Medical Data in the Digital Era - Legal Challenges Related to Providing Information Security, Applying GDPR and Respecting the Professional Secrecy

Krzysztof Świtała*
* Cardinal Stefan Wyszyński University/ Faculty of Law and Administration, Warsaw, Poland
k.switala@uksw.edu.pl

Abstract - **The processing of medical data in electronic form poses many challenges in terms of the security of these resources and ensuring patient privacy. This paper presents new dimensions of healthcare data processing, such as EHR, eHealth, mHealth, IoT or Big Data, in the perspective of the challenges of enforcing legal regulations to ensure the security of such healthcare information resources while also guaranteeing cross-border interoperability of these solutions. The technical and organizational measures applied by the controllers, as well as the legal requirements, should be consistent and comprehensive, considering not only the challenges related to the protection of personal data, but also cybersecurity and the protection of professional secrets in health care. In this context, ensuring the integrity and availability of information is also important as protecting its confidentiality.**

Keywords - eHealth, EHR, data protection, data concerning health, information security, cybersecurity, professional secrecy

I. INTRODUCTION

The protection of information processed in health care cannot be approached selectively. A coherent and comprehensive approach to ensuring the safety of such resources should respect the obligations under the GDPR, the 2022/2555 NIS2 Directive, instruments for legal protection of medical profession secrets and medical records, as well as other related regulations. No less important than ensuring confidentiality of patient information is to guarantee its integrity and availability. The processing of such resources should meet the appropriate standards of business continuity and be characterized by adequate quality guaranteeing that information is up-to-date and complete. It should be remembered that pecuniary or non-pecuniary damage associated with the loss of integrity of medical data used during a medical procedure or the lack of availability of these resources in the event of a life-threatening condition may be at least no less severe than the unauthorized disclosure of such information. Only such an integrated approach to this issue will allow for due respect for the rights and freedoms of patients as data subjects.

I The author acknowledges funding and support from the National Science Centre, Poland (NCN Preludium grant no. 2014/13/N/HS5/03523).

The purpose of this article is to identify the legal challenges associated with the processing of health data and to identify potential methods for increasing the effectiveness of regulations relating to ensuring the security of health data. Only such an integrated approach to this issue will allow for due respect for the rights and freedoms of patients as data subjects. The question whether the legal regulations relating to the protection of information resources in healthcare resulting from the GDPR and the NIS2 directive are sufficient to properly guarantee the information autonomy and patient's privacy should be answered.

II. MEDICAL DATA AND DATA CONCERNING HEALTH

The information on health condition obviously belongs to the matters linked to the private life of an individual [1], constituting the emanation of their rights to information privacy and self-determination, whose enforcement should be appropriately protected by legal, organisational and technical safeguards. Data concerning health are qualified as a particularly protected category of sensitive data laid down in Article 9 GDPR and related directly to the individual's sphere of intimate life. As such, the loss of their confidentiality may cause the feelings of shame, embarrassment, and restraint. It is worth adding that the ISO 29100 standard relating to the framework for the protection of privacy in organizations extends to data related to human health to sensitive personally identifiable information data requiring special precautions [2]. This confirms the need to take special care of such categories of data.

Therefore, any misuse of these special categories of personal data could have more severe consequences on the individual's fundamental rights related to the protection of privacy and information self-determination [3]. It is worth adding that in Poland, as in most other states, such data resources are also covered by the scope of medical professional secrets. It is the experts' opinion on Article 29 Working Party that all EHR data shall be treated as particularly protected [4]. The application of such an approach allows to unify the principles for the resources protection in health records systems, eliminating problems related to the occurrence of weak links in the security

systems and no consistency in the safeguards used. It is a guarantee of proper protection of such resources and data subjects' privacy.

Recommendation CM/Rec (2019) 2 explicitly indicating that health-related data reveal information about a person's health status and this kind of data also includes information on the provision of health services. The explanatory memorandum to the above-mentioned document indicates that the data cover all information relating to the identification of the patient in the care system or the method used for gathering and processing health data, all information obtained during a medical check-up or examination, including biological samples and genome data, all medical information such as an illness, a disability, a risk of illness, clinical, physiological or biomedical information or information concerning medical treatment, irrespective of its source, as well as all data, refer to an individual, generated by professionals practising in the medical welfare sector [5]. This category of information resources should also include data on individual predispositions and health risks related to a specific person [6]. These resources may be associated with a specific health context (such as presence in a region affected with disease) or be the result of a "self check" survey where symptoms specific to a particular disease are given [7]. Conclusions of the CJEU in the Lindqvist [8]. case confirmed the possibility of using such a wider interpretation of the concept of health-related data.

The "data concerning health" term, as known from Article 4(15) GDPR, is also defined in an analogous manner as health-related data. The terminological inconsistency that appears here, referring to similar terms, i.e. health-related data and data concerning health with identical scope, deserves criticism. The notion "personal health information" was also identified in ISO 27799 standard as information about identifiable person that relates to the physical or mental health of the individual [9], which is consistent with health definition proposed by World Health Organization. In this sense, health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity [10]. Thus, this needs to be understood that the analysed meaning of personal health information is to a large extent analogous to the earlier presented normative expression of data concerning health laid down in the GDPR. Besides sensu stricto data concerning health, patient's identification data (a number, symbol, or particulars assigned to an individual to uniquely identify the individual for health purposes) have also been included in this particular category. Attention should also be drawn to the essential link of health information, thus understood, with the data of the person - medical service provider - providing services to a given patient. Furthermore, the personal health information does not include information that, either individually or in combination with other information available to the holder, is anonymized so that the identity of the individual who was the subject of the information cannot be ascertained from the information. Such resources are called sensu largo medical data.

Therefore, it should be considered appropriate to depart from the narrowing of medical data by limiting it only to information about the health status of a specific person. The term also includes resources processed in healthcare other than personal data, such as anonymized research and statistic data, information about health conditions for the population, medical knowledge, as well as know-how. The leading value that determines the protection of data concerning health is the privacy and intimacy of the data subject. With regard to other data processed by healthcare institutions, the security of these resources is primarily provided to ensure appropriate development for medical sciences, healthcare sector and the medical industry in order to maintain and systematically improve the health condition of the population, as well as to guarantee its safety.

Attention should be drawn to inextricable links between medical and genetic data. It is often impossible to put a clear dividing line between their scope. For instance, recital 35 of the GDPR clearly indicates that data concerning health also includes information derived from genetic data [11]. Undoubtedly, such resources qualified in the GDPR for specific categories of data, due to their information potential regarding the ongoing assessment and prediction of the health status of a particular person and their relatives, require care for security appropriate to their nature and specific risks for privacy [12]. Firstly, anonymized genetic data may in the future re-identify a person by recognizing new relationships between them [13]. Secondly, the identification capacity of these resources and their ease of processing in a digital environment can pose potential threats related to identity theft [14]. Finally, the significant value of genetic data in the context of profiling processes may lead to exclusion and discrimination of specific groups of individuals by predicting their personal characteristics and health status.

III. NEW DIMENSIONS OF PERSONAL DATA PROCESSING IN HEALTHCARE

A. The role of a common approach to ensuring information security in healthcare

The processing of medical data takes place not only in an automated way or in filing systems, including health records. Healthcare professionals share oral information about specific patients or make ad hoc notes about the treatment process. These information resources are used not necessarily for purposes related to treatment processes, but also for research aims and health policy management. Furthermore, some entities performing medical activities are operators of essential services, which entails additional obligations related to their securing. The actions implementing them should be complementary to the approach to protection of other information resources in such an entity (personal data, secrets of medical professions). The importance of ensuring information security in the context of privacy protection in organizations is mentioned by the ISO 29100 standard. Therefore, it seems reasonable to apply a comprehensive approach to information security in entities carrying out medical activities, taking into account legal requirements in

the scope of personal data protection, medical profession secrets and cybersecurity.

The special categories of personal data that include health data relate not only to the sphere of privacy but also to human intimacy. The effects of unauthorized interference in the latter sphere make it difficult to reverse effects on a person's personality and undermine his or her sense of security for a long time. In the case of electronic data processing, the risks associated with such an incident are significantly higher than in an analogue environment, due to the complicated structure of data sets and network protocols, which is a source of ever new vulnerabilities.

B. Security of eHealth, mHealth and Internet of Things solutions

ICT and the Internet network have already penetrated into many social and economic life areas. One of them is the healthcare sector, in which patients, medical personnel and public institutions use these tools to implement treatment or broadly understood objectives of healthcare policy and healthcare management [15]. In WHO documents, eHealth is presented as the use of ICT in healthcare [16]. Undoubtedly, the eHealth systems, which make it possible to implement health services in a new model, along with their provision at a distance, require special standards for patients' personal data processing, the specificity of these solutions taken into account, and being adapted to new categories of threats [17]. The eHealth notion is closely related to the issues of patient's remote care [18]. In healthcare environment such technologies are hallmarks of high quality services and for this reason they are naturally accepted by patients despite some interferences in their privacy [19].

Modern patient care processes currently use not only traditional computer systems and networks, but also Internet of Things and mHealth solutions. The WHO defines these technologies in its documents as medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices [20]. In European Commission documents Internet of Things solutions refer to "a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network" [21]. Solutions of this kind are particularly useful for improving the situation of those with chronic diseases (diabetes and heart disease) and the elderly. As a result of using IoT technologies, they could be subject to constant health monitoring which, in the event of a sudden deterioration of medical indicators, would trigger an automatic call for help for the patient. Such tools allow for decentralization of treatment and diagnostics processes - through electronic personalized devices connected to the network, some activities in this area could be performed in relation to him at his home or workplace.

Besides obvious benefits of the widespread use of mHealth and IoT solutions in healthcare, one should not forget about the threats that may exploit the vulnerabilities of communication protocols, such as Bluetooth, to loss of confidentiality, data integrity and raise the possibility of identity theft [22]. Strongly symmetrical and asymmetric cryptographic algorithms with appropriately long and complex encryption keys are relatively rarely used in communication between such devices. It is also important to provide adequate technical and procedural guarantees that the user of such solutions will be properly informed of the extent to which are affect his information autonomy [23]. The mHealth and IoT technologies should be configured, even at the price of a certain reduction in their performance and universality, to ensure proper respect for values such as privacy.

C. Role of automated information processing and Big Data in healthcare

Automated processing and profiling derive not only information of the health situation of a particular patient, but also identifies a new and not fully recognized health threats to the population. In the latter case, whenever possible, anonymized or pseudonymized data should be used. The development of automated processing methods facilitates rational decision-making in healthcare. For example, such technical solutions in conjunction with artificial intelligence algorithms can be used to medical digital images recognition in diagnostic procedures [24]. Appropriate data analysis allows for greater resources usage optimization as a result of its better allocation, which eliminates waste, improves savings and the efficiency of business processes [25]. However, it is necessary to strike a proper balance between the values associated with the effective implementation of health policies or the management of an individualized treatment plan for a particular patient - in relation to the preservation of the essence of his or her privacy and information autonomy. It is of particular importance here to prevent patient discrimination based on health condition, which was determined on the basis of automated profiling methods. In accordance with Article 22(4) GDPR for special categories of personal data, making decisions based on automated processing, including profiling, is permissible if the patient's consent is obtained or is necessary for reasons of substantial public interest and on the sufficient legal basis. It seems that the last of these premises will apply, for example, in cases of epidemics and the need to respond quickly to its negative results on society in order to prevent irreversible serious effects on public health. Pursuant to Article 35(3)(a) GDPR, the data protection impact assessment is performed for the processes of systematic and extensive evaluation of personal aspects, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects. The proper conduct of this procedure is of particular importance for maintaining satisfactory security level of special personal data categories, including data concerning health [26].

The concept of Big data refers to data sets characterized by the attributes of volume, velocity, variety and veracity, as well as values that are explored to discover such relationships between resources and new phenomena which have not yet been observed. It can therefore be concluded that these large databases are somewhat an "ocean of data", while the associated methods of analysis are "types of nets and fishing strategies" [27]. Big data is a source of new economic values as well as social and technical innovations

[28]. Analysis of large data sets not only makes it possible to effectively implement treatment processes using evidence-based medicine, which allows for deeper understanding of patient disease patterns. These technologies also support the development of a series of important strategic industries related to the national economy, people's livelihood, and national security [29]. The European Commission indicates that health records, gathered in a European perspective, can lead to better treatment of major chronic conditions and help to improve equal access to high quality health services for citizens [30]. Large data sets are not only a source of information about the phenomena observed in the present time, but are also the basis for precise forecasting of future trends and potential changes in environment. This allows us to react to possible negative situations in such a scenario that their effects are counteracted, in a way, ex ante, i.e. before they occur.

IV. Legal challenges related to the new paradigm of medical data processing

A. The importance of consistent and effective organizational and technical security of medical data

The use of personal data security measures relevant to privacy threats has a positive impact on the effectiveness of legal standards related to information processing. The ECHR jurisdiction has drawn attention to the importance of the adequate protection of medical records to respect the rights of data subjects. In case I v Finland [31], the Court found Finland to have violated its positive obligations to secure respect for private life pursuant to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, due to its failure to apply appropriate guarantees, through organizational and technological measures, the confidentiality of patient personal data in a public hospital. The Court of Justice of the European Union in its case law also takes into account these security solutions - as necessary elements of implementing the right to data protection that prevent accidental loss, alteration or unlawful erasure of these resources [32]. In order to guarantee an appropriate level of personal data protection, in addition to the implementation of purely legal obligations, it is also necessary to apply appropriate organizational, physical and technical security measures adequate to the risks associated with these assets.

Most of data handled in healthcare regardless of the form and place of processing should be subject to consistent rules guaranteeing their security. A holistic view of the issue of protecting information resources in healthcare, where gaps and the weakest links could be eliminated, not only allow for proper respect for patients' right to privacy, but will also help to improve the functioning of the processes of the entire sector by creating conditions for making decisions based on up-to-date data-driven reliable evidence.

As indicated in recital 35 of the GDPR, obligations arising from this act do not apply to identifiable data that relate to the deceased. Member States may provide for rules regarding the processing of personal data of such persons. Moreover, the medical professions secrecy guarantees the protection of patients' data not only during their lives but also after death. Protection in the medical sector of information concerning the deceased person is related to the specificity of the doctor-patient relationship based on trust, assuming respect for the patient's privacy and autonomy. This means that proper and lawful security of information resources processed in medical records cannot be based solely on the GDPR requirements.

B. Ensuring business continuity as a challenge for legal regulations

Secure information is characterized by its confidentiality, integrity and accessibility attributes. In the legal context, their behavior is guaranteed by the regulations contained in the GDPR and standards of the NIS Directive. The differences relate to the scope of protected information and the purposes of both regulations. The GDPR refers to the protection of filing systems and the processing of personal data due to the protection of the data subject's rights and freedoms. In the case of provisions from Article 21 (2)(c) of the NIS2 Directive, the business continuity of essential and important entities activities is protected by guaranteeing the proper functioning of information systems, which, in addition to personal data, may include resources such as know-how, technical data, financial and accounting data, etc., as well as software and hardware used to process them. Therefore, it seems that the basic assumption of these regulations is not competition, but their mutual complementation and the synergy effect that can thus be obtained.

Maintaining business continuity is of particular importance in healthcare units where it is necessary to guarantee stability and constant availability of treatment processes. Modern evidence-based medicine is based on the use of data processed via ICT, which should be characterized by reliability and high resistance to interference. With regard to personal data processing, both Article 32(1)(b) and (c) GDPR as well as the ISO 29100 standard indicate the importance of ensuring the availability of these resources in the event of the need for their use by an authorized user. This will allow patients to have constant access to quality-stable health services.

C. Role of legal guarantees ensuring the quality of medical data

As accurately pointed out by M. Safjan, in the contemporary information society, an individual can be simultaneously a beneficiary and a victim of modern information processing technologies [33]. From the point of view of challenges related to the use of ICT in healthcare, ensuring the quality of data is an important factor. Such resources processed in these solutions should be integral and accessible to authorized entities.

The principle of accuracy and quality enshrined in Article 5(1)(d) and ISO 29100 assumes that properly protected information throughout its entire life cycle should be accurate, complete, up-to-date, adequate and relevant for the intended use. The quality of information referring to the definition in ISO 9000 is the degree to which a set of inherent characteristics (confidentiality, integrity, availability, authenticity, accountability, non-repudiation, reliability) of these resources fulfils the requirements in healthcare business processes arising from the needs of its actors (patients, doctors and other healthcare professionals, scientists, government).

In the case of medical data, it is just as important as its confidentiality to preserve quality factors - the integrity and availability of such information resources. This means that it is equally important to safeguard against unauthorized access to guarantee the continuity of medical data processing. Unavailability of these resources may threaten more than just violation of the right to privacy of a person - this situation may pose a genuine threat to his or her health and life. An example confirming the role of ensuring the integrity and accuracy of medical data used in treatment processes may be an event that is the basis for the Regional Court (pol. Sąd Okręgowy) judgment in Katowice dated 12.12.2003 [34], resulting from accidental connection in the hospital database by the medical secretary of diagnoses of two different patients, which resulted in a medical error consisting in performing an unnecessary surgical procedure mutilating the patient. Ensuring adequate quality of data has a significant impact on the achievement of health protection objectives. These resources play a role not only in the field of medical therapy, but also in scientific research and management of the entire sector. Undoubtedly, ensuring a satisfactory level of data quality and maintaining its stability are stimulated by properly formulated legal requirements imposed on health care entities.

D. Legal challenges related to the interoperability of medical data

EU documents define interoperability as the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems [35]. EU institutions support the process of eHealth systems interoperability improvement in cross-border healthcare. The e-health network was established in Article 14 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare. A further proposed legislative step in the EU concerning a common area for the exchange of medical data between Member States is the proposal for a regulation on the European Health Data Space (COM(2022)197). Achieving a satisfactory level of interoperability between EHR systems in EU Member States will allow for the necessary access for doctors and patients to a comprehensive medical history, which should contribute to improving the quality of health services provided. Ensuring respect for the right to privacy and the protection of personal data also plays an important role in these information processing activities.

There are differences in regulations regarding medical confidentiality between countries, which is undoubtedly a significant barrier to the cross-border flow of medical data. Article 29 Working Party indicated that the legal requirements for the collection, access to and cross-border transmission of data concerning health might not be the same in all EU Member States, taking into account the possibly distinct conditions, including limitations, especially the conditions arising from Article 9(4) GDPR, concerning the processing of such resources [36]. EU Member States also take different approaches with regard to the protection of patients' rights. In some countries it is expressed in terms of the individual rights of patients. Nonetheless, in others it is primarily an obligation imposed on healthcare entities [37]. For example, in France, legal protection of medical confidentiality is considered stronger than in most of other European countries [38]. This obligation, however, is not absolute and is based on the theory of will assuming that it results from the content of a contract between the doctor and the patient. The French courts verbally adhere to the concept of strict protection of medical secrecy and, at the same time allow exceptions where the essential interests related to the disclosure of information covered by this restriction of its dissemination significantly outweigh the reasons for maintaining their confidentiality [39]. While the differences in the subjective (healthcare professionals obliged to protect the privacy of their patients) - and objective (concerning all information that comes to the knowledge of healthcare professionals when practicing the profession) scope of regulation of medical secrets in EU Member States are not significant, the list of exceptions to confidentiality results from the content of legal instruments and case law of individual countries. The regulation of these issues in EU applicable law is rather vague due to the fact that it goes beyond the shared EU competences in the areas of internal market and common safety concerns in public health matters, for the aspects defined in the Treaty on the Functioning of the European Union. However, this does not prevent EU institutions from using coordinating competences related to protection and improvement of human health to support and issue soft law, encouraging Member States to gradually harmonize the principles of observing medical confidentiality in the context of interoperable cross-border processing of medical data. The proposed solutions should naturally be compatible with the legal provisions adopted in the GDPR and NIS2 Directive.

V. WAYS TOWARDS EFFECTIVE REGULATIONS OF MEASURES ENSURING THE MEDICAL DATA SECURITY

A. Role of technical standards in increasing the effectiveness of legal requirements related to the protection of personal data and information security

The use of technical standards from the ISO 27000 family - in particular ISO 27001 containing requirements for the Information Security Management System, ISO 27002 covering guidelines for the implementation of such a system, ISO 27701 supplements the privacy policy management system contained in those standards and ISO 27799 indicating the use of this standard may undoubtedly be useful for ensuring a high level of information security in entities performing medical activities for specific information security problems in healthcare.

A properly managed risk management process is significant for ensuring the validity of organizational and technical measures in the entity performing medical activities. ISO 27005 or specific-industry standards may serve as a reference point in this regard. The codes of conduct provided for in the GDPR should allow for a comprehensive approach to risk management in information security for entities performing healthcare activities. A properly carried out risk management process makes it possible, with naturally limited resources (financial, material, personal and time), to ensure the

optimal condition of information security in current conditions by implementing measures to reduce risks exceeding the specified level of acceptance.

Technical standards also describe approaches to maintaining an adequate level of privacy in an organization environment where information processing operations prevail. The ISO 29100 document characterizes the privacy framework, while the ISO 29134 being developed contains guidelines for Privacy Impact Assessment. These standards comply with the GDPR and supplement the standards of the ISO 27000 family.

A structured and comprehensive approach to ensuring business continuity in the organization guarantees the adaptation of the ISO 22301 requirements. Implementation of this standard ensures capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident. Business continuity management allows controllers access to data availability, and if they are also essential or important entities to apply such solutions, they are guaranteed to meet the requirements related to standards issued pursuant to Article 21 of the NIS2 Directive. Respecting standards of the sustainability of key information processes in an organization is particularly important in the healthcare sector, where disruption of access to data may result in a threat to such fundamental social values as patients' health and lives.

B. Vulnerability-driven approach to protection of information resources and related processes

It is good practice, not only from a medical point of view, but also in view of the management to prevent the occurrence of the causes of the problem, and not to focus solely on their effects. The earlier the vulnerability is reduced, the lower the potential likelihood and amount of costs of damage will be. In the field of technical protection of information processed in electronic form in healthcare, it is worth considering the development of industry-specific standards that will expand general approaches resulting from such knowledge bases as Open Web Application Security Project [40] sources or ENISA reports on the state of vulnerabilities [41]. Appropriate identification of vulnerabilities at the planning stage of specific personal data processing processes will allow for the most effective implementation of the privacy and data protection by design principles, as reflected in Article 25 GDPR.

The importance of vulnerability management in EU for effective information systems security has been highlighted in Article 12 of the NIS2 Directive. Information on these protection issues should be exchanged among competent entities in a secure communication environment both at a national and European level. Proper procedures in this area and efficient reaction to anomalies observed make it possible to reduce the risk of exploitation of identified vulnerabilities by threats, which may cause serious disruption to the activities of various entities. It should be mentioned that international technical standards, such as ISO/IEC 30111 and ISO/IEC 29417, refer to the management of this area of security and they should complement the legal regulations in this area. Sharing information about identified vulnerabilities in information systems enables a proactive and preventive approach to ensuring their security, unlike a reactive incident management model.

Pursuant to Article 25 of the GDPR, the vulnerability analysis should not be limited to the design phase of the processing activity, but should extend to its entire life cycle. Such a conclusion results from the content of Article 25 of the GDPR. The controller should identify and manage security vulnerabilities both at the time of the determination of the means for processing and at the time of the processing itself. This could be done not only on the basis of expert knowledge, but primarily on the basis of the analysis of empirical data from ISMS monitoring and related Intrusion Detection System/Intrusion Prevention System [42]. The latter tools are useful not only to detect the vulnerabilities of information resources, but mainly to identify threats directly affecting them.

It is necessary to manage technical safeguards life cycle. Cryptographic solutions (e.g. MD5 hash function [43]), they may no longer provide an adequate level of security. This is an effect of technological advances that allow these threats to bypass or break security, which undermines the effectiveness of information protection.

The hardware and software have vulnerabilities, the detection and disclosure of which is a continuous process. Some of them are identified by the threats (exploits) themselves for the first time (0-day vulnerabilities), which means that we would not find any advice or solutions in the available sources to counteract the effects of this incidents [44]. Working Party Art. 29 pointed to the growing importance for security of informing users as soon as possible about identified new vulnerabilities of IoT solutions [45]. The occurrence of such situations confirms the necessity for systematic hardening of the configuration of own information systems, which allows for self-improvement of the level of security of processed resources.

C. Role of documentation of the information security and personal data protection management system

Among the threats occurring on the Internet, the use of social engineering aimed at vulnerable users as well as Advanced Persistent Threat attacks is becoming increasingly significant. This means that the implementation of appropriate organizational solutions is no less important than ensuring physical and technical security of information systems. Properly maintained, structured and constantly updated documentation is their indispensable element. It contains not only the descriptions of procedures or current records but above all policies providing the framework for the information security management system functioning in the organization.

A consistent, comprehensive and current Information Security Policy, indicating the direction of management and support for security resources in accordance with business requirements and universally applicable regulations and other standards, should be the basic element of the information processing documentation in medical entities. The content of this document should make personnel, other cooperating entities and patients believe that their data are properly protected. It implements the principle of transparency resulting from Article 5(1)(a) of

the GDPR and expanded in Article 12. For this reason, the information security policy should be drafted in a language understandable to its recipients and should focus on the specific features of processing these resources in the organization. Such a document, which forms the basis for training in the organization and disseminating knowledge about data protection, increases awareness of threats and the methods of counteracting them in specific cases [46]. It leads to the creation and consolidation of a local proactive information security culture.

Information security policy may be uniform or may constitute a set of documents presenting selected thematic areas. Properly put in place and maintained policies are an important aspect of the implementation of the accountability principle laid down in Article 5(2) of the GDPR [47] and in ISO 29100 standard. This documentation describes the scope, limits, user roles and purposes of the personal data security management system functioning in a specific organization, which allows it to demonstrate the proper implementation of the other principles of protecting these resources [48].

According to the ISO 27003 standard, the content of the information security policy covers the following issues: scope, objectives, principles, key outcomes and related policies. The description of information security principles should refer to how they are implemented in a particular organization. The objectives of information security come not only from the content of legal instruments, but also relate to the nature of the organization's business activities and its mission. Moreover, this part of the policy confirms the implementation of the purpose limitation principle arising from Article 5 (1)(b) of the GDPR. Furthermore, the document should contain a list of key outcomes that will be achieved if the policy objectives are implemented, which will allow for evidence-based verification of its effectiveness. An appropriate adoption of the policies requires far more than the mere presence of these documents. In addition, the procedures for verifying the effectiveness of personal data security play an important role in the context of implementing the accountability principle. To sum up these considerations, the security policy may concern the information processes in the organization as a whole and create a comprehensive vision of their protection.

In a health care organization, not only information resources related to clinical, financial accounting and administrative processes should be properly protected, but also the documentation relating to the information security management system. Properly maintained documentation of information resources and personal data processing is a key organizational safeguard that allows the organization to demonstrate proper implementation of not only the accountability principle, but also the other principles arising from the GDPR. De lege ferenda EDPB and ENISA should consider formulating guidelines for maintaining documentation of information security management systems, with particular regard to the methods of its adequate protection. This proposal of the Art. 29 Working Party seems to be still justified for some controllers (such as individual medical practices) processing special categories of personal data, such as data concerning health. This will be a pattern for small entities to provide them with substantive support in implementing appropriate organizational security measures related to the specific characteristics of data processing.

D. Striking an appropriate balance between interoperability and information security

Ensuring interoperability is not only related to the effective implementation of business processes in the strict sense as a result of the effective exchange of data needed to implement such activities. At each of its levels, we should also consider taking into account the common standard of security-related exchange of health data. It is worth noting that in Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community, the concept of interoperability is understood as the ability of the rail system to ensure safe and uninterrupted train travel. In a similar vein, the interpretation of this term should promote the protection of health and privacy- to ensure the security of these information resources as well as the persons concerned is as important as achieving the purposes of effective processing health data.

The current level of ICT development allows for the implementation of the principle of time limitation by using cyclical tasks and triggers in databases containing electronic medical health records. These modern technical solutions have radically extended the data lifecycle, without its erosion as a result of forgetfulness and the promise of natural obliteration [49]. Therefore, a controller should have systematic procedures for data erasure embedded in the processing [50]. This effect can be achieved by using appropriately configured software, where the user's role is limited to exercising supervision over these processes.

There is a need for further debate on due measures for the observance of patients' rights with regard to interoperable cross-border exchanges of electronic health records, eHealth and telemedicine. Consideration should be given to further enhancing the role of trust services (eIDAS) in cross-border healthcare to guarantee authenticity and non-repudiation of health records exchanged between medical entities in the Member States. Such technical solutions allow patients to provide their medical consent in a secure way over the Internet. Particular emphasis should be placed on emergencies where information autonomy may be limited due to the risk to the health of the patient or other persons. In such a situation, however, full accountability of access to medical data should be ensured and the data subject would be guaranteed actual control rights over this process.

The confidentiality of information about patients in healthcare require effective protection. A controller is required to limit the number of those who can have access to personal data. This approach ensures the accountability of activities performed in EHR, thus facilitating the determination of responsibility for medical procedures confirmed by entries in this filing system. This is particularly important in the context of ensuring the patient-physician confidence not only in ICT itself, but primarily in medical data processing in which various health care entities are involved not only from a given EU Member State. Data exchange in cross-border healthcare requires

the accountability, authenticity and non-repudiation of related activities to preserve the confidentiality and integrity of these resources.

E. Principle of accountability and the privacy by design approach in relation to the concept of continuous improvement

Effective implementation by the controller of the accountability principle arising from Article 5(2) GDPR and the obligations related to appropriate protection of personal data processing activities pursuant to Articles 24 and 32 GDPR and the content of recital 78 should be based on the use of a continuous improvement approach. According to the ISO 27000 standard, it means recurring activity to enhance performance. This is an ongoing effort to improve key business processes in organization.

PDCA cycle is an iterative four-step (plan–do–check–act) model of process enhancement. It consists of the following phases:

- plan - includes formulation of goals, indication of actions leading to their achievement, together with the assigned resources;
- do - implementation of a previously established and approved plan;
- check - monitoring the changes introduced and observing deviations from the assumed indicators for the purposes;
- act - taking corrective actions in the event of significant deviations [51].

The application of this approach is characteristic of quality management systems based on the ISO 9001 standard and information security management implementing the requirements of the ISO 27001 standard. The issues of quality and ensuring information security are important aspects of the functioning of healthcare entities that use ICT solutions [52]. The PDCA continuous improvement cycle is compatible with the concepts of Privacy and Data Protection by Design due to compliance with their principles: Proactive not reactive approach, Privacy embedded into design and End-to-end security - full lifecycle protection [53]. These approaches to ensuring the security of information resources relate to the management of technical and organizational measures in healthcare and e-Health systems [54]. The DPIA process model has also iterative nature and review phase as PDCA. Moreover, the concept of continuous improvement is the foundation of IT system management methodologies such as COBIT, ITIL and ISO 20000-1. ISO 29100 also mentions the importance of periodic privacy compliance audits for information systems. This process enhancement model based on the PDCA cycle could also support the effective and proactive implementation of cybersecurity strategies in EU and its Member States [55].

As part of the process of continuous improvement of the ISMS based on the PDCA cycle, knowledge of data breaches and other cyber security incidents is used. It should be recalled that Article 33 GDPR (in relation to controllers) and Article 23 NIS2 (in relation to essential or important entities from the healthcare sector) introduce obligations to report incidents to supervisory authorities. Investigating the circumstances of an incident is part of the check phase, while action to counteract the effects of such incident is taken at the act phase. In the context of giving effect to the implementation of the approach based on continuous improvement and Privacy by Design, it is necessary to integrate the processes of improving the information security and personal data protection with the quality management processes in healthcare entities. Such a consistent approach to managing various areas of the organization's activities will allow for a synergy effect to be achieved.

F. Role of codes of conduct in healthcare

The use of soft law and self-regulation is a manifestation of a tendency to govern issues characterized by high dynamics of changes and relating to the boundaries between the legal system, business management and ICT. This approach is based on flexible instruments that do not manipulate the behavior of their addressees. Soft law solutions are not competitive but complimentary to universally applicable law.

Codes of conduct are used to organize the approach to ways and means of securing personal data in entities undertaking a similar type of activity. As recital 77 GDPR indicates, these are sets of guidelines for the implementation of appropriate measures and internal procedures to limit the risk of information processing and it is a way of demonstrating compliance with common legal and technical standards. Therefore, codes of conduct are voluntary accountability tools which set out detailed rules of data protection for controllers [56]. However, this should not be a one-size-fits-all approach where such seemingly versatile and universal document would apply to each and every healthcare entity. It seems reasonable to separate codes for hospitals, pharmaceutical companies, as well as individual and group medical practices due to the different nature and objectives of their activities.

A draft code of conduct on privacy for mobile health applications has been created for such ICT solutions in healthcare. It contains a description of the document (purpose, scope, governance model and enforcement), practical guidelines for software developers (consent management, application of data protection principles, fulfillment of the information obligation, data processing periods, security measures implementation, admissibility of advertisements, use of data for secondary purposes, transferring data to third parties, data breach response procedure, children's data handling) as well as a Privacy Impact Assessment template. The following principles of data processing are presented in the discussed code: purpose limitation, data minimisation, transparency, privacy by design and privacy by default as well as data subject’s rights. On 10 April 2017 Working Party 29 rejected this code due to its insufficient compliance with the GDPR requirements and the lack of added value in relation to Directive 95/46/EC [57]. Such a document should also guarantee appropriate enforcement mechanisms taking into account the data subject's rights [58]. However, this is an important attempt to develop a universal European standard for processing data concerning health via mobile devices.

Codes of conduct should not duplicate the content of legal instruments. Rather, they should complement them by

specifying the obligations imposed on the controller conducting specialized activities. It is also important to put in place effective mechanisms for independent verification of the requirements contained therein.

VI. Conclusion

In order to ensure an adequate level of information security in entities performing medical activities, it is not sufficient to merely comply with the scope of the GDPR and the national provisions of the NIS2 Directive. In this regard, national legal regulations relating to the protection of medical professional secrets also play a vital role. Undoubtedly, codes of conduct, industry-specific guidelines and technical standards can effectively supplement the requirements of the universally applicable law, thus ensuring an appropriate level of security of information resources processed in entities in the healthcare sector.

Maintaining information security, taking into account confidentiality, integrity and availability, requires the use of appropriate security measures tailored to the specificity of the activity of a given healthcare entity, which should be specifically oriented towards maintaining the continuity of the technical and organizational solutions used. It is possible to achieve this as a result of a properly implemented risk management process, taking into account the vulnerabilities of the resources processed by these entities to be protected.

In terms of the challenges related to the COVID-19 post-pandemic cyberspace environment and the aging of the societies of developed countries, the possibility of safe and effective exchange of medical data with due respect to patients' privacy is particularly important. Their interoperable uninterrupted data flow will enable the achievement of goals related to treatment processes and implementation of health policies.

Acknowledgment

The author acknowledges funding and support from the National Science Centre, Poland (NCN Preludium grant no. 2014/13/N/HS5/03523).

References

[1] Constitutional Tribunal judgement of 19 May 1998 (case K U 5/97), OTK of 1998, no. 4, item 46.

[2] ISO 29100:2011 Information technology — Security techniques — Privacy framework (ISO 2011) pp. 9.

[3] Article 29 Working Party (A29WP), Advice paper on special categories of data ("sensitive data")' (Ref. Ares(2011)444105, 20 April 2011) pp. 4.

[4] Article 29 Working Party (A29WP), 'Working Document on the processing of personal data relating to health in electronic health records (EHR)' (WP 131, 15 February 2007) .

[5] Explanatory memorandum to Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data (adopted by the Committee of Ministers on 27 March 2019 at the 1342nd meeting of the Ministers' Deputies) 4.

[6] Article 29 Working Party, Letter of 5 February 2015 to Paul Timmers (Director of Sustainable and Secure Society Directorate), Annex I – health data in apps and devices, Letter and Annex regarding health data in apps and devices, <https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf> accessed 19 January 2022, pp. 2-3.

[7] European Data Protection Board, Guidelines 3/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak (21 April 2020) pp. 4.

[8] CJEU Case C-101/01 Lindqvist (2003).

[9] ISO 27799:2016 Health informatics - Information security management in health using ISO/IEC 27002 (ISO 2016) pp. 3.

[10] This definition is based on Preamble to the Constitution of WHO as adopted by the International Health Conference, New York, 19 June - 22 July 1946; signed on 22 July 1946 by the representatives of 61 States (Official Records of WHO, no. 2, 100) and entered into force on 7 April 1948.

[11] Article 29 Working Party (A29WP),Working Document on Genetic Data (WP 91, 17 March 2004) pp. 5.

[12] W. Lowance, Privacy, Confidentality and Health Research, Cambridge University Press, 2012, pp. 111.

[13] D. Hallinan, M, Friedewald, P. De Hert, "Genetic Data and the Data Protection Regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data", Computer Law and Security Review, no. 29, 2013, pp. 322 - 323.

[14] E. Joh, "DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing", Boston Law Review, no. 91(2), 2011, pp. 672.

[15] J. Herveg, Y. Poullet, "Which Major Legal Concerns in future e-Health?" in P. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, V. Laurent (eds), The Information Society: Innovation, Legitimacy, Ethics and Democracy, New York: Springer, 2007, pp. 159-160.

[16] WHO, eHealth <https://www.emro.who.int/health-topics/ehealth/> accessed 5 July 2023.

[17] C. Dierks, "Legal and Social Responsibility in Health Service Chains" in B. Blobel, P. Pharow, M. Nerlich (eds), eHealth: Combining Health Telematics, Telemedicine, Biomedical Engineering and Bioinformatics to the Edge, Amsterdam: IOS Press, 2008, pp. 107.

[18] C. George, D. Whitehouse, P. Duquenoy, "Assessing Legal, Ethical and Governance Challenges in eHealth" in C. George, D. Whitehouse, P. Duquenoy (eds), eHealth: Legal, Ethical and Governance Challenges, Berlin Heidelberg: Springer, 2013, pp. 3.

[19] H. Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009, pp. 6.

[20] WHO, mHealth - New horizons for health through mobile technologies < https://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1&isAllowed=y> accessed 10 March 2023, pp. 6.

[21] European Commission, Advancing the Internet of Things in Europe' accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitising European Industry - reaping the full benefits of a Digital Single Market (SWD (2016) 110, 19 April 2016), pp. 6.

[22] U. Pagallo, M. Durante, S. Monteleone, "What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT" in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds), Data Protection and Privacy: (In)visibilities and Infrastructures, Dordrecht: Springer, 2017, pp. 70.

[23] L. Andrews, "A New Privacy Paradigm in the Age of Apps", Wake Forest Law Review, no 53, 2018, pp. 424.

[24] T. Davenport, R. Kalakota, "The potential for artificial intelligence in healthcare", Future Healthcare Journal, no. 5(2), 2019, pp. 97.

[25] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251, October 2017) pp. 5.

[26] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP 248, 4 April 2017), pp. 8-9.

[27] B. Szafrański, „Realizacja zadań publicznych a big data" in Grażyna Szpor (ed.), Internet. Publiczne bazy danych i Big data, Warsaw: C.H Beck 2014, pp. 12.

[28] V. Mayer-Schönberger, K. Cukier, Big Data: A Revolution that Will Transform how We Live, Work, and Think, Boston: Harcourt 2013, pp. 12.

[29] M. Chen, S. Mao, Y. Zhang, V. Leung, Big Data Related Technologies, Challenges and Future Prospects, Cham: Springer 2014, pp. 22.

[30] European Commission, Shaping Europe's digital future (COM(2020) 67, 19 February 2020), pp. 12.

[31] ECHR Case 20511/03, I v Finland (2008).

[32] CJEU, Case C-293/12, Digital Rights Ireland, ECLI:EU:C:2014:238.

[33] M. Safjan, „Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym", Państwo i Prawo, no. 6, 2002, pp. 3.

[34] II C 911/01/5, Prawo i Medycyna 2005, No. 2 with the voice of M. Nesterowicz, pp. 122- 130.

[35] European Commission, New European Interoperability Framework. Promoting seamless services and data flows for European public administrations <https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf>, Luxembourg 2017, accessed 9 March 2023, pp. 5.

[36] Article 29 Working Party(A29WP), Letter on 11 April 2018 to Clemens-Martin Auer (e-Health Network Member State) regarding Agreement between National Authorities or National Organisations responsible for National Contact Points for eHealth on the Criteria required for the participation in Cross-Border eHealth Information Services, < https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=52057> accessed 1 March 2023, pp. 3.

[37] European Commission, Patients' Rights in the European Union - Mapping eXercise <https://health.ec.europa.eu/system/files/2018-01/2018_mapping_patientsrights_exe_en_0.pdf>, Luxembourg 2016, accessed 2 March 2023, pp. 18 - 19.

[38] M. Guedj, M. Munoz-Sastre, E. Mullet, P. Sorum, "Do French lay people and health professionals find it acceptable to breach confidentiality to protect a patient's wife from a sexually transmitted disease?", Journal of Medical Ethics, no. 32(7), 2006, pp. 414.

[39] S. Michalowski, "Medical Confidentiality and Medical Privilege - a Comparison of French and German Law", European Journal of Health Law, no. 5, 1998, pp. 112.

[40] OWASP, Top 10 - 2021 The Ten Most Critical Web Application Security Risks <https://owasp.org/www-project-top-ten/> accessed 20 January 2023.

[41] ENISA, State of vulnerabilities 2018/2019 - Analysis of Events in the life of Vulnerabilities <https://www.enisa.europa.eu/publications/technical-reports-on-cybersecurity-situation-the-state-of-cyber-security-vulnerabilities/at_download/fullReport> Heraklion 2019, accessed 3 March 2023, pp. 1 - 50.

[42] M. Stevens, A. Lenstra, B. de Weger, "Chosen-prefix collisions for MD5 and applications", International Journal of Applied Cryptography, no. 2(4), 2012, pp. 323.

[43] S. Sengan et. al., "Secured and Privacy-Based IDS for Healthcare Systems on E-Medical Data Using Machine Learning Approach", International Journal of Reliable and Quality E-Healthcare no. 11(3), 2022, pp. 1 – 2.

[44] M. Janiszewski, A. Felkner, P. Lewandowski, "A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence", Journal of Telecommunications and Information Technology, no. 2, 2019, pp. 8.

[45] Article 29 Working Party (A29WP), Opinion 8/2014 on the on Recent Developments on the Internet of Things (16 September 2014), pp. 22.

[46] L. Stevens, C. Dobbs, K. Jones, G. Laurie, "Dangers from Within? Looking Inwards at the Role of Maladministration as the Leading Cause of Health Data Breaches in the UK" in R. Leenes, R. van Brakel, S. Gutwirth, Paul De Hert (eds), Data Protection and Privacy: (In)visibilities and Infrastructures, Dordrecht: Springer 2017, pp. 225.

[47] Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability (13 July 2010), pp. 4.

[48] R. Thomas, "Accountability - a modern approach to regulating the 21-century data environment" in H. Hijmans, H. Krankenborg (eds), Data Protection Anno 2014: How to Restore Trust?, Cambridge: Intersentia 2014, pp. 142.

[49] T. Gerety, "Redefining Privacy", Harvard Civil Rights-Civil Liberties Law Review, no. 2, 1977, pp. 288.

[50] European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default (13 November 2019), pp. 12.

[51] M. Taylor et al., "Systematic review of the application of the plan–do–study–act method to improve quality in healthcare", BMJ Quality & Safety, no. 23, 2014, pp. 293.

[52] A. Appari, M. Johnson, "Information security and privacy in healthcare: current state of research", International Journal of Internet and Enterprise Management, no. 6(4), 2010, pp. 280.

[53] A. Cavoukian, Privacy by Design. The 7 Foundational Principles <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf> Toronto 2011, accessed 28 February 2023, pp. 2.

[54] G. Drosatos et. al., "Towards Privacy by Design in Personal e-Health Systems" in J. Gilbert et.al. (eds), Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies, Volume 5: HEALTHINF (ROME: SCITEPRESS 2016), pp. 473.

[55] A. Kańciak. "In search of EU law in the domain of cyberspace protection – the proposal based on the Cyber-PDCA model", Journal of Cyber Security Technology, no. 1(2), 2017, pp. 131.

[56] European Data Protection Board, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 (12 February 2019), pp. 6.

[57] Reply to the letter of 7th December 2017 and a new draft code of conduct with the request of a positive opinion from the WP29 under the Data Protection Directive (11 April 2018).

[58] E. Mantovani, J. Antokol, M. Hoekstra, S. Nouwt, N. Schutte, P. Zilgalvis, J. Castro Gómez-Valadés, C. Prettner, "Towards a Code of Conduct on Privacy for mHealth to Foster Trust Amongst Users of Mobile Health Applications" in R. Leenes, R. van Brakel, S. Gutwirth, P. De Hert (eds), Data Protection and Privacy: (In)visibilities and Infrastructures, Dordrecht: Springer 2017, pp. 104.