ORGANIZATIONAL STANDARDS FOR MEDICAL TELECONSULTATIONS AND PERSONAL DATA PROTECTION

Standardy organizacyjne teleporad medycznych a ochrona danych osobowych

Łukasz Nosarzewski

Administrative, Constitutional and Labour Law, Faculty of Law and Administration, Łazarski University, Poland

Łukasz Nosarzewski – ORCID 0000-0001-8769-6757

Abstract

Introduction and objective: The article discusses the organizational standards for providing medical teleconsultations, including patient identification, confidentiality rules and the use of technical measures to secure patient data, regulated by the Ordinance of the Minister of Health of 12 August 2020 on the organizational standard for teleconsultations in primary healthcare. The relationship between these standards and the personal data protection regulations established by 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), was discussed. **Material and methods:** The study uses the methods of legal science: the dogmatic and theoretical-legal approach. The analysis included normative acts, recommendations, and guidelines in the field of personal data protection, as well as scientific studies and literature. **Results:** As a result of this analysis, the thesis that the basic organizational requirements for medical teleconsultation are not sufficient to maintain all requirements for the protection of personal data was verified. **Conclusions:** Since the mandatory organizational standard for teleconsultations defined by law is not sufficient for the protection of personal data, teleconsultations should be organized in accordance with the above-standard requirements compared to those provided for by the legislator. It is also worth using codes of conduct approved by the President of the Personal Data Protection Office.

Streszczenie

Wprowadzenie i cel: W artykule omówiono standardy organizacyjne teleporad medycznych, obejmujące identyfikację pacjenta, zachowanie zasad poufności i stosowanie środków technicznych zabezpieczających dane pacjenta, uregulowane w rozporządzeniu Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej. Analizie poddano relacje między tymi standardami a prawem ochrony danych osobowych, uregulowanym w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, RODO). **Materiał i metody:** Wykorzystano metody z obszaru nauk prawnych – dogmatyczną i teoretycznoprawną. Analizą objęto akty normatywne, zalecenia i wytyczne z obszaru ochrony danych osobowych oraz opracowania naukowe i piśmiennictwo. **Wyniki:** W wyniku analizy zweryfikowano tezę, zgodnie z którą podstawowe wymagania organizacyjne dla teleporady uregulowane w rozporządzeniu Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej nie są wystarczające, aby zachować wszystkie wymogi ochrony danych osobowych. **Wnioski:** Skoro określony rozporządzeniem obligatoryjny standard organizacyjny dla teleporad zbyt nisko ustanowił wymogi minimalne i nie są one wystarczające, aby uczynić zadość wszystkim obowiązkom administratora danych osobowych wynikającym z RODO, to teleporady powinny być organizowane z założenia wedle wymogów ponadstandardowych względem tych, które przewidział prawodawca. Warto przy tym sięgać do zatwierdzonych przez Prezesa Urzędu Ochrony Danych Osobowych kodeksów postępowania.

Keywords: primary healthcare, telemedicine, personal data protection, personal data, medical teleconsultation

Słowa kluczowe: podstawowa opieka zdrowotna, telemedycyna, ochrona danych osobowych, dane osobowe, teleporada medyczna

DOI 10.53301/lw/174749

Received: 17.08.2023

Accepted: 08.11.2023

Corresponding author:
Łukasz Nosarzewski
Chair of Administrative, Constitutional and Labour Law at the Faculty of Law and Administration, Łazarski University in Warsaw
43 Świeradowska Str., 02-662 Warsaw
e-mail: l.nosarzewski@wp.pl

Introduction

In legal sciences, a standard may refer to the content of legal norms that describe, in a relatively measurable way, the properties or attributes of the given good or conduct of the given subject of law, in reference to the achievements of specific disciplines of science, with the aim to obtain a relatively accurately defined "product" by indicating those properties or attributes. In law, the notion of standard is used, when the intention is to ensure a uniform, yet in a certain way evolutionary, developing level of the fulfilment of the fundamental goals and tasks of the state. In the doctrine of administrative law, the notion of standard appears in various contexts, and its content remains in various relations with the law. In some cases, the law is either constitutive or declares objectivised properties of the natural law, or transforms them. In others, the law refers to criteria and evaluations that have been developed outside the legal system, however considering them so important for the functioning of the society within certain scopes that it sanctions their realisation in various, direct and indirect ways. At the same time, in its regulations, administrative law ensures the existence of standardisation documents that are developed by authorised entities and ethical committees [1]. Therefore, the notion of standard is not new in the doctrine of law, although it has not been defined in the provisions of medical law. Here, the term "standard" may refer to a certain pattern or model of conduct related to providing healthcare services. Defined standards are norms that define the fundamental requirements that are set in connection with providing healthcare services or organising the process of their provision. However, in legal regulations this term may be expressed with the use of certain synonyms, such as "good practices", "recommendations" or "procedures".

In medical law, standards take various forms of legal regulations, and sometimes they do not have normative values. Due to that, they differ in terms of validity, from acts of commonly binding law (e.g. ordinances of the Minister of Health), through acts of internal law (such as by-laws or procedures established by the manager of the healthcare entity) to guidelines or recommendations that support the process of providing healthcare services [2]. An example of a standard in medical law, where the legal regulations directly refer to the notion, is the Ordinance of the Minister of Health of August 12 2020 on the organisational standard of teleconsultations in primary healthcare (Journal of Laws of 2022, item 1194, hereinafter: the "Ordinance"). It was issued base on Art. 22 item 5 of the Act of April 15 2011 on Medical Activity (Journal of Laws of 2022, item 633 incl. further amendments, hereinafter referred to as: the "Act on Medical Activity" or "AMA"), and it is one of the six organisational standards in healthcare that were established by the competent Minister for health.

The requirements contained in the Ordinance are obligatory for entities that conduct medical activity within the scope covered by the standard. Obviously, it is possible to fulfil requirements that are beyond the standard, particularly if it is required by specific circumstances of providing healthcare services. On the other hand, it is unacceptable not to comply with the requirements defined in organisational standards for healthcare, as they are considered to be minimum requirements. Therefore, the nature of the organisational standard for medical teleconsultations is that of commonly binding law that defines an obligatory model of conduct and contains norms that specify the fundamental, minimum requirements.

Objective, materials and methods

The article provides an analysis of the relations between the organisational standard for teleconsultations in primary healthcare and the personal data protection law. The author formulates the thesis that such basic organisational requirements for teleconsultations are insufficient to comply with all the regulations on the protection of personal data. The research was conducted with the use of the methods applied in legal sciences, i.e. the dogmatic and theoretical legal methods. The subject of the analysis were normative acts, guidelines and recommendations related to personal data protection, as well as academic studies and subject literature.

Unfortunately, the analysed issue has not been analysed in detail in existing subject literature. The authors of few overview works provided a wider discussion of the legal aspects of telemedicine or teleconsultations, pointed to the need to ensure data security and indicated the related threats. As a result, it is necessary to provide deeper insights in this area. The article presents the legal state as of the 31st of May 2023.

The notion of medical teleconsultation

The term "teleconsultation" was defined in §2 item 3 of the ordinance as a healthcare service that is provided remotely with the use of ICT or communication systems. The person providing a teleconsultation may be a physician, a nurse or a midwife, who provide services at the primary healthcare service provider defined in Art. 9 item 1 of the Act of October 27 2017 on Primary Healthcare (Journal of Laws of 2022, item 2527, hereinafter: the "Act on Primary Healthcare" or the "APH"). Furthermore, pursuant to Art. 2 item 1 (10) and Art. 3 item 1 of the Act on Medical Activity, healthcare services are actions that are aimed at maintaining, saving, restoring, or improving health and other medical actions that result from the treatment process or from separate provisions that regulate the principles of providing them, which may be provided through ICT or communication systems.

Thus, teleconsultation is a traditional consultation provided to a patient who is in a location other than that of the service provider, i.e. a de-localised consultation. The regulations do not specify the location where the person providing the services should provide them. However, they state that, for healthcare services that are provided through ICT or communication systems, the place of providing the services is the location of the person performing a medical occupation who provides these services. Due to that, a teleconsultation provided for a patient who is staying outside the territory of Poland should be governed by the principles of the national legal system and be subject to the same requirements as a teleconsultation provided for a patient who remains in Poland at that time. The regulations do not specify the communication

system, either. Therefore, telephone calls, calls with the use of video communication applications or electronic messaging systems are acceptable [3].

Currently, teleconsultations have become a part of telemedicine [3, 4]. Telemedicine means providing healthcare services with the use of ICT systems in situations when the healthcare employee and the patient (or two healthcare employees) are not in the same location. The services provided in telemedicine involve the transmission of data and medical information (in forms of text, image, sound, or any other forms) that are necessary for preventive actions, diagnosis, treatment, and checking the health of the patient.

Telemedicine includes a wide range of varied services. The ones that are most commonly listed in mutual evaluations are: teleradiology, telepatomorphology, teledermatology, teleconsultations, telemonitoring, telesurgery, and teleophtalmology. Other possible types of telemedicine services are call centres for patient services or online information centres for patients, remote consultations (e-consultations) and videoconferences for healthcare employees [5].

In conclusion, a medical teleconsultation is a healthcare service that is provided remotely by a competent subject, i.e. a physician, nurse or midwife, with the use of ICT or communication systems. The place of providing the teleconsultation is determined by the location of the person who provides the service. However, legal regulations do not provide specific requirements concerning the communication tools used. As teleconsultations are part of telemedicine, the guidelines for providing telemedicine services are applied.

Teleconsultations and issues related to the protection of personal data

For healthcare services that are provided in form of teleconsultations, the principles of providing services and the scope of duties of the physician remain the same. During teleconsultation, one should remember, first of all, about the main duties related to the diagnosis and treatment of illnesses. At the same time, compliance with all legal requirements concerning the security of processing medical data must be maintained.

As legal regulations do not specify the communication tools that may be used for teleconsultations, the service provider may choose them at his/her own discretion, which carries the risk of errors or violations. The requirement to meet the relevant organisational and technical conditions is a priority, in particular from the point of view of the security of personal data of the patients who use such healthcare services [4]. This is also connected to the main risk of teleconsultations, as they involve a threat of the disclosure of information that is subject to medical confidentiality and of sensitive personal data [3]. This opens a wide field for consideration of the scope of responsibility under the provisions of the 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) (Official Journal of the EU, L 119 of 4.05.2016, p. 188, hereinafter: GDPR).

The GDPR became effective on May 25 2018. Since that time, the issues related to personal data protection have enjoyed growing interest, which leads to new obligations and an increasing number of the results of inspections of their implementation by the Head of the Personal Data Protection Office (hereinafter: the Head of the PDPO) and administrative courts. The legal instrument that complements the GDPR and regulates the protection of personal data in Poland is the Act of May 10 2018 on Personal Data Protection (Journal of Laws of 2019, item 1781 incl. further amendments).

The protection of personal data of natural persons is one of the fundamental rights. It is guaranteed in Art. 8 item 1 of the European Convention on Human Rights, Art. 8 item 1 of the Charter of Fundamental Rights of the European Union, and in Art. 47 and 51, item 1 of the Constitution of the Republic of Poland, pursuant to which everyone has the right to legal protection of their private life, including the personal data concerning this person. Furthermore, nobody may be obliged to disclose their personal data in a manner other than statutory. The main objective of the GDPR is not only to ensure the right to the protection of personal data of natural persons, but also to ensure the free movement of such data. This dualist approach to the objectives is in line with the concept that the organisation of processing personal data should serve humanity (objective 4 of the GDPR), without obstructing the free movement of such data, which is important for both public and private sectors in terms of conducting business activity and maintaining fair competition.

The notions that are essential for our considerations are those defined in the GDPR, such as the data controller and the processor (i.e. the entity that processes data). The controller means the natural or legal person or entity which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4, point 7 of the GDPR). Joint controllers are two or more controllers who jointly determine the purposes and means of processing (Art. 26 of the GDPR). A natural or legal person or entity which processes personal data on behalf of the controller is referred to as the processor (Art. 4, item 8 of the GDPR). Hence, the personal data controller may be both the healthcare provider that, for example, employs the physician, and the person who provides a teleconsultation and is a sole medical practitioner. In the light of the GDPR, it is the controller who bears the main responsibilities connected to the protection of personal data. Due to that, a healthcare facility should have a binding security policy and the compliance with such policy should be one of the obligations of its employees (e.g. a physician who is employed based on a civil law contract). In such event, the healthcare provider should act in compliance with the security policy and other internal documents that regulate the principles of protecting medical data, including the rules for handling medical documentation [6].

In the context of the adherence to standards, one should remember the principle of accountability provided in

Art. 5 item 2 of the GDPR, which states that every controller shall be responsible for, and be able to demonstrate compliance with the provisions of the GDPR. Due to that, one should take into account the provisions of Art. 24 item 3 of the GDPR, pursuant to which the adherence, among others, to approved codes of conduct as referred to in Article 40 may be used as an element by which to demonstrate compliance with the obligations of the controller. Such code of conduct that has been approved by the Head of the PDPO under the GDPR is the Code of Conduct concerning the protection of personal data that are processed in small healthcare facilities (the so-called Zielona Góra Agreement) of November 9 2022 (hereinafter: the ZGA Code) [7], which contains guidelines concerning teleconsultations. The Code emphasised that in the provision of teleconsultations it is important to ensure the identification of patients who use them, safe conditions of providing teleconsultations, and the adequate means of technical security in their provision (Point 12 of the ZGA Code). Other recommended solutions in this respect are also provided in the Guidelines on exercising the right to information remotely by entitled persons, which were prepared by the Ombudsman for Patients'' Rights and the Head of the PDPO [8].

Organisational standards of teleconsultations in the light of the GDPR

The provisions of the Ordinance regulating the organisational standards for teleconsultations in primary healthcare do not refer directly to the category of personal data protection or to the provisions of the GDPR. At the same time, however, they regulate three important areas that involve the need to ensure the protection of personal data:

- identification of the patient (§3 item 3 of the Ordinance);
- compliance with the principles of confidentiality (§3 item 5 of the Ordinance);
- application of technical means that protect the personal data of the patient (§ 3 item 6 of the Ordinance).

Standard of patient identification

The first organisational standard for teleconsultations refers to patient identification, i.e. verification of the patient's identity by the person who provides the teleconsultation. This should take place before the telecommunication starts. The identity is confirmed based on the data that are specified in Art. 25 item 1(1) of the Act of November 6 2008 on Patients' Rights and the Ombudsman for Patients' Rights (Journal of Laws of 2022, item 1876 incl. further amendments, hereinafter referred to as: the "Act on Patients' Rights" or the "APROPR") that are provided by the patient via ICT systems or communication systems. This refers to the identification data of the patient, including the surname and first name(s), date of birth, assigned gender, residence address, PESEL number (if it has been assigned, for newborns the PESEL number of the mother, and for persons who have not been assigned a PESEL number – the type and number of the identification document). Additionally, if the patient is a minor, a person who is legally incapacitated or incapable of expressing informed consent, the first name, surname, and residence address of the statutory representative. Moreover, the identity is to be confirmed based on the data provided in medical documentation or in the declaration of choice specified in Art. 10 of the Act on Primary Healthcare, or by presenting an identification document by the patient during the provision of healthcare services in form of a video consultation, or through the electronic patient's account created by the patient to verify their identity in person, or in the manner specified in Art. 20a item 18 of the Act of February 17 2005 on computerisation of activity of entities implementing public tasks (Journal of Laws of 2023, item 57).

In the light of the GDPR, the notion of personal data applies to all information concerning an identified or identifiable natural person, while the person may be identified by reference to an identifier such as a name, an identification number (PESEL) or to one or more factors specific to the identity of that natural person (Art. 4, item 1 of the GDPR). At the same time, the GDPR provides separate definitions of "genetic data", i.e. personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question, and "biometric data", being personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data. Moreover, the GDPR regulates the category of "data concerning health", i.e. 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. These three distinguished data categories constitute, at the same time, so-called sensitive data that require special basis for processing (Art. 9 items 1 and 2 of the GDPR). The European legislator also explained that personal data concerning health 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. These data include:

- information about the natural person collected in the course of the registration for, or the provision of, health care services;
- a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes;
- information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples;
- and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an *in vitro* diagnostic test (Recital 35 of the GDPR).

It should also be noted that the GDPR regulates pseudonymised data, i.e. data processed in such a manner that the personal data can no longer be attributed to a specific

data subject (pseudonyms) without the use of additional information, provided that such additional information is kept and secured separately (Art. 4, item 5 of the GDPR). As opposed to anonymisation, pseudonymisation is a reversible action that is used to protect personal data. On the other hand, anonymisation is a process that transforms personal data into non-personal data. As a result of the process, such data do not refer to an identified or identifiable natural person, so it becomes impossible to identify the data subject. Such anonymised data are not regulated by the GDPR, as they are permanently and irreversibly depersonalised.

During teleconsultation, the identity of the patient is verified by processing his/her personal data. Processing of personal data means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available (Art. 4 item 2 of the GDPR). The filing system is any structured set of personal data which are accessible according to specific criteria, i.e. any structured set of two or more items of personal data (Art. 4 item 6 of the GDPR), for example medical documentation. The content of medical documentation and the rules for maintaining, storage, and disclosure of medical documentation are regulated separately, in Art. 23–30a of the Act on Patients' Rights and the Ombudsman for Patients' Rights).

In this context, the basis for processing so-called sensitive data is important. As a rule, the processing of genetic and biometric data and data concerning health is prohibited, unless the data subject has given explicit consent or the processing is necessary to protect the vital interests of the data subject and the data subject is physically or legally incapable of giving consent (Art. 9 item 2 (a) and (c) of the GDPR).

Other exceptions that enable the processing of sensitive data in the context of providing healthcare services include:

- processing that 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, provided that in such event the personal data may be processed by or under the responsibility of a professional subject to the obligation of professional secrecy (Art. 9 item 2 (h) and item 3 of the GDPR);
- processing that is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Art. 9 item 2 (i) of the GDPR).

The guidelines of the ZGA Code that refer to sources of identity verification and problems with videoconferences may be helpful in identifying the patient. Based on the assumption that the patient is known to the primary healthcare service provider, the source of data for verification of their identity on part of the person providing the teleconsultation may be, depending on the situation, the medical documentation, declaration of choosing the primary healthcare physician, nurse or midwife or the Internet Patient's Account, while on part of the patient such sources are: their identification document presented during the teleconsultation (if it is provided in form of a video call) or the patients themselves, who present their information to the person providing the teleconsultation. It is, however, inacceptable to verify the identity of the patient based on an identity document during a video teleconsultation if the video call is recorded, due to the lack of legal basis for recording and storing the image of such document. If the technical settings allow, recording the video call should be stopped for the moment of showing the identity document (point 12.1.1. of the ZG Code).

In conclusion, the standard of patient identification includes four ways to confirm the identity:

- based on data provided by the patient;
- based on medical documentation or declaration of choice;
- based on the online patient's account;
- for video consultations – based on the presented identification document.

In this context, it should be remembered that the personal data must be accurate in updated if necessary. The healthcare provider that provides the teleconsultation should take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (Art. 5 item 1 (d) of the GDPR). This is related to the rights of data subjects, i.e. the right to access their personal data (Art. 15 of the GDPR), the right to demand the data controller to rectify or complete the data (Art. 16 of the GDPR), and the right to restrict the processing of personal data, he accuracy of the personal data is contested by the data subject (Art. 18 of the GDPR). The data controller should not refuse to acquire additional information from the data subject in order to facilitate the exercising of their rights (Recital 57 of the GDPR), which may serve as a guideline if patients provide excessive data. One should however bear in mind that in the light of the principle of data minimisation, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (Art. 5, item 1 (c) of the GDPR).

Confidentiality standard

The second organisational standard of teleconsultations states that the teleconsultation should be provided in conditions that enable confidentiality, including preventing unauthorised access to information transmitted via ICT systems or communication systems in connection with the teleconsultation. The telemedicine service is a service, whose nature requires providing it in such a way that prevents unauthorised persons to access the transmitted content. The obligations concerning confi-

dentiality and security of information are supported by the need to maintain confidential the information related to the patient and obtained in connection with providing healthcare services. The service provider is obliged to ensure that no third parties participate in providing the teleconsultation and that the information provided by the patient cannot be heard outside the room where the service provider is staying. Moreover, the service provider should also implement suitable mechanisms to protect the provided digital data from unauthorised access. Due to the absence of physical contact, it is also reasonable to implement mechanisms that guarantee unambiguous identification. For this purpose, it is recommended to share the data between individual accounts [4]. In this context, the guidelines on the aspects of ensuring the confidentiality of teleconsultations and verifying the patient's identity, provided in the Guidelines of the Supreme Medical Council on providing telemedicine services [6] still remain valid. The guidelines of the ZG Code that recommend that the teleconsultation should take place in such location where it is impossible for unauthorised persons to overhear a telephone or video conversation or to look at the screen, are also consistent. Remote services should be provided in a separate, closed room that cannot be accessed by patients or other unauthorised persons. If the teleconsultation is recorded, the patient must be informed about this before the start of consultation, and information sent by e-mail should be sent from an e-mail account that is inaccessible for unauthorised persons, with means of security that have been previously consulted with an IT technician and data protection inspector (item 12.2 of the ZG Code).

Therefore, the confidentiality standard involves the necessity to prevent unauthorised access to the information transmitted during the teleconsultation, which is consistent with the obligation to maintain confidential all information about the patient that was obtained in connection with performing a medical profession. Only authorised persons should participate in the teleconsultation, i.e. no third parties should be present. The provided information should not be heard by third parties outside the room where the service provider is located. Additionally, suitable mechanisms should be implemented to protect the transmitted content from unauthorised access.

Standard of safe technical and organisational solutions

The third standard concerns the cases when information about the patient's health status is transmitted, including digital representations of medical documentation, by means of ICT systems. This standard involves the use by the primary healthcare service provider of such technical and organisational solutions that guarantee that electronic documents in graphic and text forms are transmitted in a way that ensures their integrity and protection against unauthorised use, accidental or unlawful destruction, loss, modification, unauthorised disclosure or access. Therefore, the primary healthcare service provider is obliged to protect the patient from the violation of their personal data. Such violations include the security violation that leads to accidental or unlawful destruction, loss, modification, unauthorised disclosure of or access to personal data that are transmitted, stored or processed in any other way (Art. 4, item 12 of the GDPR). However, in order to comply with this standard, the primary healthcare service provider has to fulfil all its obligations of the data controller that are not mentioned in the Regulation. At the same time, the standard of integrity and confidentiality of personal data results from the GDPR and the principle that personal data must be processed violations in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Other requirements of the GDPR

In analysing the provisions of the Ordinance, it should be noted that they focus mainly on the duties that are performed in direct connection with a specific teleconsultation. It is during such teleconsultation that the service provider is obliged to maintain confidentiality and identify the patient immediately before the start of consultation. Only the issues of technical means of security refer to transmitting information about the patient's health status, which may take place before, during, or after the teleconsultation. Although the Ordinance does not specify the timeframe of the teleconsultation, so it is impossible to determine when it precisely starts and what elements in includes, in the light of personal data protection it should be noted that the organisational standards refer to actions connected with the healthcare service in itself, without focusing on systemic aspects. Meanwhile, jurisprudence demonstrates that in the light of the GDPR the legislation authorities have diverged from the static determination of the technical and organisational measures required from the data controller towards a dynamic assessment of the adopted means of security. This means that both the data controller and processor are obliged to implement adequate security measures. Pursuant to the provisions of Art. 32 item 1 of the GDPR, 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. The assessment of the adequacy of the level of security takes into account, in particular, the risk connected to processing, resulting from accidental or unlawful destruction, loss, modification, unauthorised disclosure of or access to personal data that are transmitted, stored, or processed in any other way.

In consequence, the binding legal regulations do not provide a list of adequate security measures, and it is the data controller who is obliged to make the relevant assessment and to select means of security that are adequate, among others, to the current state of technical knowledge or to the risk of violation of rights (judgment of the Supreme Administrative Court of February 9 2023, III OSK 3945/21, CBOSA). Pursuant to the GDPR, the primary healthcare service provider as the data controller is obliged to conduct the risk assessment prior to the commencement of processing the data with the use of adequate technical and organisational measures that ensure compliance with the GDPR and the accountability of processing personal data. These measures should take into account the nature, scope, context, and purposes of

processing and the risk of violating the rights and freedoms of natural persons (Recital 74 of the GDPR). However, the Regulation does not provide any specific solutions that ensure adequate protection of personal data. The guidelines of the ZG Code related to the implementation of such measures are also very general. The Code only points out that, in order to ensure that the transmission of information during teleconsultations should take place in a way that will ensure its integrity and protect it from unauthorised access, accidental or unlawful destruction, loss, modification, unauthorised disclosure or access, the service provider should use technical and organisational solutions that have been consulted with an IT technician (in terms of technical security measures) and with the data protection inspector (hereinafter: DPI) in terms of compliance with the requirements of personal data protection and information security (point 12.3 of the ZG Code).

Further obligations to ensure the security of data processing that were not included in the Ordinance are: the necessity to maintain a record of processing activities (Art. 30 items 1 and 4 of the GDPR), to notify personal data breach to the supervisory authority and to document such breaches (Art. 33 items 1, 2, and 5 of the GDPR) and to communicate the personal data breach to the data subject (Art. 34 item 1 of the GDPR). The data controller is also obliged to perform the informational duties (Articles 13 and 14 of the GDPR) and to exercise the rights of data subjects (Art. 15–22 of the GDPR). In order to prepare to perform these duties with respect to providing teleconsultations, the data controller is required to implement a personal data protection system and an adequate organisation of work at the preliminary stage, before providing teleconsultations.

The healthcare provider that performs the activity as the data controller is also obliged to meet the requirements concerning the selection of the appropriate processor (Art. 28 items 1 and 5 and Art. 32 items 1 and 2 of the GDPR). In creating medical documentation, the data controller must follow the principles provided in the GDPR, although in practice, due to the enormous amounts of data, medical documentation is often maintained by specialist companies. However, the Ordinance does not contain the relevant guidelines. Upon entering into an agreement with such a company, the healthcare facility should enter into an agreement on entrusting the processing of personal data that will meet the requirements of Art. 28 of the GDPR. At the same time, the data controller is obliged to use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject. Therefore, pursuant to the GDPR, the agreement on entrusting data processing should contain, among others, the subject and duration of processing, the nature and purpose of processing, type of data, categories of data subjects, rights and obligations of the data controller and a clause obliging the persons who are authorised to process personal data to maintain their confidentiality [9]. In some cases, the data controller will be obliged to appoint a Data Protection Inspector. Appointing a DPI is mandatory if the main activity of the data controller consists in large-scale processing of special categories of personal data, including data concerning health status. The main duties of the DPI will include notifying the data controller, the processor, and employees who process personal data about their obligations under the GDPR, monitoring compliance with the GDPR and cooperating with the supervision authority. The GDPR formulates the obligations of the Inspector in a general way, without specifying the mode or periods for their fulfilment. The PDI shall perform an advisory and verification function with respect to the activities of the data controller [10], also concerning the provision of telemedicine services.

Conclusions

It was the intention of the legislator that the organisational standards would define the interrelations and the assignment of duties (rights and responsibilities) related to providing healthcare services. This may refer, in particular, to the qualifications of the healthcare personnel who participate in providing healthcare service, the sequence of performing medical actions in the diagnostic and treatment process and the relations between the competences of the personnel, as well as the scope of the personnel's responsibility [11]. In this light, the organisational standard of teleconsultations, which, as far as personal data protection is concerned, refers only to the identification of the patient and the need to ensure confidentiality and security of the technical and organisational solutions, in fact only reproduces the general requirements for all data controllers, to a limited extent. The standard does not provide any specific practical solutions in these narrowly defined areas, either. One may state that, as far as personal data protection is concerned, the organisational standard for teleconsultations neither takes into consideration nor defines the tasks, obligations, and scope of responsibility of persons who provide teleconsultations and primary healthcare service providers. Moreover, it does not provide them with any specific and practical organisational guidelines. In this respect, the ZG Code or the guidelines of the Supreme Medical Council may be considered more important. As a result, the minimum requirements set by the binding organisational standard for teleconsultations defined in the Ordinance are too low. They are insufficient to fulfil all the obligations of the data controller that result from the GDPR. Due to that, teleconsultations should, in fact, be organised based on higher requirements than those that were foreseen by the legislation authorities. These requirements must take into account the implementation of procedures of conducting the calls and disclosing sensitive data concerning the patient's health remotely, in order to ensure the appropriate level of security and confidentiality. The procedures should include instruction manuals for using IT hardware, technical support, and the principles of conduct in the event of violation of personal data protection, including notifying the Data Protection Inspector. It is necessary to implement procedures in order to meet the individual rights of data subjects, including the rules for informing them about these rights, in particular considering the special basis for processing data for the purposes of providing healthcare services. The adopted procedures should take into consideration emergency circumstances, such as life-threatening situations, when it is necessary to provide aid immediately, or such situations as the lack of cooperation and other improper use of healthcare services.

In every case, the data should be processed to the necessary extent. Due to that, considering the principle of data minimisation, conversations with patients who call should be recorded only in exceptional circumstances, taking into account their purpose and risk analysis.

The healthcare facility should have a security procedure in place, along with mechanisms that ensure compliance. Healthcare providers should introduce the records required under the GDPR, as well as a record of authorisations for persons who act on behalf of the data controller and have access to personal data. At the same time, the provider should ensure that the orders to process data for employees (based on by-law or connected to their scope of duties) are formulated in a transparent way, so as to comply with the requirements of Art. 29 of the GDPR.

In taking actions to protect personal data during teleconsultations it is worth consulting the codes of conduct approved by the Head of the PDPO. Currently, although the GDPR has been in force for over 5 years, only two such national codes have been approved: the ZG Code and the Code of Conduct for the Healthcare Sector, created by the Polish Federation of Hospitals. However, in applying the existing standards, guidelines, and recommendations, one should first of all adopt a systemic point of view, so that the measures applied to protect personal data are adequate to the specific nature of medical teleconsultations and take into account the typical related risks.

References

1. Niżnik-Dobosz I. Pojęcie standardu w prawie administracyjnym, jego nauce i w praktyce. In: Duniewska Z, Stahl M, Rabiega-Przyłęcka A, eds. Standardy współczesnej administracji i prawa administracyjnego. Warszawa–Łódź, Wolters Kluwer Polska, 2019: 39–57
2. Budzisz R. Standardy organizacyjne opieki zdrowotnej oraz standardy akredytacyjne w ochronie zdrowia jako przykłady standardów w prawie medycznym. In: Duniewska Z, Stahl M, Rabiega-Przyłęcka A, eds. Standardy współczesnej administracji i prawa administracyjnego, Warszawa–Łódź, Wolters Kluwer Polska, 2019: 492–505
3. Łazarska A, Niemczyk S. Standardy prawno-medyczne udzielania teleporad a dobro pacjenta – wyzwania i zagrożenia. In: Chmielnicki P, Minich D, eds. Prawo jako projekt przyszłości. Warszawa, Wolters Kluwer Polska, 2022: 227–256
4. Czaplińska M, Sakowska-Baryła M. Telemedycyna i teleporady w dobie pandemii – aspekty prawne i organizacyjne. Mon Praw, 2022; 12: 648–650
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and socjety https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52008DC0689 (access: 31.05.2023)
6. Resolution No. 89/20/P-VIII of the Presidium of the Supreme Medical Council of July 24 2020 on adopting the guidelines for providing telemedicine services. https://nil.org.pl/aktualnosci/4980-wytyczne-dla-udzielania-swiadczen-telemedycznych?previewmode=4ffbd5c8221d-7c147f8363ccdc9a2a37 (access: 31.05.2023)
7. Code of Conduct concerning the protection of personal data that are processed in small healthcare facilities (Zielona Góra Agreement) of November 9 2022, https://uodo.gov.pl/pl/426/1110 (access: 31.05.2023)
8. Guidelines on the realisation of the right to information remotely, by entitled persons, Ombudsman for Patients' Rights, Head of the Personal Data Protection Office, https://www.gov.pl/web/rpp/wytyczne-dotyczace-realizacji--prawa-do-informacji-przez-osoby-uprawnione-na-odleglosc (access: 31.05.2023)
9. Marcinkowski B. Ochrona danych osobowych pacjenta w telemedycynie w świetle RODO. In: Lipowicz I, Szpor G, Świerczyński M, eds. Telemedycyna i e-zdrowie Warszawa, Wolters Kluwer Polska, 2019: 174–180
10. Fundacja Telemedyczna Grupa Robocza *(Foundation Telemedicine Working Group)*. Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia? Warszawa, Fundacja Telemedyczna Grupa Robocza, 2018: p. 86. http://telemedycyna-raport.pl/#raport, (access: 31.05.2023)
11. Grounds for the Draft of the Act amending the Act on Medical Activity and certain other Acts. Druk Sejmowy No. 562, Sejm of the 8th Term. https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=562 (access: 31.05.2023)