IUS ET ADMINISTRATIO ISSN 2300-4797

NR 1/2021 (44) DOI: 10.15584/iuseta.2021.1.5

Weronika Wojturska
MA, PhD candidate, Doctoral School in the Social Sciences in the field of Legal Science, University of Warsaw (Poland)
ORCID: 0000-0002-9514-961

Medical data security in digital transformation of healthcare: Assessment of e-Health solutions standarisation in the European Union

Bezpieczeństwo danych medycznych w obliczu cyfrowej transformacji w ochronie zdrowia: Ocena procesu standaryzacji rozwiązań e-Zdrowia w Unii Europejskiej

Abstract

The paper assesses the security of medical data processing in the standardization of e-Health solutions in the European Union. First, the main cyber risks are identified, and then the effectiveness of health data protection and its interoperability between ICT systems is analysed in terms of strategy and regulatory support provided by the EU. The study indicates that the provisions of the GDPR seem to enhance processing of technological standardisation of e-Health solutions to follow the principle of technological neutrality when defining the required security measures.

Keywords: medical data security, digital transformation, e-Health services, standardisation of e-Health process, GDPR

Streszczenie

W artykule dokonano oceny kondycji bezpieczeństwa przetwarzania danych medycznych w kontekście procesu standaryzacji rozwiązań e-Zdrowia w Unii Europejskiej (UE). W tym celu zidentyfikowano zasadnicze ryzyka cybernetyczne, a następnie zweryfikowano skuteczność ochrony danych dotyczących zdrowia oraz zapewnienia ich interoperacyjności pod kątem strategii i wsparcia regulacyjnego, jakie wprowadza UE. Artykuł dowodzi, że przepisy Rozporządzenia 2016/679 (RODO) sprzyjają faktycznemu procesowi standaryzacji technologicznej rozwiązań

wykorzystywanych w ramach e-Health, przyjmując u podstaw zasadę neutralności technologicznej w sposobie określania wymaganych środków bezpieczeństwa.

Słowa klucze: bezpieczeństwo danych medycznych, transformacja cyfrowa, e-Zdrowie, standaryzacja e-Zdrowia, RODO

I. Introduction

In the age of information and communication technology (ICT) standardisation, the interdisciplinary definition of information understood as a transferable, intangible good that reduces uncertainty is gaining significance more than ever[1]. Although all forms of organisation of society have relied on information, the "information society" is the only one distinguished by the perception of the mechanisms of its production, processing and transmission as fundamental sources of productivity and power[2]. The same processes contribute to the increasing importance of collected clinical data in healthcare, revealing its potential in improving management in this sector. It is particularly essential with regard to the demographic challenges facing Europe, related to aging populations and systematically rising healthcare expenditure. Undoubtedly, ICT increases the efficiency and effectiveness of public health systems and the availability of patient-oriented services[3]. At the same time, the secure sharing of health information will enable citizens to become more proactive in managing their personal health data, improve their health and disease experiences, while supporting coordinated care[4].

The issue of ensuring the protection of medical data and respecting patients' privacy seems to be topical due to the growing demand for electronic health records (EHR) systems that collect and manage personal data concerning health of individuals and implementation of comprehensive e-Health IT solutions at the regional and national level. Eliminating data silos, automating data integration, as well as providing new intelligence to service patients and caregivers are expected to bring rational value across the care continuum[5]. In the concept of pri-

[1] I. Lipowicz et al., *Prawo administracyjne. Część materialna*, Warszawa 2004, p. 97.

[2] M. Castells, *Społeczeństwo sieci*, transl. M. Marody et al., Warszawa 2007, p. 36.

[3] C. Di Iorio, F. Carinci, *Privacy and health care information systems: Where is the balance?* [in:] *eHealth: Legal, ethical and governance challenges*, (ed.) C. George et al., Berlin–Heidelberg 2013, p. 77.

[4] D. Detmer et al., *Integrated personal health records: transformative tools for consumer-centric care* "BMC Medical Informatics and Decision Making" 2008, 8 (1), p. 45.

[5] Cf. G. Gopal et al., *Digital transformation in healthcare–architectures of present and future information technologies* "Clinical Chemistry and Laboratory Medicine" 2018, p. 333; A. Kou-

vacy formulated by Ruth Gavison, its basic element, apart from the issue of guaranteeing the right to respect the solitude and anonymity, is confidentiality[6]. Medical data as a special category of personal data, due to its significant social and economic value, requires the introduction of an appropriate level of security, especially since one of the main identified barriers to the implementation and development of e-Health services is still a lack of trust from both patients and medical professionals. This is due to the belief that the existing legal instruments for the protection of privacy are fragmentary and inadequate[7]. To develop the digital transformation, it is necessary not only to ensure a level of security commensurate with the risk, but also to ensure their interoperability between ICT systems.

Given the fact that using new technologies in health information management plays an increasingly strategic role, the article assesses the security of medical data processing in the standardisation of e-Health solutions in the European Union (EU). The study aims to answer the question of what role the provisions of the GDPR play in the process of technological standardisation of e-Health solutions. Therefore, first, the main cyber risks are identified, and then the effectiveness of health data protection and its interoperability between ICT systems are analysed by the formal-dogmatic method in terms of strategy and regulatory support provided by the EU legislator, in particular key changes introduced by Regulation 2016/679 (GDPR)[8].

II. The concept of e-Health in health information management

The digital transformation in healthcare is associated with the introduction of technical solutions on a large scale, profitably optimising not only the treatment process *sensu stricto*, but also the efficient circulation of medical data. E-Health has been the object of a long-lasting strategy launched by the European

roubali et al., *The new European interoperability framework as a facilitator of digital transformation for citizen empowerment* "Journal of Biomedical Informatics" 2019, Vol. 94, p. 1.

[6] R. Gavison, *Privacy and the limits of law* "The Yale Law Journal" 1980, Vol. 89, No. 3, p. 423.

[7] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century* COM(2012) 736, hereinafter: Communication COM(2012) 736.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016.

Commission in 2004 with the "eHealth Action Plan"[9]. In 2012, a new approach to this area was presented with the ultimate purpose of removing the major obstacles encountered in the implementation of ICTs in routine healthcare[10]. According to "EU-funded projects on ICT for Ageing Well" which is a specific programme adopted within the more general framework of the Digital Single Market strategy, the ICTs would enable EU health systems to achieve a "triple win"[11]. Namely: (i) improving the quality of healthcare services, (ii) supporting the sustainability and the efficiency of the EU health and social care systems, and (iii) enhancing the competitiveness of EU industries through the opening of new markets and businesses[12].

The term e-Health (electronic health) is commonly understood as the use of ICTs in the mutual relations of physicians, healthcare institutions and their patients to improve health and healthcare, including support for therapeutic and diagnostic processes by using technologies such as the Internet and mobile devices[13]. E-Health includes tools that can be used by health authorities (administration) and professionals (medical staff), as well as personalised (individual)

---

[9] Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: *e-Health - making health care better for European citizens: An action plan for a European e-Health Area* COM(2004) 356, hereinafter: Communication COM(2004) 356.

[10] European Commission launched a new "*eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century*".

[11] Policies for Ageing Well with Information and Communication Technologies, https://ec.europa.eu/digital-single-market/en/policies/ageing-well-ict, [accessed: 24.10.2018]

[12] European Commission, Directorate-General for Communications Networks, Content and Technology, Electronic Health Records for Clinical Research, *eHealth for triple win*, Brussels 2014, p. 28, https://www.i-hd.eu/i-HD/assets/File/EHR4CR/presentations/EHR4CR%20-%20 April % 209%20-%20Timmers.pdf [accessed: 24.10.2018].

[13] According to the European Commission: „e-Health describes the application of information and communications technologies across the whole range of functions that affect the health sector. e-Health tools or solutions include products, systems and services that go beyond simply Internet-based applications. (…) e-Health is today's tool for substantial productivity gains, while providing tomorrow's instrument for restructured, citizen-centred health systems and, at the same time, respecting the diversity of Europe's multi-cultural, multi-lingual health care traditions". See: Communication COM(2004) 356, p. 4. The World Health Organization (WHO) presents it in a similar way: „eHealth involves a broad group of activities that use electronic means to deliver health-related information, resources and services: it is the use of information and communication technologies (ICT) for health. eHealth foundation actions build an enabling environment for the use of ICT for health. These include supportive eHealth policy, legal and ethical frameworks, adequate funding from various sources, infrastructure development and developing the capacity of the health workforce through training". See: WHO, *Atlas – eHealth country profiles: based on the findings of the second global survey on eHealth*, Global Observatory for eHealth series, Geneva 2011, Vol. 1, http://www.who.int/goe/publications/ehealth_series_vol1/en/ [accessed: 24.10.2018]

healthcare services for citizens. It should be clarified that it is a broader concept than telemedicine, which is understood as the use of electronic communication systems to exchange medical information from one location to another for the provision of remote healthcare by medical personnel[14]. E-Health covers also various health services related to the model *in absentia*, which can be carried out in the absence of simultaneous presence of participants in a place (e.g. a doctor's office)[15]. Among the referents of this concept, the European Commission distinguishes: health information networks, EHR, telemedicine services, personal wearable and portable communicable systems, health portals, and many other information and communication technology based tools assisting prevention, diagnosis, treatment, health monitoring, and lifestyle management[16].

The innovative technology that is used to create an IT system is based on the assumptions of the Internet of Things (IoT) concept, being an environment combining the operating system with components in the form of devices[17]. McKinsey Global Institute estimates the potential economic impact of the Internet of Things to be 3.9 trillion dollars to 11.1 trillion dollars per year by 2025[18]. Across the health-care applications, IoT technology could have an economic impact of

[14] See: D.A. Perednia, A. Allen, *Telemedicine technology and clinical applications* "Journal of the American Medical Association" 1995, 273 (6), pp. 483-488; C. Botrugno, *Telemedicine in daily practice: Addressing legal challenges while waiting for an EU regulatory framework* "Health Policy and Technology" 2018, Vol. 7, Iss. 2, pp. 131-136. According to the well-known definition adopted by the WHO, telemedicine shall be intended as: "the delivery of health care services, where distance is a critical factor, by all health care professionals using in- formation and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of dis- ease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interest of advancing the health of individuals and their communities". See: WHO, *Report on the second global survey on e-health*, 30.06.2017, http://www.who.int/goe/publications/goe_telemedicine_2010.pdf [accessed: 12.11.2018]

[15] COCIR eHealth Toolkit, *Integrated Care: Breaking the Silos*, p. 58, https://www.cocir.org/fileadmin/4.4_Digital_Health__Public_Website_/15013.COC_2.pdf, [accessed: 12.11.2018]

[16] Communication COM(2004) 356, p. 4.

[17] Y. Yin et. al., *The internet of things in healthcare: An overview* "Journal of Industrial Information Integration" 2016, Vol. 1, p. 4; M. Shamim Hossain, G. Muhammad, *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring* "Computer Networks" 2016, Vol. 101, pp. 192-193; Goldman Sachs Report, *How the Internet of Things Can Save the American Healthcare System $305Billion Annually*, 23 June 2016, https://www.engagemobile.com/goldman-sachs-report-how-the-internet-of-things-can-save-the-american-healthcare-system-305-billion-annually/ [accessed: 15.11.2018]; I. Lee, K. Lee, *The Internet of Things (IoT): Applications, investments, and challenges for enterprises* "Business Horizons" 2015, Vol. 58, Iss. 4, pp. 431-432.

[18] McKinsey Global Institute report, *The Internet of Things: Mapping the value beyond the hype*, 2015, p. 3, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world [accessed: 12.12.2018]

170 billion dollars to 1.6 trillion dollars per year by 2025[19]. The dynamic development of IoT tools is conducive to the efficient collection, transmission and analysis of data provided from sources, i.e. EHR or sets of medical and health-related data, including those associated with the functioning of the patient's body, which are generated and transmitted in real time from measuring devices[20]. Its availability is an attribute that provides access to information about patient to authorised entities. The information integrity verification procedure under the IoT should also enable verification of the authenticity[21]. As a result, unauthorised modification of the data undesirable from the perspective of the interest of the subject, can be avoided.

III. Cyber threats for e-Health services

The use of the ICTs in therapeutic processes is accompanied by inherent safety concerns[22]. The rapid development of the Internet over the past decade appeared also to have facilitated an increase in the incidents of online attacks. The digital transformation has become an area for maneuver for criminal (hacking) activities, and their growth and development now seem to be on par. Hackers more and more often attack demanding and well-secured systems, not taking into account the possibility of tragic consequences for the life and health of citizens. In the literature, the most frequent cyber threats to which e-Health services are exposed include: ransomware, Denial of Service (DoS) and the associated risk of connecting IoT devices to botnets[23].

---

[19] Ibidem, p. 3.

[20] Cf. M. Shamim Hossain, G. Muhammad, *Cloud-assisted Industrial…*, p. 192; G. Noto La Diega, *British perspectives on the Internet of Things - the Clouds of Things-Health Use Case*, pp. 62-73, https://www.researchgate.net/publication/313270496_British_Perspectives_on_the_Internet_of_Things_The_Clouds_of_Things-Health_Use_Case [accessed: 12.12.2018]

[21] Y. Yin et al., *The internet of things…*, p. 7. See also: A. Hamid, A. Sarmad, *Evaluation of E-health Services: User's Perspective Criteria* „Transforming Government: People, Process and Policy" 2008, Vol. 2 Iss. 4.

[22] More on the new challenges in the field of patient privacy protection due to the specificity of the current generation of medical applications: L. Andrews, *A new privacy paradigm in the age of apps* "Wake Forest Law Review" 2018, Vol. 53, p. 426.

[23] Cf. A. Hamid et al., *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring* "Computer Networks" 2016, Vol. 101; C. Elliott, *Botnets: To what extent are they a threat to information security?* "Information Security Technical Report" 2010, Vol. 15, Iss. 3; A. Adamski, *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich* „Państwo i Prawo" 2013, nr. 11.

The first of the indicated powerful and harmful attacks – ransomware – works schematically by first encrypting potential patients' medical data with malware and then demanding a ransom to restore access to it. The year 2017 saw the largest in scale cyberattack using blackmailing software − WannaCry[24]. Thousands of computers around the world were infected, including the British National Health Service, causing a great deal of chaos. As a result of the hacking attack in the UK, computers were blocked in 25 hospitals with the reservation that they would be unlocked after paying a ransom in electronic bitcoin. The most serious effect of the attack between 12th-19th May with a direct impact on health safety was the cancellation of approximately 19,000 treatments, generating a loss of nearly 20 million pounds. Subsequent costs were estimated at an additional 72 million pounds[25]. This incident made professionals around the world realize how healthcare – in building cybersecurity systems – lags far behind other industries, such as the financial sector. The essence of the threat is emphasised by the fact that the e-Health solutions have a direct impact on the life and health of the patient – the subject of medical data. Therefore, a cyberattack, which the vector carrying the threat is *de facto* an IoT device, may equally affect the aforementioned personal goods. The technical course of an attack will always result in a breach of the availability, integrity or confidentiality of the information processed.

The growing use of wireless technology in healthcare systems and devices makes them particularly open to cyber-attacks, including also DoS and information theft via sniffing (eaves-dropping) and phishing attacks[26]. It is a one-to-one phenomenon that impairs or prevents the legitimate users from accessing a system, a network, or an application, by utilising its resources. The refusal to provide the service occurs through overloading the system infrastructure elements and using the error to collapse the work in the application[27]. DoS attacks usually consume bandwidth, overload the network handling software, and send precise packets to use up the limited available resources. The attacker sends

[24] See: M. Akbanov et al., *Ransomware detection and mitigation using software-defined networking: The case of WannaCry* "Computers & Electrical Engineering" 2019, Vol. 76, pp. 111-121; https://www.europol.europa.eu/wannacry-ransomware; https://www.bbc.com/news/world-europe-39907965; https://www.cert.pl/news/single/wannacry-ransomware/ [accessed: 10.01.2019]

[25] See: M. Field, *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled* „The Telegraph" 11.10.2018, https://www.telegraph.co.uk/technology/2018/10/11 /wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/ [accessed: 10.01.2019], M. Akbanov et al., *Ransomware detection…,* pp. 111-121.

[26] J.M. Vidal et al., *Adaptive artificial immune networks for mitigating DoS flooding attacks* "Swarm and Evolutionary Computation" 2018, Vol. 38, pp. 94-95.

[27] Ibidem, pp. 94-95.

excessive requests to the target (victim) with a spoofed IP address, which is thus flooded simultaneously with a large number of packets from different target machines. Dealing with DoS attacks at all layers of cloud systems is a major challenge due to the difficulty of distinguishing the attackers' requests from legitimate user requests[28]. Based on IoT devices for the implementation of e-Health services, this could effectively block the possibility of further monitoring the patient's vital signs or real-time reporting of his/her health condition.

A distributed DoS (DDoS) attack is launched by a mechanism called "botnet" through a network of controlled computers. It is mostly defined as a collection of compromised machines running the bot program and controlled by a remote command and control infrastructure[29]. Cybercriminals use botnets as a tool to penetrate systems via spear phishing[30]. Their goal is to deliver malware which will enable a network to be probed for open ports and vulnerabilities[31]. The scale of the threat is reflected in the fact that botnets can comprise between ten thousand and one million compromised machines in any one network. Most computer or device users are unaware that their machine has been compromised and is being given remote instructions, and worse still, is potentially capturing their personal data. These attacked devices are no longer controlled by authorised medical personnel and begin to follow the instructions of the botnet managers. This is exemplified by the risk of a pacemaker malfunction. A recent report from WhiteScope[32] found approximately 8,600 security vulnerabilities in third-party data libraries in four pacemaker programmers from four separate manufacturers. The pacemakers available on the market are equipped with wireless communication interfaces, which is a solution adopted for the convenience of patients, yet with many disadvantages. The authors of the report emphasise that the implantable cardiac device ecosystem inherits security features associated with the underlying system-of-systems architecture[33]. If adequate security controls are not implemented, weaknesses associated with architecture and imple-

[28] Cf. C. Modi et al., *A survey on security issues and solutions at different layers of cloud computing* "The Journal of Supercomputing" 2013, 63 (2), pp. 561-592.

[29] C. Elliott, *Botnets: To what extent*…, p. 80.

[30] Understood in the article as: "type of social engineering attack where the attacker sends a targeted deceptive email that tricks the recipient into performing dangerous action for the adversary". See: G. Ho et al., *Detecting credential spearphishing in enterprise settings*, Conference paper from 26th Security Symposium (USENIX' 17), 2017, pp. 469-485.

[31] C. Elliott, *Botnets: To what extent*…, p. 89.

[32] B. Rios, J. Butts, *Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies*, WhiteScope report, 17 May 2017, https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVlBeGVCSW8/view [accessed: 15.11. 2019]

[33] B. Rios, J. Butts, *Security Evaluation…*, p. 7.

mentation interdependencies have the potential to compromise ecosystem confidentiality, integrity, and/or availability – resulting in potentially negative consequences to patient care if those weaknesses are exploited[34]. If hackers could access the pacemaker remotely, they would be able to alter programmed therapy settings or even kill the patient.

In each of the above-mentioned cases, there is a risk of losing control over IoT devices by the data administrator. As more and more of a nation's infrastructure becomes dependent on the Internet, the exposure increases along with the risk that the infrastructure will be targeted for compromise. This cannot be allowed when it comes to ensuring that the patient's right to privacy is preserved. It will be inextricably linked with the necessity to implement specialised solutions for the security of ICT systems supporting the information system in healthcare. Access to sensitive data processed in them should be limited using authentication and authorisation mechanisms. Then the confidentiality of these resources will be guaranteed using appropriately strong cryptographic algorithms. E-Health solutions should be particularly characterised by the security of the processed data resources while maintaining a useful level of interoperability and technological neutrality of the ICT systems. The first step towards the introduction of appropriate standards at the regional (national) level is their establishment and, as a result, harmonisation in the EU. Therefore, in the following sections of the paper it will be verified whether and how the EU legislator supports strategically and regulatory the protection of health-related data processing in the standardisation of e-Health solutions.

IV. Medical data interoperability

In the rapidly evolving field of ICT, it is common for technical and market developments to precede the establishment of appropriate policies, legal and regulatory mandate and monitoring capacity. For the proper conduct of the technological standardisation of e-Health solutions, it is crucial to ensure the interoperability of medical data exchange. Both these mechanisms require the creation of an appropriately harmonised legal framework in the EU. Interoperability is seen as a key requirement of the single digital e-Health market but also for continuity of care[35]. Otherwise, it cannot be delivered, and citizens cannot

[34] *Ibidem*, p. 7.

[35] European Commission, Directorate-General for Communications Networks, Content and Technology, Electronic Health Records for Clinical Research, *eHealth…*, p. 31.

have an overall view of their health information. First of all, this is related to the situation of an individual patient, whose data is scattered in EHR, and they are at the disposal of various entities performing medical activities. In this case, ensuring the possibility of their uninterrupted flow between healthcare providers allows to recreate a complete history of the disease, improving diagnostic and treatment processes. Secondly, with the prospect of ensuring health security to a larger group of communities, the data (processed in anonymised form) are used to monitor the health condition of the population in a specific area on an ongoing basis for an early response in the case of a sudden health threat.

The reality often clashes with expectations, as in this case, because although national and regional health systems generate and store large amounts of EHR data for every citizen, most of them are still restricted in data silos[36]. The limited interoperability between digital health solutions effectively restrains the possibility of reusing data for further healthcare. Dispersed data repositories and departmental systems store health-related data using different information models, which makes data capture often inconsistent or suited to incompatible formats. Frequently, the data are of varying quality and unstructured as free text, which makes it even more challenging for automatic processing. This showsthat e-Health systems are not always designed with the collective use of medical data in mind for innovative purposes such as their aggregation, exchange, analysis or decision support. Standardisation of information and document exchange has significantly contributed to the sharing of data concerning health. However, its quality and integrity require cooperation and negotiation between stakeholders while existing e-Health systems only collect and exploit fragmented information without revealing its true potential[37]. Patients, who are consumers of healthcare, are not yet fully empowered to direct access to and exchange of their own health information.

The EU having recognised the need for interoperability among member states, has created the Interoperability Solutions for European Public Administrations (ISA) funding programme (2010-2015)[38] to enable the creation and interoperability of eGovernment services to European public administrations, businesses and citizens. With the end of this project, there were calls for a revision and extension of the existing European Interoperability Framework in the Communication on a Digital Single Market Strategy for Europe of 6th May 2015

[36] Cf. A. Kouroubali et al., *The new European interoperability…*, p. 2 et seq.

[37] A. Kouroubali et al., *The new European interoperability…*, p. 2.

[38] Decision No 922/2009/EC of the European Parliament and of the Council of September 2009 on interoperability solutions for European public administrations (ISA), OJ L 260, 3.10.2009.

in which interoperability was recognised as a prerequisite for "efficient connections across borders, between communities and between public services and authorities"[39]. The lack of an agreed approach in the EU as to how to understand the concept of interoperability and its role has been recognised by the Member States as the cause of the diversity of solutions and their mutual incompatibility. This hinders the harmonisation of public services in the EU and the cross-sectoral exchange of information[40]. The Digital Agenda for Europe will only be successful if interoperability based on standards and open solutions is ensured[41]. Therefore, the current European interoperability framework and strategy have been implemented through instruments such as the ISA successor − the ISA^2 programme (2016-2020)[42]. This has involved a variety of actions that aimed to improve and support digital collaboration for interoperable cross-border and cross-sector public services in Europe.

Due to the changing external conditions, changes in the policies and programmes of the EU and development in the field of technology, in 2017 the new European Interoperability Framework (new EIF) was adopted by the European Commission. It proposes recommendations, models and guidance that have the potential to improve interoperability within the European public sector. This framework was designed to improve the delivery of one of the top priorities i.e., the creation of a Digital Single Market in Europe. Over time, this strategy had to adapt to new information processing trends such as open data and cloud computing. The new EIF defines interoperability, within the European public service delivery, as "the ability of organizations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organizations, through the business processes they support, by means of the exchange of data between their ICT systems"[43]. The new EIF presents the consolidated

[39] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *A Digital Single Market Strategy for Europe*, COM(2015) 192.

[40] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *Towards interoperability for European public services* COM(2010) 0744, p. 2, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52010DC0744 [accessed: 20.01.2019]

[41] Ibidem, p. 2.

[42] Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA^2 programme) as a means of modernising the public sector, OJ L 318, 4.12.2015.

[43] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: *European Interoperabil-*

conceptual model of the EIF based on the synthesis of the interoperability model and the model of integrated public services. Importantly, the EIF identifies four main levels of public service interoperability: legal, organisational, semantic, technical[44]. The explanation of both the principles and the models is illustrated by the 47 detailed recommendations that relate to each of the levels mentioned above. They set out requirements and constraints on how to plan, design, implement and deploy European digital services[45]. Compared to the previous strategy, the interoperability recommendations are described in more detail, with greater emphasis on openness and information management, data portability, interoperability management and service integration, and facilitating their implementation. The latest version of the new EIF is accompanied by an Interoperability Action Plan, which sets out the priorities that should support its implementation from 2017 to 2020, was published in Annex 1 to the Communication COM(2017) 0134[46]. Successful implementation of the Interoperability Action Plan will require an active involvement of all actors, in particular public administrations. The planned activities will ensure the achievement of the ultimate goal of user-oriented interoperable public services in the EU. Through the ISA² program, the European Commission will manage and coordinate the implementation and monitoring of the new EIF using key performance indicators and defined measurable targets[47].

On the institutional side, achieving interoperability of cross-border e-Health services are supported by a voluntary network bringing together national authorities responsible for these issues designated by the Member States. Art. 14 of Directive 2011/24EU on the application of patients' rights in cross-border healthcare[48], where indicated in art. 168 par. 2 of the Treaty on the Functioning of the European Union (TFEU)[49], the coordinating and supporting competence of the European Union in the field of healthcare was enriched with the possibility of supporting cooperation and exchange of information between the Member

ity Framework – Implementation Strategy COM(2017) 0134, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN [accessed: 20.01.2019], hereinafter: Communication COM(2017) 0134.

[44] Annex 2 to Communication COM(2017) 0134, p. 21.

[45] The number of recommendations increased from 25 to 47. See: Annex 2 to Communication COM(2017) 0134, p. 8.

[46] Ibidem, p. 21.

[47] Communication COM(2017) 0134, p. 10.

[48] 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, OJ L 88, 4.4.2011, p. 45.

[49] OJ C 326, 26.10.2012.

States belonging to the voluntary network of national authorities responsible for e-Health. The European eHealth Network regularly issues appropriate guidelines not only on technical and organisational issues, but also on legal solutions. Its fundamental goals include: drawing up guidelines on a non-exhaustive list of data, taking into account the principles of their protection resulting from legal provisions in order to maintain continuity of care and patient safety in the cross-border aspect. In 2012, the European Commission, in one of its announcements, already presented the above-mentioned "eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century"[50] to support the efficiency and innovation of Member States' healthcare systems.

V. Security of medical data processing in GDPR

Regulation 2016/679 should be considered the next key step towards regulatory support for the security of medical data processing. The GDPR introduces a risk-based approach (often graduated) that addresses the violation of the rights and freedoms of data subjects. This means that the controller and, to a different extent, the processor must consider the existing and potential risks to the protection of personal data in order to apply appropriate solutions. This approach allows to focus on the highest risk situations, while maintaining an appropriate level of protection when this risk is low and does not require the use of the entire set of measures provided for by the GDPR[51].

The analysis should begin with examining the recitals of the GDPR. In the interoperable data exchange, it is important to indicate in recital 13 GDPR that the most essential objective of this act – apart from ensuring an adequate level of protection of personal data – is to ensure the free movement of such resources in the internal market. It should be emphasised that ensuring an appropriate standard of protection of information resources, guaranteeing the implementation of the interests and rights of natural persons, naturally reduces barriers to the free flow of personal data. However, the uninterrupted flow of medical data related to the implementation of health goals may notunreasonably and excessively interfere with the privacy of the data subjects. The case law of the CJEU also confirms that the condition of the free flow of data may interfere with the rights and freedoms of a person if it is legal, intentional and necessary, but in order to

[50] Communication COM(2012) 736.

[51] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, p. 341.

be considered justified, it must not infringe their essence[52]. An example of this is a situation in which medical data resources are processed for purposes related to medical rescue or combating cross-border health threats.

A direct reference to medical data can be found in recital 35 GDPR, according to which "Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU"[53]. This means data provided by the patient during registration, obtained during a medical interview or as a result of tests performed. In addition, this recital mentions an open catalogue of information that falls under this category of personal data: a number, symbol or designation assigned to a natural person for unambiguous identification for health purposes; information from laboratory or medical tests of body parts or body fluids, including genetic data and biological samples; and all information, e.g. on: disease, disability, disease risk, medical history, clinical treatment, physiological or biomedical condition of the data subject, regardless of their source. This source can be, for instance, a physician or other health care professional, hospital, medical device, or an *in vitro* diagnostic test.

Further guidance is provided by recital 53 which indirectly refers to health data by indicating that "Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole". Moreover, recital 53 also contains a catalogue of situations in which special categories of personal data (including medical data) are processed for health purposes:

- the management of health and social care services and systems, including the processing of such data by governing bodies and national central health authorities for the purposes of quality control;
- obtaining management information and general national and local oversight of the health care and social security system;
- ensuring continuity of healthcare or social security and cross-border healthcare;
- for safety, monitoring and health alert purposes;

[52] Judgment of the Court (Third Chamber), 22 November 2012, C-139/11.

[53] 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, OJ L 88, 4.4.2011.

- for archival purposes in the public interest;
- for scientific or historical research purposes;
- for statistical purposes based on European Union or Member State law and serving the public interest;
- for public interest analysis in the field of public health.

Among the provisions of the GDPR, one can find a legal definition of data concerning health, indicating that it is „personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status". This definition is consistent with the definition of health proposed by the WHO, according to which health is the body's physical and mental well-being[54]. Medical data fall under special categories of personal data. This is indicated by art. 9 par. 1 GDPR, which prohibits the processing of personal data that reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". This means that this type of data is assigned the nature of sensitive data, because their processing poses a threat to the patient's privacy to a greater extent than the so-called regular data. Their processing is in principle prohibited, however, there are many exceptions to this prohibition, included in the closed catalogue in art. 9 par. 2 GDPR. Under it, sensitive data may be processed in a situation where: „processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3". At this point, it should be referred to the quoted par. 3 of art. 9 GDPR, because on its basis, it is permissible to process sensitive data if it is processed by – or under the responsibility – of an employee subject to professional secrecy under EU law or the law of a Member State, or provisions established by competent national authorities or by another person also subject to the obligation of professional secrecy under Union or Member State law or rules laid down by competent national authorities. Moreover, pursuant to art. 9 par. 4 Member States may maintain or introduce further conditions, including restrictions, with regard to the processing of genetic data, biometric data or data

[54] http://www.who.int/suggestions/faq/en/ [accessed: 20.01.2019]

concerning health. Compared to the previously applicable regulation, the catalogue of conditions set out in art. 9 par. 2 remains similar, although the GDPR draws attention to two new exceptions to the prohibition of processing sensitive data: public interest in public health and the implementation of archival purposes in the public interest, scientific, historical or statistical purposes. There is no doubt that the specificity of these data as relating to the sphere of privacy or even human intimacy makes it necessary to apply specific protection standards in the processing of this information[55]. Maintaining medical secrecy and allowing the processing of medical data under certain conditions are closely related. The provisions of art. 9 par. 2 in conjunction with art. 9 par. 3 GDPR should be treated broadly to prevent possible violations of patients' rights, primarily through inadequate protection of the patient's processed data, which violates the basis of the relationship between a medical professional and a patient, who by nature should be protected by confidentiality, so that the treated person has a sense of security and comfort.

The obligation to ensure security can be found primarily in the second section of Chapter IV of the GDPR, art. 32: "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (…)". The possibility of considering the cost of implementing a technical and organisational measure deserves approval. This seems to be an expression of the concept of relativisation in the GDPR. According to it, the obliged entity, with the possibility of obtaining the maximum technical knowledge, should only, taking into account the premise of the "costs of its implementation", compare it with the actual economic possibilities. Then, in the further part of the provision, the EU legislator introduces a catalogue of measures:

1. pseudonymisation and encryption of personal data (par. 1 (a));

2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (par. 1 (b));

3. the ability to quickly restore the availability and access to personal data in the case of a physical or technical incident (par.1 (c));

4. regularly testing, measuring and evaluating the effectiveness of technical and organisational measures to ensure the security of processing (par. 1 (d)).

This provision indicates the obligation, in accordance with the principle of technological neutrality, to select measures adequate to the risk. In par. 2, the EU

[55] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie…*, p. 278.

legislator formulates directly to the controller an obligation to take into account the risk related to data processing, in particular: "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". The definition is the same as the content of art. 4 point 12 GDPR, in which the essence of the breach of personal data protection is specified. The following paragraphs allow the possibility of meeting the indicated requirements by adhering to an approved code of conduct or an approved certification mechanism.

An expression of the principle of integrity and confidentiality (art. 5 par. 1 (f) GDPR) seems to be the subsequent obligation of the controller or the processor to take steps to ensure that any natural person, acting under authorization and having access to medical data, processes them only at the request of the controller (art. 32 par. 4 in conjunction with art. 29 GDPR). In practice, as Konrad M. Mazur rightly points out, the obligated entity, to consider the current state of technical knowledge, should assess how the software offered on the market protects medical data, relate it to the general technical standard and, bearing in mind its own financial capabilities, choose a solution ensuring a level of security adequate to the risk related to the data processed by it[56].

Art. 33 par. 1 GDPR can be seen as belonging to the category of novelty in strengthening the security pillar.s It introduces an obligation unknown so far to the Personal Data Protection Act of August 29, 1997[57]. In the case of a personal data breach, the controller shall „without undue delay and – where feasible, not later than 72 hours after having become aware of it – notify the personal data breach to the supervisory authority" and "document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken". Interestingly, the regulations do not limit the severity of reported infringements. Another proposal that should be assessed approvingly is the obligation to assess the data protection implications as the greatest manifestation of the relativisation of the reformed personal data protection law. The purpose of the regulation under art. 35 GDPR is therefore not to eliminate the risk, but to implement proportionate measures considering criteria independently selected and indicated under the basic art. 32 GDPR[58].

---

[56] K.M. Mazur [in:] *Ochrona danych medycznych. RODO w ochronie zdrowia* (ed.) M. Jackowski, Warszawa 2018, p. 185.

[57] J.L. 1997 No. 133 item. 883.

[58] D. Lubacz [in:] *RODO. Ogólne rozporządzenie o ochronie danych, Komentarz* (ed.) D. Lubacz, Warszawa 2018, pp. 587-590.

VI. Conclusions

The digital transformation of healthcare is associated with a large-scale introduction of technical solutions that profitably optimise not only the treatment process *sensu stricto*, but also the efficient circulation of medical data. This, as a special category of personalities closely related to health and genetic data, due to their significant social and economic value, requires the introduction of an appropriate level of security. Still, one of the identified basic barriers to the implementation of e-Health services is a lack of trust on the part of both patients and medical professionals. This is associated with the fact that digital transformation has inevitably also become a field of maneuver for criminal activities, and their growth and development now appear to be on par.

The study indicates that the provisions of the GDPR seem to enhance processing of technological standardisation of e-Health solutions to follow the principle of technological neutrality when defining the required security measures. It is reflected in art. 24 GDPR supplemented by art. 32 GDPR, which defines the general obligations of the controller, obliging him to follow the risk-based approach during the implementation of the measures. It means it is necessary to demonstrate that the processing activity complies with the GDPR and the measures adopted are effective. This approach should be implemented in the light of the principle of technological neutrality. According to it, the controller is obliged to select organisational and technical measures in a way they correspond to the nature, scope, purposes of processing and the risk of infringements of various severity. It is essential in the standardisation of IoT solutions used in e-Health. In practice, the selection of appropriate organisational and technical security measures within e-Health may seem problematic, as the ongoing standardisation process was not originally designed with the protection of medical data in mind. However, the possibility to implement self-regulatory and certification activities, or to prepare codes of conduct aimed at supporting the proper application of the GDPR, considering the specificities of the various processing sectors, is already an achievement. For instance, it is promising that the healthcare industry in Poland has already started work on its own code, which aims to provide clear guidelines for the application of the GDPR, aimed at increasing the security of data concerning health[59]. Furthermore, due to art. 53 of

[59] P. Najbuk et. al., *Branża medyczna już pisze swój własny kodeks ochrony danych osobowych*, http://prawo.gazetaprawna.pl/artykuly/1064902,rodo-dane-osobowe-ochrona-danych-sluzba-zdrowia.html [accessed: 20.01.2019]

the Personal Data Protection Act of May 10, 2018[60], amended in accordance with the EU requirements, the President of the Office for Personal Data Protection is authorised to issue recommendations on the security of processing, which may indirectly affect the appropriate selection of e-Health system measures.

Bibliography

Literature

Adamski A., *Botnety jako zagadnienie prawno-kryminologiczne na tle doświadczeń amerykańskich*, „Państwo i Prawo", Nr. 2013/11.

Akbanov M. et al., *Ransomware detection and mitigation using software-defined networking: The case of WannaCry* "Computers & Electrical Engineering" 2019, Vol. 76.

Andrews L., *A new privacy paradigm in the age of apps* "Wake Forest Law Review" 2018, Vol. 53.

Bielak-Jomaa E., Lubasz D., *RODO. Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Botrugno C., *Telemedicine in daily practice: Addressing legal challenges while waiting for an EU regulatory framework* "Health Policy and Technology" 2018, Vol. 7, Iss. 2.

Castells M., *Społeczeństwo sieci,* transl. M. Marody et al., Warszawa 2007.

Detmer D. et al., *Integrated personal health records: transformative tools for consumer-centric care* "BMC Medical Informatics and Decision Making" 2008, 8 (1).

Di Iorio C., Carinci F., *Privacy and health care information systems: Where is the balance?* [in:] *eHealth: Legal, ethical and governance challenges*, (ed.) C. George et al., Berlin–Heidelberg 2013.

Elliott C., *Botnets: To what extent are they a threat to information security?* "Information Security Technical Report" 2010, Vol. 15, Iss. 3.

Gavison R., *Privacy and the limits of law* "The Yale Law Journal" 1980, Vol. 89, No. 3.

Gopal G. et al., *Digital transformation in healthcare–architectures of present and future information technologies* "Clinical Chemistry and Laboratory Medicine" 2018.

Hamid A., Sarmad A., *Evaluation of E-health Services: User's Perspective Criteria* „Transforming Government: People, Process and Policy" 2008, Vol. 2 Iss. 4.

Hamid A. et al., *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring* "Computer Networks" 2016, Vol. 101.

Ho G. et al., *Detecting credential spearphishing in enterprise settings*, Conference paper from 26th Security Symposium (USENIX' 17), 2017.

Jackowski M. (ed.), *Ochrona danych medycznych. RODO w ochronie zdrowia*, Warszawa 2018.

Kouroubali A. et al., *The new European interoperability framework as a facilitator of digital transformation for citizen empowerment* "Journal of Biomedical Informatics" 2019, Vol. 94.

Lee I., Lee K., *The Internet of Things (IoT): Applications, investments, and challenges for enterprises* "Business Horizons" 2015, Vol. 58, Iss. 4.

Modi C. et al., *A survey on security issues and solutions at different layers of cloud computing* "The Journal of Supercomputing" 2013, 63 (2).

[60] J.L. 2018 item. 1000.

Perednia D.A., Allen A., *Telemedicine technology and* clinical applications "Journal of the American Medical Association" 1995, 273 (6).

Shamim Hossain M., Muhammad G., *Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring* "Computer Networks" 2016, Vol. 101.

Vidal J.M. et al., *Adaptive artificial immune networks for mitigating DoS flooding attacks* "Swarm and Evolutionary Computation" 2018, Vol. 38.

Yin Y. et. al., *The internet of things in healthcare: An overview* "Journal of Industrial Information Integration" 2016, Vol. 1.

Legislation

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European Interoperability Framework – Implementation Strategy COM(2017) 0134.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe, COM(2015) 192.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century COM(2012) 736.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards interoperability for European public services COM(2010) 0744.

Communication to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health - making health care better for European citizens: An action plan for a European e-Health Area COM(2004) 356

Decision (EU) 2015/2240 of the European Parliament and of the Council, of 25 November 2015, establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens (ISA² programme) as a means of modernising the public sector, OJ L 318, 4.12.2015

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, OJ L 88, 4.4.2011.

Decision No 922/2009/EC of the European Parliament and of the Council of September 2009 on interoperability solutions for European public administrations (ISA), OJ L 260, 3.10.2009.

Judgment of the Court (Third Chamber), 22 November 2012, C-139/11.

Personal Data Protection Act of August 29, 1997, J.L. 1997 No. 133 item. 883.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016.

Treaty on the Functioning of the European Union (TFEU), OJ C 326, 26.10.2012.

Internet sources

https://www.bbc.com/news/world-europe-39907965

https://www.cert.pl/news/single/wannacry-ransomware/

COCIR eHealth Toolkit, *Integrated Care: Breaking the Silos*, https://www.cocir.org/fileadmin/4.4_Digital_Health__Public_Website_/15013.COC_2.pdf

European Commission, Directorate-General for Communications Networks, Content and Technology, Electronic Health Records for Clinical Research, *eHealth for triple win*, Brussels 2014, https://www.i-hd.eu/i-HD/assets/File/EHR4CR/presentations/EHR4CR%20-%20April%209%20-%20Timmers.pdf

Field M., *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled* „The Telegraph" 11.10.2018, https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Goldman Sachs Report, *How the Internet of Things Can Save the American Healthcare System $305Billion Annually*, 23 June 2016, https://www.engagemobile.com/goldman-sachs-report-how-the-internet-of-things-can-save-the-american-healthcare-system-305-billion-annually/

McKinsey Global Institute report, The Internet of Things: Mapping the value beyond the hype, 2015, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

Najbuk P., Stępniowski J., Kazimierczyk P., *Branża medyczna już pisze swój własny kodeks ochrony danych osobowych*, http://prawo.gazetaprawna.pl/artykuly/1064902,rodo-dane-osobowe-ochrona-danych-sluzba-zdrowia.html

Noto La Diega G., *British perspectives on the Internet of Things - the Clouds of Things-Health Use Case*, https://www.researchgate.net/publication/313270496_British_Perspectives_on_the_ Internet_of_Things_The_Clouds_of_Things-Health_Use_Case

Policies for Ageing Well with Information and Communication Technologies, https://ec.europa.eu/digital-single-market/en/policies/ageing-well-ict.

Rios B., Butts J., *Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies*, WhiteScope report, 17 May 2017, https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVlBeGVCSW8/view

WHO, *Atlas – eHealth country profiles: based on the findings of the second global survey on eHealth*, Global Observatory for eHealth series, Geneva 2011, Vol. 1, http://www.who.int/goe/publications/ehealth_series_vol1/en/

WHO, Report on the second global survey on e-health, 30.06.2017, http://www.who.int/goe/publications/goe_telemedicine_2010.pdf

https://www.europol.europa.eu/wannacry-ransomware