the entities mentioned above are implemented and operated with the consideration of their functionality, reliability, usability, efficiency, transferability and maintainability, with the consideration of norms and professionally accepted standards and methods. The management of services provided by ICT systems aims at offering the services at the declared accessibility levels and it follows documented procedures.

[5] Art. 2. Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565

[6] Act of 15 April 2011 on medical activity , Dz.U. (Journal of Laws) 2011 No. 112 , item 654

[7] Freedom of Economic Activity Act of 2 July 2004 , Dz.U. (Journal of Laws) 2010, No. 220, item 1447 (as amended in 2) in all forms provided for economic activity unless the act provides otherwise

[8] Art. 2 item 2 . Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565

[9] Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and information-sharing in electronic formats and minimum requirements for ICT systems (Journal of Laws) 2012, item. 526

Regulations indicate standards whose implementation results in meeting the above requirements. The processes of designing, implementing, exploiting, monitoring, viewing, maintaining and improving the service management should be in line with Polish Standards PN-ISO/IEC 20000-1 and PN-ISO/IEC 20000-2.

A system should be equipped with hardware and software that enables sharing the data with other ICT systems with the use of coding and communication protocols defined by current regulations, norms, standards or recommendations provided by a national or EU standardization entity. In the cases when there are no regulations, norms or standards, international standards are applied[10]

There are standards of encoding the characters in documents that are sent from or received by ICT systems - also as regards sharing the information between the systems via teletransmission lines[11]. The ICT systems share the information resources in at least one of the data formats provided by regulations. Moreover, standards are established as regards receiving electronic documents that are applied in the operations performed by public entities[12].

Establishing an **information security management system** is one of the most important responsibilities. Every entity that applies ICT systems to implement public tasks develops, establishes, implements, operates, monitors, views, maintains and improves a system that ensures confidentiality, availability and integrity of information with the considerations of such properties as authenticity, accountability, non-repudiation and reliability.

There are two ways that enable the implementation of a system:

- individual development and implementation,

[10] developed particularly by:
1) Internet Engineering Task Force (IETF) and published in the form of Request For Comments (RFC),
2) World Wide Web Consortium (W3C) and published in the form of W3C Recommendation (REC) – adequately to the requirements resulting from the task being implemented and the current state of IT. The information on the accessibility of the above descriptions of standards is published in the BIP (Public Information Bulletin) by the minister competent for computerization

[11] If the sharing concerns the sharing of characters, it is conducted according to the Unicode UTF-8 standard defined by ISO/IEC 10646 with amendments or other standard replacing it . In justified cases, UTF-16 character encoding is acceptable. The application of encoding cannot have a negative impact on the co-operation with an ICT system

[12] Art. 18 item.2 Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and information-sharing in electronic formats and minimum requirements for IT systems (Journal of Laws) 2012, item. 526

- development of the system on the basis of specified standards, i.e. Polish PN-ISO/IEC 27001 standard; the security provision, risk management and auditing are carried out on the basis of Polish Standards[13] related to the above standard,.

If an entity independently develops and establishes, implements and operates, monitors and views, maintains and improves an information security management system, it should follow the requirements presented in Table 3.

Table 3. Requirements for the development, implementation and maintenance of an Information Security Management System

- ensure the update of internal regulations as regards the changing environment,
- keep the inventory of hardware and information processing software updated, with regard to its type and configuration,
- conduct regular analyses of the risk of the information integrity loss, its accessibility and confidentiality and react to minimize the risk in accordance with the results of the analyses,
- take measures to ensure that persons involved in data processing are authorized and act adequately to the tasks and responsibilities with the aim to ensure data protection; change their competencies in the case of the change of their responsibilities,
- provide training to individuals involved in data processing with a particular consideration of such issues as: • the threat to information security, • the results of the breach of information security, including legal liability; • the implementation of information security measures, including devices and software that minimizes the risk of human errors,
- ensure the protection of data being processed against theft, unauthorized access, damage or interferences by: • monitoring the access to information, • operations aiming at the detection of unauthorized attempts to process the data, • providing means to protect against unauthorized access on the level of operating systems, network services and applications,
- establish basic rules to guarantee the security of mobile data processing and teleworking,
- protect the data to prevent from its unauthorized disclosure, modification, removal or destruction,
- ensure an adequate information security level when signing servicing contracts with third parties,
- establish information handling rules to minimize the risks of stealing the information and information processing means, mobile devices included,
- ensure an adequate security level in ICT systems mainly by: • software updating, • minimizing the risk of information loss due to breakdowns, • protection against errors, loss and unauthorized modification, • implementing cryptographic mechanisms adequately to the threats or the requirements of the provisions of law, • providing the security of system files,

[13] Including:

- PN-ISO/IEC 17799 – regarding security provision;
- PN-ISO/IEC 27005 – regarding risk management;
- PN-ISO/IEC 24762 – regarding the restoration of ICT systems following a disaster within business continuity management;
- if justified by the ICT system risk analysis, the entities implementing public tasks should be provided with additional security.

• reducing the risk resulting from publishing technological vulnerabilities of ICT systems, • immediate reaction after noticing undisclosed vulnerabilities of ICT systems as regards the possibility of security breaches, • control of the compliancy of ICT systems with adequate standards and security policies;
- immediate reporting on the incidents of information security breaches in a defined and predetermined way to enable a prompt corrective reaction,
- ensure a regular, at least annual, internal audit as regards information security.

Source: Authors' development on the basis of National Interoperability Framework.

Accountability in ICT systems involves a reliable documentation in the form of electronic records entered into logs. It is obligatory to enter into logs the operations of users or system elements that regard:

- the access to the system with administrative powers,
- configuration of the system, including the security configuration,
- the data processed in the data systems that are subject to legal protection within the scope required by the provisions of law.

Apart from the operations of the users and system elements, other events related to the functioning of the system can be entered:

- operations of users who do not have administrative powers,
- system events that do not have a crucial significance to the functioning of the system,
- events and the parameters of the environment in which the ICT system is operating.

The information is kept in the logs from the moment of its entry for a period specified by separate regulations or for two years if the period is not provided by separate regulations.

The entries to the logs can be stored in external IT carriers in conditions that provide information security. In justified cases the logs can be kept in a paper form.

Bibliography

[1] 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 Dz.U. (Journal of Laws) No. 100, item 1024)

[2] Ordinance of the Council of Ministers of 12 April 2012 on the National Interoperability Framework, minimum requirements for public registers and information-sharing in electronic formats and minimum requirements for ICT systems (Journal of Laws) 2012, item 526
[3] Act of 15 April 2011 on medical activity , Dz.U. (Journal of Laws) 2011 No. 112 , item 654
[4] Act of 17 February 2005 on computerization of activities of entities implementing public tasks. Dz.U.(Journal of Laws) 2005, No. 64, item 565
[5] Act of 2 July 2004 on freedom of business activity , Dz.U. (Journal of Laws) 2010, No. 220, item 1447 (as amended)
[6] Act of 29 August 1997 on personal data protection, Dz.U. (Journal of Laws) 2002, No. 101, item 926

Abstract

Medical data include personal data and particularly the data that is particularly protected, i.e. sensitive data. Such data is subject to special legal protection that requires adequate security procedures. The article presents several requirements that regard the obligation to apply security procedures and other standards that are required for ICT medical systems. It points out to the fact that the majority of such obligations refer also to health data processing in resources that are shared in the cloud. The article also presents requirements concerning personal data security as well as the responsibilities related to the implementation of standards applied in the ICT systems that are the basis for cloud computing. The information security management system discussed in the paper must constitute an essential element of ICT systems, including the ones that are based on the cloud computing model.