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

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

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

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

NEW TECHNOLOGIES – AVAILABLE INSTITUTIONAL AND SOFTWARE MEASURES TO PROTECT MEDICAL DATA

Introduction

The article discusses the impact of some new technological solutions on the security and confidentiality of medical data and presents possible institutional and software measures that support healthcare in the assurance of appropriate medical data security in compliance with the new regulations.

Devices that monitor patient's life parameters and other numerous telemedical solutions generate a significant amount of medical data that is subject to protection. Trade and telecommunications secrets may constitute a certain security system. The article discusses the development principles of IT systems: *privacy by design* and *privacy by default*, the new e-privacy regulation and codes of conduct as the elements that help improve the security of medical data. It also presents the role of risk assessment and software audit in healthcare entities with regard to personal data security.

1. Medical equipment – the Internet of Things vs. data security system

Data security system in healthcare must consider the security of all kinds of devices that are necessary for the functioning of modern healthcare entities and frequently communicate

with one another through Wi-Fi networks. This type of systems is often a part of the Internet of Things (IoT). The term refers to devices that are used to collect, process and automatically share the information that comes from different resources (from sensors, mobile devices and machines)[1].

There are numerous devices in healthcare that support patient treatment processes and share data at the same time. They include remote monitoring systems of patient life parameters that use medical measuring devices and online data transmission (either audio or video). These are, among other things, systems to monitor such parameters as blood pressure, heart rate, oxygen saturation, body temperature, lungs capacity and blood glucose level. The collected data is transmitted to the doctor.

One of the interesting solutions may be the application of silicon microchips that are placed in pills, which helps monitor patients' intake of prescribed medicines. Moreover, new solutions include implanting programmable-bio-nano-chips to detect heart diseases or cancer markers from patient saliva. Such implant could constitute an early warning system before any symptoms are discovered by the patient[2].

The majority of these complicated devices process personal data and simultaneously communicate with the servers that are used not only by doctors but also by manufacturers or distributors. Thus, the issue arises on the selection of an adequate data controller.

In the case of IoT, there is a clear differentiation by the following criteria:

- who developed the system;
- who developed the devices;
- who manages the information;
- who is the user.

Article 29 Working Party, which is an advisory body for EU institutions[3] issued an opinion[4] on IoT. The document admits that the data generated by IoT devices may be considered personal data. Thus, the producers of such devices and software developers may as a rule be considered personal data controllers. Consequently, they will have obligations resulting from the UE and

[1] K. Chylińska, *Zastępca Europejskiego Inspektora Ochrony Danych Osobowych: Nowe technologie – Internet rzeczy*, http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/ (accessed 04.2018).

[2] E. Kwiatkowska, *Rozwój Internetu rzeczy – szanse i zagrożenia*, http://www.wz.uw.edu.pl/pracownicyFiles/id26574-6.0_Rozw%C3%B3j_internetu_rzeczy_-_szanse_i_zagro%C5%BCenia%5B1%5D.pdf (accessed 04.2018).

[3] Established under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995

[4] Opinion 8/2014 of the Article 29 Working Party on the recent developments on the Internet of Things (WP 223), https://giodo.gov.pl/pl/1520203/8646

national regulations on persona data protection while IoT users should be informed on who is processing the data. They should also express their consent for such processing if required by the regulations.

The opinion also concentrates on technological issues. Most of the sensors on the market are not capable of using the encrypted communication link as the computing requirements have an impact on the device effectiveness that is limited by its low-power batteries.

The opinion particularly emphasizes the fact that persons whose life activities are monitored should express their consent. It is indicated that recording devices, as in the case of *Quantified Self*[5], mainly record data concerning individual's wellbeing. They do not necessarily concern health but they may promptly provide information on individual's health as they are recorded in real time. This makes it possible to make conclusions from the changes in health in a given period. Data controllers should predict the possible change and take necessary steps.

Hacking attacks on diagnostic equipment and life support devices enable the theft of the collected data, its sales and the control over the devices. This will particularly pose a threat to the advanced equipment which protects people's safety. Thus, such devices should be provided with security measures that would protect them against breaking-in and ensure the encryption of the transmitted data. Moreover, there are doubts concerning who should have the rights to the data generated by sensors as they may be an attractive product on the market. The rights to such data should be granted to IoT users, the owners of data collection platforms and the device producers[6].

2. Trade secret

Trade secret means „publicly unavailable technical, technological and company organizational information or any other information of commercial value to which the trader has taken the necessary steps to preserve their confidentiality"[7]. Trade secret binds employees, persons that provide services under civil law agreements and supervising institutions. A new

[5] Also known as lifelogging , is a specific movement by Gary Wolf and Kevin Kelly from Wired magazine, which began in 2007 and tries to incorporate technology into data acquisition on aspects of a person's daily life. People collect data in terms of food consumed, quality of surrounding air, mood, skin conductance as a proxy for arousal, pulse oximetry for blood oxygen level, and performance, whether mental or physical. Wolf has described quantified self as "self-knowledge through self-tracking with technology".

[6] D. Koseła, *Internet Rzeczy – rewolucja technologiczna i nowe wyzwania dla prawników*, http://bpcc.org.pl/pl/publikacje/internet-rzeczy-rewolucja-technologiczna-i-nowe-wyzwania-dla-prawnikow (accessed: 04.2018).

[7] Notice of the Marshal of the Sejm of the Republic of Poland of 9 February 2018 on the announcement of a consolidated text of the act on combating unfair competition, Art.11 item 4 (Journal of Laws 2018, item 419).

definition of trade secret has been provided by EU regulations[8], which will soon result in the amendment of the above definition. Pursuant to the new wording *trade secret* refers to technical, technological and company organizational information or any other information of commercial value which is not as a body or in the precise configuration and assembly of its components, generally known among, or readily accessible to, persons that normally deal with the kind of information in question, and has been subject to reasonable steps by the person lawfully in control of the information, to keep it secret[9].

The disclosure of a secret may result in criminal liability of the infringer when the disclosure causes a considerable damage and the infringer discloses the information despite his/her duties to the trader. Moreover, there is criminal liability of persons who unlawfully acquire a trade secret and disclose it to a third party or use it in their own economic activity.

Internal rules of procedure, confidentiality agreements and competition clauses are the most common trade secret regulations. It is a common practice that an employee, when entering into a job, signs regulations that clearly define company procedures – also the ones on handling information. The provisions of the regulation oblige employees to follow the rules. Besides that, traders tend to choose other form of trade secret protection[10].

The issue of patient data secrecy is dealt with by numerous regulations that regard healthcare areas which are regulated by separate legal acts, e.g. mental health, occupational medicine.

Moreover, the healthcare sector involves secrets that are related to the operations of particular institutions, for example eWUŚ[11] (Electronic Verification of Eligibility of Beneficiaries). Health data are also subject to statistical confidentiality, social worker confidentiality and confidentialities that are related to other operations which involve lawful health data processing.

[8] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Official Journal of the European Union L 157 of 15.06.2016, p.1).

[9] 9 June 2018 is the deadline for the implementation in Poland of the Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[10] *Tajemnica przedsiębiorstwa a zakaz konkurencji*, https://poradnikprzedsiebiorcy.pl/-tajemnica-przedsiebiorstwa-a-zakaz-konkurencji (accessed: 04.2018).

[11] Regulation of the Minister of Health of 20 December 2012 on the conditions for applying for e-documents that confirm the right to healthcare services, par.3.3 item 2b. (Journal of Laws 2012, item 1500).

3. Telecommunications secret

There are areas that are not directly influenced by persons responsible for data security in healthcare institutions. Every electronic document which is transferred to other entities through ICT networks, including the ones that contain patient health data, can be controlled by the entity that generated it only until it is present in the entity's system. If it is transferred to other entities, e.g. via e-mail, the process can be controlled in the course of the transmission only by the network operator and other legally authorized institutions. These entities are obliged to telecommunications secret.

The secret includes:

1) user data;

2) the contents of particular messages;

3) transmission data, i.e. data that is processed to transmit messages in ICT networks, including all location data, i.e. data that indicate the geographical position of the end-user of publicly available ICT services.

The entities that participate in the provision of ICT services in public networks and the entities that cooperate with them are obliged to telecommunications secret. They are also obliged to observe due diligence in the scope justified by technical or economic conditions while securing ICT devices, networks or data sets against the disclosure of telecommunications secret. A person coming into possession of a message not intended for him/her when using a radio or end-user device equipment should keep telecommunications confidentiality[12].

4. Secrecy related to entity control

The obligation to secrecy also applies to entities that are allowed to control personal data in an entity, healthcare entities including. It is conducted by the Minister of Health within an audit provided by law through persons who are obliged to keep professional secrecy. The President of the Personal Data Protection Office (UODO) is subject to restrictions as regards legally protected data. There is a possibility for a party in data breach proceedings to restrict the President from information, documents or their parts that include trade secret. In such cases, the party is obliged to present the UODO President with a document version without the information subject to restriction.

[12] Telecommunications Law of 16 July 2004,(Journal of Laws No.171, item 1800 as amended)

5. Principles of *privacy by design* and *privacy by default*

The above issue is related to the GDPR principles of personal data processing - *privacy by design* and *privacy by default*. According to the first one, data protection should be embedded into the system at the stage of designing the system for personal data processing (procedures, documentation and hardware) and into the processing system itself. As a result, already at the time of designing the system, the applications or the system and at the time of applying them in data processing, the data controller is obliged to ensure appropriate technical and organizational measures to protect the data. Practically, the principle consists in the necessity to predict and prevent possible problems regarding data protection at the preparation stage of particular system solutions with the obligation to evidence the decisions. Consequently, the following criteria have to be considered:

1. minimization – the volume of the collected data is limited to the indispensable minimum;
2. concealment –data and the relations between them are not visible to persons that have access to them (additional operation to have the access to the data)
3. separation – processing data that is separated and dispersed in particular sets;
4. aggregation – processing the data in the highest possible degree of aggregation[13].

According to the latter principle, processing can be done by default only for personal data that is necessary to accomplish a particular purpose of processing. In other words, data protection must be active by default without the necessity to take decisions by data subjects. The measures applied should ensure default settings that enable the protection of the processed personal data. Practically, in line with this principle, making personal data available to an unspecified number of other persons by a user of an application, system, program or service is possible only after a modification of default settings by the user.

6. Codes of conduct as an option for a data security system

One of the key aspects is- together with the new rights and obligations that are introduced by GDPR with regard to the security of personal data processing –the acceptance of the adoption of the codes of conduct by associations and other entities representing particular

[13] A. Wolanin, *Privacy by design - nowa zasada planowania przetwarzania*, https://www.rodokompas.ostrowski-legal.net/single-post/2018/01/22/privacybydesign (accessed 04.2018).

categories of data controllers or processing entities (e.g. medical sector). The rules in the codes express a self-regulation policy in a given sector although they have a legal status that results from their formal acceptance by a supervising body. Consequently, when a medical institution complies with the regulations of its code of conduct, it indicates that it complies with the GDPR regulations.

In practice, the managers of medical institutions obtain a document that makes it possible to make an optimal choice with regard to data security in compliance with GDPR. The document indicates how to select technical and organizational measures in order to introduce safeguards adequate to the financial capacity of the entity. The document can be applied by all healthcare entities – irrespectively of their legal and ownership structure, the founding body and the way how healthcare services are provided (financed from public means, commercial)

7. e-Privacy Regulation

GDPR is the only legal regulation that will have an impact on all data subjects. e-Privacy is to supplement GDPR regulations and be a lex specialis to the cases when the data acquired in the provision of communications services are personal. The regulation does not only protect the privacy of natural persons (as it is the case of GDPR) but its provisions also apply to legal persons.

The objective of e-Privacy is to increase the privacy of persons and entities that provide services (including medical services) through the monitoring of all end-user devices such as smartphones or laptops that are used by them. This can be done by:

- the increase of requirements as regards end-users consent to use the information about their equipment or the information stored in their devices (e.g. within the scope of consent on data storage with the use of cookies); this also applies to the use of information for marketing purposes;
- the increase of transparency as regards cookies;
- the correlation of e-Privacy provisions with the GDPR;
- the protection of metadata, including the information on geographical location, duration of calls and the websites visited;
- the obligation to provide the calling line identification (the prefix) for marketing calls;

- administrative fines for non-compliance with the provisions of the regulation up to 20 000 000 EUR or up to 4 % of the total worldwide annual turnover [14].

The regulation protects (e.g. data confidentiality obligation) electronic communications data. This does not only refer to the data that is acquired in relation to the provision of traditional communications services but also the information related to the new, Internet-based services that facilitate communication, e.g. VoIP, Internet communicators, on-line e-mail services (i.e. OTT, *Over-the-Top communications services*).

Electronic communications data means all the information that is exchanged or transferred (electronic communications content) and the information concerning end-users, including data to trace and identify the sources and destination of a communication, geographical location, time, duration and the type of communication.

The protection also covers metadata as data that may directly reveal highly sensitive information such as habits, activities of everyday life and social relationships. Metadata include the numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call, etc.

The regulation concerns data to the extent it is available through communications networks and provided to an undefined group of users (e.g. public hotspots). However, it does not apply to company networks that are available only to the users of one organization.

The regulation is also applicable to the transmission of machine-to-machine communications in cases when signals are conveyed over a network. This particularly concerns IoT-based solutions. The EU legislator provides for the possibility for a special regulation of appropriate security measures in this area by separate legal regulations.

8. Risk and security assessment in healthcare IT systems

Risk assessment is one of the crucial factors concerning information and data security in IT systems. Data controllers (the heads of healthcare entities) are responsible for the assurance of data security that is stored not only in the IT system but also in any other form. An IT system is secure when its user can rely on it and its software operates in compliance with the specification[15]. Nevertheless, even the most developed software with advanced security

[14] e-Privacy Regulation. *Większa ochrona użytkowników urządzeń końcowych (komputerów, telefonów, smartfonów, czy tabletów) przed nadmierną ingerencją w sferę ich prywatności*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/alerty-prawne/rozporzadzenie-eprivacy-przewodnik.html (accessed 04.2018).
[15] S. Garfinkel, PRACTICAL UNIX AND INTERNET SECURITY, ed. II., O'Reilly, 2003

elements is subject to human error as human is the weakest link in IT systems. Information security in IT systems is based on three fundamental parameters that are referred to as CIA (*Confidentiality*, *Integrity*, *Availability*)[16].

Confidentiality – data and services should be accessible only to persons, processes and other services that are authorized. The access to accounts and data is protected by user names, passwords, one-time passwords, encryption, etc. In more complex scenarios multi-step authentication is applied. Two other terms are closely related to confidentiality, they are – authentication, i.e. the confirmation of identity, and authorization, i.e. the confirmation of rights.

Integrity – data and services should not be infringed by unauthorized entities (persons, processes, services). Any attempts of such operations (either successful or not) should be detected and recorded. In order to achieve this, software audit, risk assessment and behavior monitoring should be conducted.

Availability – this principle concerns practically one but fairly significant condition: any authorized entity should be able to use the resources to the full extent of its rights. The assurance of availability is mainly within the responsibilities of the IT system administrator.

Security is not a state that is established once and for all; consequently it is impossible to introduce a system configuration that would ensure security for ever. Security is a continuous process which involves several operations on the part of the IT system administrator and other employees.

The basic security hazards can be divided into two types:

1. purposeful (desire for profit or appreciation , revenge),
2. coincidental (user's ignorance, negligence, naivety, hardware and software faults).

The assurance of security against coincidental hazards is the most difficult tasks as the responsible persons cannot predict what can be expected from system users and such external factors as flooding or fire. Thus, it is extremely important to perform security audits and risk assessments.

The significance of risk and security assessments is illustrated best by the two events presented below which occurred in the Polish and British healthcare systems.

In Poland, the personal data of patients and employees of a healthcare entity in Koło was stored in the servers that were not secured by a password. As a result, there was a leakage of

[16] A. Białas, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.

personal data of the personnel and approx. 50 thousand patients who were registered in 2003-2007.

As regards Britain, in 2017 there was a most significant attack on the British healthcare system. Everything indicates that the attack was possible only because the system update, which was developed and shared by the manufacturer, was not implemented. The event took place despite the fact that ICO (Information Commissioner's Office) policy was to impose severe fines on entities that did not implement the updates that were recommend by them. A few years before, an information was made public about a vulnerability in OpenSSL protocol, referred to as *Heartbleed*. OpenSSL protocols are used to secure online communications between servers and computers that are connected to the network. The security flaw was used by the *Anonymous* group and resulted in an unauthorized access to a dozen or so of employee mailboxes. They included over 30 thousand e-mails and some of them contained the staff sensitive data. Gloucester City Council was fined £100 000. It should be added that the vulnerability had been discovered almost immediately; however, further negligence resulted in a successful attack of the *Anonymous* group.

9. Software audit

Software audit is the company evaluation with regard to license management and legality of the software used. It is performed in all workstations and servers and provides detailed information about the installed applications and files that are stored on discs and which may not comply with company regulations and the applicable law. The software audit should give the answer to three basic questions whether the software is necessary, legal and its versions are updated.

The objective of the software audit is to bring order and to ensure the person responsible for company software that every program installed in the company is used in compliance with the license, that the number of programs reflects the real demand and the software is used to its optimum. It is recommended to perform the audit in appropriate stages (see: Figure 1). First, it starts with the classification of the software together with its use and the location of installation, this is followed by the description of the software and finally the license management. It is expected from the audit that it will:

- create an inventory of the software,
- prepare a list of the installed software together with the acquired licenses,

- manage security policies and procedures,
- develop a registration plan with the consideration of appropriate documentation.

Software audit may be related to hardware audit and the best moment to perform such audits is the so called zero audit, i.e. the inventory of software and hardware that is performed for the first time in a company. The basic benefits of the audit include:

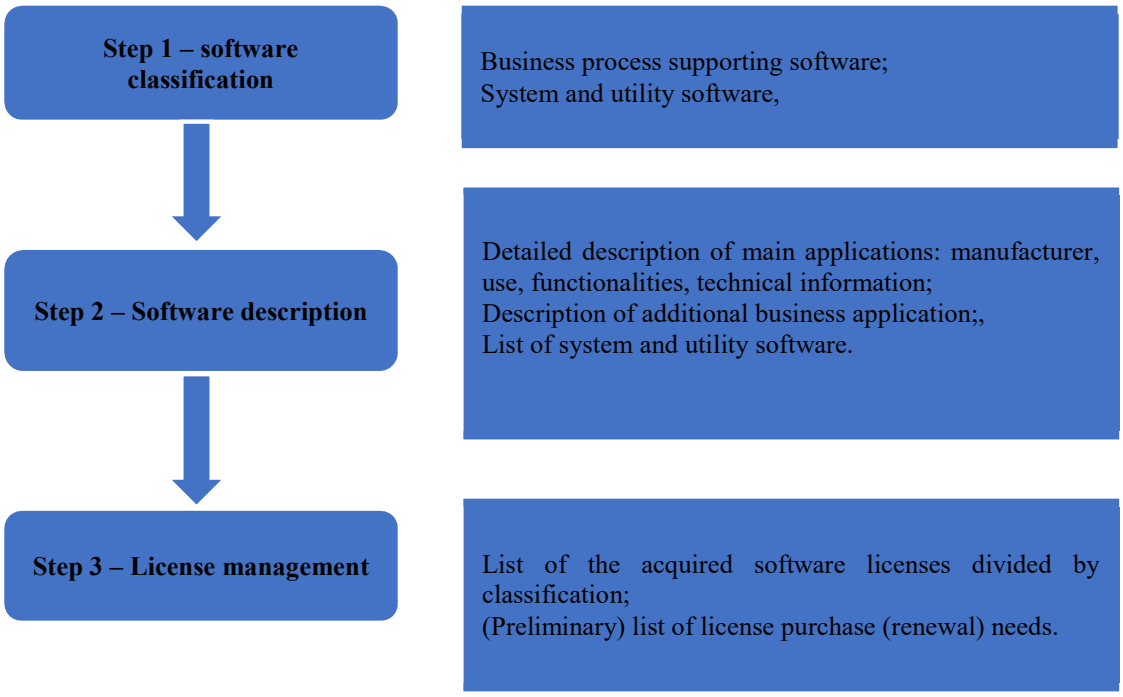
- financial benefits that result from a conscious use of the acquired software and the use of optimal purchasing options,
- optimization of software investment plans (purchasing software that is really needed),
- update of the licenses that are really used (which results in effective financial benefits for the whole company),
- reduction of technical support costs that results from the standardization and removal of unnecessary and outdated elements of the infrastructure.

An example of the inventory stages of software is given in detail in Fig. 1.

The software audit itself is not the same as the security audit of data stored in IT systems and risk identification and the analysis of hazards to health data security are its inseparable elements. The main objective of the risk identification is the determination of possible hazards that result from two basic areas:

1. human errors –caused by healthcare entity staff who do not follow the principles of security policy or by a faulty policy.
2. external errors –independent of humans or caused by wrongly estimated risks. They include such risks as server or entity flooding, fire, a theft of computers because of an inadequate security of premises.

Figure 1. Example of software inventory



Source: Authors' research.

Thus, healthcare entities that process health data, including health data of individuals, should have a written information security policy that is accepted by the management, made public and communicated to all employees and possible external parties. Due to the fact that security policy is a continuous process, it should be reviewed at least once a year. The frequency of the policy update depends on the size of the healthcare entity, however, the document update is necessary after a data security breach[17].

The elements of risk and management analyses should include numerous aspects, among them:

- identification of assets (to complete it, the above mentioned software audit is performed), threats and weaknesses;
- impact assessment on entity operations;
- hazard probability and system vulnerability evaluation;
- determination of the level of risk or of several security breach risks;
- comparison of current audits with the previous ones and identification of excess risk areas;

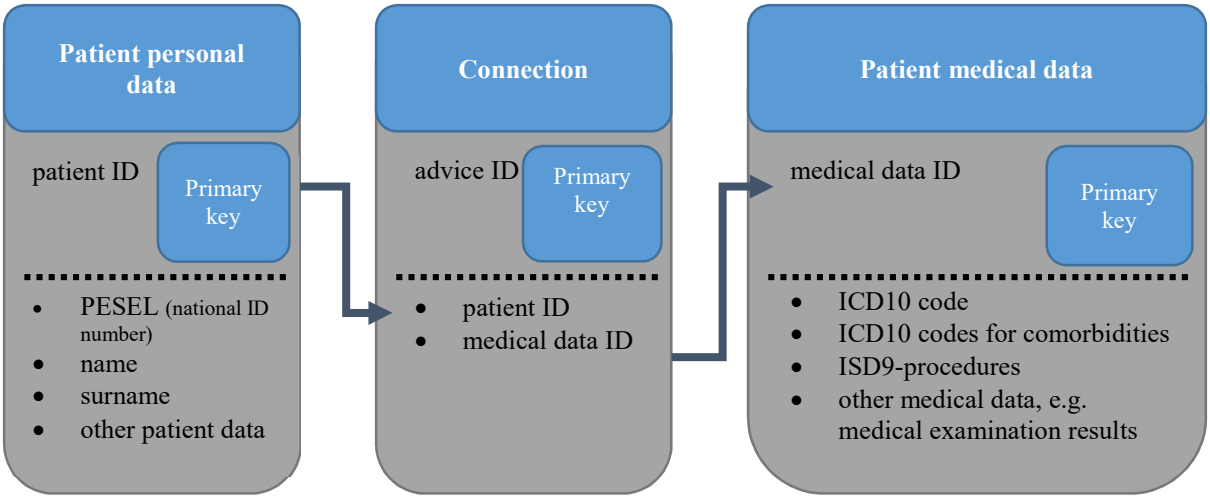
[17] ISO/IEC 27002: 2013; Information technology -- Security techniques -- Code of practice for information security controls

- mapping audit decisions.

One of the recommended methods of prevention against unauthorized access is to design applications in such a way that data separation should be ensured (see: Fig.2) [18]. There should be a physical and logical separation of patient medical data from patient personal (demographic) data. As a result, medical data are independent of patient personal data.

The separation of data in healthcare entities is presented in Fig. 2.

Figure 2. Separation of data in healthcare entities



Source: Authors' research.

Conclusions

Data generated by IoT devices may be considered personal data. Thus, the producers of such devices and software developers may as a rule be considered personal data controllers. Consequently, they will have obligations resulting from the UE and national regulations on persona data protection while IoT users should be informed on who is processing the data. They should also express their consent for such processing if this is required by the regulations.

The privacy by design and privacy by default principles consist in the necessity to predict and prevent possible problems regarding data protection at the preparation stage of particular system solutions with the obligation to evidence the decisions.

A code of conduct is a document that makes it possible to make an optimal choice with regard to data security in compliance with GDPR. It indicates how to select technical and

[18] Ibidem.

organizational measures in order to introduce safeguards adequate to the specificity and financial capacity of the entity. The mangers of medical institutions are given a kind of manual that facilitates the development of a personal data security system.

The objective of e-Privacy is to increase the privacy of persons and entities that provide services (including medical services) through the monitoring of all end-user devices such as smartphones or laptops that are used by them.

Security is not a state that is established once and for all; consequently, it is impossible to introduce a system configuration that would ensure security for ever. Security is a continuous process which involves several operations on the part of the IT system administrator and other employees. Risk assessment and software audit are significant elements of this process.

Bibliography

[1] Białas A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwa Naukowo-Techniczne, Warszawa 2006.
[2] Chylińska K., *Zastępca Europejskiego Inspektora Ochrony Danych Osobowych: Nowe technologie – Internet rzeczy,* http://blog.e-odo.pl/2015/10/17/nowe-technologie-internet-rzeczy/.
[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
[4] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Official Journal of the European Union L 157 of 15.06.2016, p.1).
[5] ISO/IEC 27002: 2013; Information technology -- Security techniques -- Code of practice for information security controls.
[6] Koseła D., *Internet Rzeczy – rewolucja technologiczna i nowe wyzwania dla prawników*, http://bpcc.org.pl/pl/publikacje/internet-rzeczy-rewolucja-technologiczna-i-nowe-wyzwania-dla-prawnikow.
[7] Kwiatkowska E., *Rozwój Internetu rzeczy – szanse i zagrożenia*, http://www.wz.uw.edu.pl/pracownicyFiles/id26574-6.0_Rozw%C3%B3j_internetu_rzeczy_-_szanse_i_zagro%C5%BCenia%5B1%5D.pdf.
[8] Notice of the Marshal of the Sejm of the Republic of Poland of 9 February 2018 on the announcement of a consolidated text of the act on combating unfair competition, Journal of Laws 2018, item 419.
[9] Opinion 8/2014 on the on recent developments on the Internet of Things, https://giodo.gov.pl/pl/1520203/8646.
[10] Regulation of the Minister of Health of 20 December 2012 on the conditions for applying for e-documents that confirm the right to healthcare services, Journal of Laws 2012, item 1500
[11] Garfinkel S., PRACTICAL UNIX AND INTERNET SECURITY, II e., O'Reilly, 2003.

[12] *Tajemnica przedsiębiorstwa a zakaz konkurencji*, https://poradnikprzedsiebiorcy.pl/-tajemnica-przedsiebiorstwa-a-zakaz-konkurencji.
[13] Telecommunications Law of 16 July 2004,(Journal of Laws No.171, item 1800 as amended)
[14] Wolanin A., *Privacy by design - nowa zasada planowania przetwarzania*, https://www.rodokompas.ostrowski-legal.net/single-post/2018/01/22/privacybydesign.

Abstract

The article discusses the impact of some new technological solutions on the security and confidentiality of medical data and presents possible institutional and software measures that support healthcare in the assurance of appropriate medical data security in compliance with the new regulations.

Data generated by IoT devices may be considered personal data. Thus, the producers of such devices and software developers may as a rule be considered personal data controllers. Consequently, they will have obligations resulting from the UE and national regulations on persona data protection.

The privacy by design and privacy by default principles consist in the necessity to predict and prevent possible problems regarding data protection at the preparation stage of particular system solutions with the obligation to evidence the decisions.

A code of conduct is a document that makes it possible to make an optimal choice with regard to data security in compliance with GDPR. Practically, the mangers of medical institutions are given a kind of manual that facilitates the development of a personal data security system.

The objective of e-Privacy is to increase the privacy of persons and entities that provide services (including medical services) through the monitoring of all end-user devices such as smartphones or laptops that are used by them.

Security is a continuous process which involves several operations on the part of the IT system administrator and other employees. Risk assessment and software audit are significant elements of this process.

Key words

Internet of Things, risk assessment, e-Privacy, software audit, GDPR, codes of conduct