STANDARDY ORGANIZACYJNE TELEPORAD MEDYCZNYCH A OCHRONA DANYCH OSOBOWYCH

Organizational standards for medical teleconsultations and personal data protection

Łukasz Nosarzewski

Katedra Prawa Administracyjnego, Konstytucyjnego i Prawa Pracy na Wydziale Prawa i Administracji, Uczelnia Łazarskiego, Polska

Łukasz Nosarzewski – ORCID 0000-0001-8769-6757

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.

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.

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

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

DOI 10.53301/lw/174973

Praca wpłynęła do Redakcji: 17.08.2023

Zaakceptowano do druku: 02.11.2023

Autor do korespondencji:
Łukasz Nosarzewski
Katedra Prawa Administracyjnego, Konstytucyjnego i Prawa Pracy na Wydziale Prawa i Administracji
Uczelnia Łazarskiego
ul. Świeradowska 43, 02-662, Warszawa
e-mail: l.nosarzewski@wp.pl

Wstęp

W nauce prawa standardem można opisać treść norm prawnych określających względnie wymiernie cechy lub atrybuty danego dobra albo zachowania danego podmiotu prawa w nawiązaniu do dorobku poszczególnych dziedzin nauki po to, aby dzięki wskazaniu tych cech lub atrybutów uzyskać względnie ściśle oznaczony „produkt". Prawo sięga do pojęcia standardu, kiedy chce zapewnić jednolity, ale i w jakiś sposób ewolucyjny, rozwojowy poziom realizacji podstawowych celów i zadań państwa. W doktrynie prawa administracyjnego pojęcie standardu pojawia się w wielu kontekstach, a sama jego treść pozostaje w różnych relacjach z prawem. W niektórych przypadkach prawo jest tu konstytutywne albo deklaruje zobiektywizowane właściwości prawa natury lub je przekształca, w innych – odsyła do kryteriów i ocen wypracowanych poza systemem prawa, uznając je w pewnych zakresach jednak za tak istotne dla funkcjonowania społeczeństwa, że różnorodnie, wprost lub pośrednio, sankcjonuje ich realizację. Jednocześnie prawo administracyjne zapewnia w swoich regulacjach byt dokumentów normalizacyjnych opracowywanych przez uprawnione podmioty i komitety techniczne [1]. Pojęcie standardu nie jest więc nowe dla doktryny prawa, chociaż w przepisach prawa medycznego nie zostało zdefiniowane. Standardem można nazwać tu pewien wzorzec, model postępowania związanego z udzielaniem świadczenia zdrowotnego. Ustalone standardy to normy wyznaczające podstawowe wymagania stawiane w związku ze udzielaniem lub organizacją procesu udzielania świadczeń zdrowotnych. W przepisach prawa pojęcie to może jednak przybierać inne, bliskoznaczne określenia, jak „zasady dobrej praktyki", „zalecenia" czy „procedury".

Standardy w prawie medycznym znajdują różne formy regulacji prawnej, a czasem nie mają waloru normatywnego. W związku z tym różnią się mocą obowiązywania – od aktów prawa powszechnie obowiązującego (np. rozporządzenia ministra zdrowia) przez akty prawa wewnętrznego (np. regulaminy, procedury ustalane przez kierownika podmiotu leczniczego), do zaleceń czy rekomendacji wspierających proces udzielania świadczeń zdrowotnych [2]. Przykładem standardu w prawie medycznym, gdzie regulacje prawne wprost odnoszą się do tego pojęcia, jest rozporządzenie ministra zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej (Dz.U. z 2022 r. poz. 1194; dalej: „rozporządzenie" lub „r.s.o.t."). Zostało ono wydane na podstawie art. 22 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2022 r. poz. 633, z późn. zm.; dalej: „u.d.l.") i stanowi jeden z sześciu standardów organizacyjnych opieki zdrowotnej ustalonych przez ministra właściwego do spraw zdrowia.

Dla podmiotów wykonujących działalność leczniczą w zakresie objętym standardem wymogi w nim określone mają charakter obligatoryjny. Oczywiście możliwe jest realizowanie wymogów ponadstandardowych, zwłaszcza jeżeli wymagają tego konkretne okoliczności udzielania świadczeń zdrowotnych. Niedopuszczalne zaś jest niewypełnianie norm ustalonych w standardach organizacyjnych opieki zdrowotnej, gdyż uznaje się, że mają one charakter minimalny [2]. Tym samym standard organizacyjny teleporady medycznej ma charakter prawa powszechnie obowiązującego, wyznaczającego wzorzec, model obligatoryjnego postępowania, zawierający normy określające minimalne, podstawowe wymagania.

Cel pracy, materiał i metody

W artykule poddano analizie relacje między standardem organizacyjnym teleporady w ramach podstawowej opieki zdrowotnej (POZ) a prawem ochrony danych osobowych, formułując tezę, że takie podstawowe wymagania organizacyjne dla teleporady nie są wystarczające, aby zachować wszystkie wymogi ochrony danych osobowych. W pracy wykorzystano metody z zakresu nauk prawnych – dogmatyczną i teoretycznoprawną. Analizą objęto akty normatywne, zalecenia i wytyczne z obszaru ochrony danych osobowych oraz opracowania naukowe i piśmiennictwo.

W literaturze przedmiotu podjęte zagadnienie nie zostało poddane szczegółowym badaniom. W nielicznych pracach poglądowych autorzy szerzej odnosili się do prawnych aspektów telemedycyny lub teleporad, wskazując na konieczność zapewnienia bezpieczeństwa danych i zagrożenia z tym związane. Stąd potrzeba pogłębienia refleksji w tym obszarze. Artykuł prezentuje stan prawny na 31 maja 2023 r.

Pojęcie teleporady medycznej

Pojęcie teleporady zostało zdefiniowane w § 2 pkt 3 r.s.o.t. jako świadczenie zdrowotne udzielane na odległość przy użyciu systemów teleinformatycznych lub systemów łączności. Osobą udzielającą teleporady może być lekarz, pielęgniarka lub położna, którzy udzielają świadczeń u świadczeniodawcy POZ, o którym mowa w art. 9 ust. 1 ustawy z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz.U. z 2022 r. poz. 2527; dalej: u.p.o.z.). Zgodnie zaś z art. 2 ust. 1 pkt 10 i art. 3 ust. 1 u.d.l. świadczenie zdrowotne to działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania, które mogą być udzielane za pośrednictwem systemów teleinformatycznych lub systemów łączności.

Teleporada to klasyczna porada udzielana pacjentowi znajdującemu się w innym miejscu niż osoba udzielająca świadczeń, czyli konsultacja odmiejscowiona. Przepisy nie dookreślają miejsca, w którym osoba udzielająca świadczeń ma ich udzielać, chociaż wskazują, że w przypadku udzielania świadczeń zdrowotnych za pośrednictwem systemów teleinformatycznych lub systemów łączności miejscem udzielania świadczeń jest miejsce przebywania osób wykonujących zawód medyczny udzielających tych świadczeń. Dlatego teleporada na rzecz pacjenta przebywającego poza granicami kraju powinna odbywać się na zasadach krajowego porządku prawnego i podlega takim samym wymogom jak teleporada na rzecz pacjenta przebywającego w Polsce. Przepisy nie precyzują również systemu łączności. Dopuszczalne jest więc połączenie telefoniczne lub przy wykorzystaniu aplikacji do połączeń wideo czy komunikatorów elektronicznych [3].

Obecnie teleporada stała się częścią telemedycyny [3, 4]. Telemedycyna jest to bowiem świadczenie usług zdrowotnych z wykorzystaniem technologii informacyjno-komunikacyjnych w sytuacji, gdy pracownik ochrony zdrowia i pacjent (lub dwaj pracownicy ochrony zdrowia) nie znajdują się w tym samym miejscu. Usługi telemedyczne wiążą się z przesyłaniem danych i informacji medycznych (jako tekstu, obrazu, dźwięku lub w innej formie), które są konieczne do działań prewencyjnych, diagnozy, leczenia i kontroli stanu zdrowia pacjenta.

Telemedycyna obejmuje szeroki i różnorodny zakres usług. Do najczęściej wymienianych we wzajemnych ocenach należą: teleradiologia, telepatomorfologia, teledermatologia, telekonsultacje, telemonitorowanie, telechirurgia i teleokulistyka. Inne możliwe ich typy obejmują centra telefonicznej obsługi pacjentów lub centra informacji online dla pacjentów, konsultacje na odległość (e-wizyty lekarskie) bądź wideokonferencje między pracownikami ochrony zdrowia [5].

Podsumowując, teleporada medyczna to świadczenie zdrowotne udzielane na odległość przez wykwalifikowany podmiot: lekarza, pielęgniarkę lub położną, przy użyciu systemów teleinformatycznych lub systemów łączności. Miejsce teleporady determinuje miejsce przebywania osoby udzielającej świadczenia. Przepisy prawa nie precyzują przy tym szczególnych wymagań dla stosowanych narzędzi komunikacji. Teleporada jest częścią telemedycyny, dlatego w zakresie jej udzielania aktualne pozostają wytyczne dla świadczeń telemedycznych.

Teleporady a problematyka ochrony danych osobowych

W przypadku świadczenia usług zdrowotnych w ramach teleporady zasady udzielania świadczeń i zakres obowiązków lekarza pozostają bez zmian. Podczas teleporady należy pamiętać przede wszystkim o podstawowych powinnościach związanych z rozpoznawaniem i leczeniem chorób. Równocześnie muszą być spełnione wszelkie wymogi prawne dotyczące bezpieczeństwa przetwarzania danych medycznych.

Skoro przepisy prawa nie precyzują, jakich narzędzi komunikacyjnych można używać podczas teleporady, decyzja w tym zakresie jest pozostawiona świadczeniodawcy, co obciąża go ryzykiem wystąpienia błędów czy naruszeń. Wymóg spełnienia odpowiednich warunków organizacyjnych i technicznych ma priorytetowe znaczenie, zwłaszcza z punktu widzenia bezpieczeństwa danych osobowych pacjentów korzystających z tego rodzaju świadczeń zdrowotnych [4]. Wiąże się to również z podstawowym ryzykiem teleporad, podczas których występuje zagrożenie ujawnienia informacji objętych tajemnicą lekarską i wrażliwych danych osobowych [3]. Otwiera to szerokie pole do rozważań na temat zakresu odpowiedzialności wynikającego z przepisów rozporządzenia 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) (Dz.U. L 119 z 4.05.2016, s. 188; dalej: RODO).

RODO weszło w życie w dniu 25 maja 2018 r. Od tego czasu problematyka ochrony danych osobowych cieszy się rosnącym zainteresowaniem, co wiąże się z nowymi obowiązkami oraz coraz liczniejszymi wynikami kontroli ich realizacji przez Prezesa Urzędu Ochrony Danych Osobowych (dalej: „PUODO") i sądy administracyjne. Uzupełniającym RODO instrumentem prawnym regulującym ochronę danych osobowych w Polsce jest ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781, z późn. zm.).

Ochrona danych osobowych osób fizycznych jest jednym z praw podstawowych. Jest gwarantowana w art. 8 ust. 1 Europejskiej Konwencji Praw Człowieka, art. 8 ust. 1 Karty Praw Podstawowych Unii Europejskiej, a także w art. 47 i 51 ust. 1 Konstytucji RP, zgodnie z którymi każdy ma prawo do ochrony prawnej życia prywatnego, w tym danych osobowych, które go dotyczą. Nikt też nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania dotyczących go informacji. Głównymi celami RODO jest nie tylko zapewnienie prawa do ochrony danych osobowych osób fizycznych, ale również swobodny przepływ tych danych. Taki dualizm celów wpisuje się w idee, aby organizacja przetwarzania danych osobowych służyła ludzkości (motyw 4 RODO), nie utrudniając przy tym swobodnego ich przepływu, istotnego dla sektora zarówno publicznego, jak i prywatnego w obszarze prowadzenia działalności gospodarczej i zachowania równej konkurencji.

Dla prowadzonych rozważań istotne znaczenie mają pojęcia określone w RODO, takie jak administrator i podmiot przetwarzający (tzw. procesor). Administratorem jest podmiot samodzielnie lub wspólnie z innymi ustalający cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO). Współadministratorami będą co najmniej dwaj administratorzy wspólnie ustalający takie cele i sposoby (art. 26 RODO). Podmiot, który przetwarza dane osobowe w imieniu administratora, zwany jest podmiotem przetwarzającym (art. 4 pkt 8 RODO). Tym samym administratorem danych osobowych może być zarówno podmiot leczniczy, przykładowo zatrudniający lekarza, jak i osoba udzielająca teleporady działająca w ramach indywidualnej praktyki lekarskiej. W świetle RODO to właśnie na administratorze spoczywa główny ciężar obowiązków związanych z ochroną danych osobowych. Dlatego w placówce medycznej powinna obowiązywać polityka bezpieczeństwa, której przestrzeganie stanowi jeden z obowiązków jej pracowników (np. lekarza pracującego na podstawie umowy cywilno-prawnej). W takim przypadku należy działać w sposób zgodny z polityką bezpieczeństwa i innymi dokumentami wewnętrznymi regulującymi zasady ochrony danych medycznych, w tym zasady postępowania z dokumentacją medyczną [6].

W kontekście realizacji standardów należy pamiętać o zasadzie rozliczalności z art. 5 ust. 2 RODO, sprowadzającej się do wymogu wykazania przez każdego administratora danych osobowych przestrzegania przepisów RODO. Dlatego należy mieć na względzie art. 24 ust. 3 RODO, zgodnie z którym stosowanie m.in. zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących

na nim obowiązków. Takim kodeksem zatwierdzonym zgodnie z wymogami RODO przez PUODO jest Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych (Porozumienie Zielonogórskie) z 9 listopada 2022 r. (dalej: Kodeks PZ) [7], w którym zawarto wytyczne w zakresie teleporad. Podkreśla się w nim, że przy realizacji teleporad istotne jest zadbanie o identyfikację pacjentów z nich korzystających, bezpieczne warunki ich udzielania oraz odpowiednie zabezpieczenia techniczne przy ich realizacji (pkt 12 Kodeksu PZ). Rekomendowane rozwiązania w tym względzie zawierają również Wytyczne dotyczące realizacji prawa do informacji przez osoby uprawnione na odległość, przygotowane przez Rzecznika Praw Pacjenta i PUODO [8].

Standardy organizacyjne teleporady w świetle RODO

Przepisy rozporządzenia regulującego standardy organizacyjne teleporady w ramach POZ nie odnoszą się wprost do kategorii ochrony danych osobowych czy przepisów RODO. Jednocześnie regulują trzy istotne obszary związane z koniecznością zapewnienia ochrony danych osobowych:

- identyfikacja pacjenta (§ 3 pkt 3 r.s.o.t.);
- zachowanie zasad poufności (§ 3 pkt 5 r.s.o.t.);
- stosowanie środków technicznych zabezpieczających dane pacjenta (§ 3 pkt 6 r.s.o.t.).

Standard identyfikacji pacjenta

Pierwszy standard organizacyjny teleporady obejmuje identyfikację pacjenta, czyli potwierdzenie jego tożsamości przez osobę udzielającą teleporady, co ma nastąpić przed jej udzieleniem. Potwierdzenie tożsamości odbywa się na podstawie danych, o których mowa w art. 25 ust. 1 pkt 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2022 r. poz. 1876, z późn. zm.; dalej: „u.p.p.r.p.p.”), przekazanych przez pacjenta za pośrednictwem systemów teleinformatycznych lub systemów łączności. Dotyczy to danych identyfikujących pacjenta, takich jak nazwisko i imię (imiona), data urodzenia, oznaczenie płci, adres miejsca zamieszkania, numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość. Dodatkowo w przypadku, gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania. Potwierdzenie tożsamości ma nastąpić ponadto na podstawie danych wskazanych w dokumentacji medycznej lub deklaracji wyboru, o której mowa w art. 10 u.p.o.z., lub po okazaniu przez pacjenta dokumentu potwierdzającego tożsamość, przy udzielaniu świadczenia opieki zdrowotnej w formie wideoporady, lub przy wykorzystaniu elektronicznego konta pacjenta utworzonego w wyniku potwierdzenia jego tożsamości osobiście lub w sposób określony w art. 20a ust. 1 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2023 r. poz. 57).

W świetle RODO pojęcie danych osobowych odwołuje się do wszelkich informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Identyfikacja możliwa jest zaś za pomocą identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny (PESEL) lub inne czynniki określające tożsamość osoby fizycznej (art. 4 pkt 1 RODO). RODO odrębnie definiuje przy tym „dane genetyczne”, dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o jej fizjologii lub zdrowiu i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej, „dane biometryczne”, wynikające ze specjalnego przetwarzania technicznego, dotyczące cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiające lub potwierdzające jej jednoznaczną identyfikację, takie jak wizerunek twarzy lub dane daktyloskopijne. Dodatkowo uregulowano kategorię danych dotyczących zdrowia, definiowanych jako dane o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej, a więc dane ujawniające informacje o stanie jej zdrowia. Te trzy wyodrębnione kategorie danych stanowią równocześnie tzw. dane wrażliwe wymagające szczególnych podstaw przetwarzania (art. 9 ust. 1 i 2 RODO). Prawodawca unijny wyjaśnił też, że do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą:

- informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej;
- numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby do celów zdrowotnych;
- informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych;
- wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne *in vitro* (motyw 35 RODO).

Należy również wskazać, że RODO podlegają dane spseudonimizowane, czyli przetworzone w taki sposób, by nie można ich było przypisać konkretnej osobie (pseudonimy) bez użycia dodatkowych informacji, pod warunkiem, iż takie dodatkowe informacje są przechowywane i zabezpieczane osobno (art. 4 pkt 5 RODO). Pseudonimizacja w przeciwieństwie do anonimizacji jest czynnością odwracalną, służącą zabezpieczaniu danych osobowych. Anonimizacja to z kolei proces zmiany danych osobowych w dane nieosobowe, prowadzący do tego, że dane takie nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a więc identyfikacja osoby, której dane dotyczą, nie będzie możliwa. Tak zanonimizowane dane nie podlegają RODO, gdyż są trwale i nieodwracalnie zdepersonalizowane.

Potwierdzenie tożsamości pacjenta w trakcie teleporady odbywa się poprzez przetworzenie jego danych osobowych. Przetwarzanie danych osobowych oznacza

operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie (art. 4 pkt 2 RODO). Z kolei zbiorem danych jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, czyli jakkolwiek uszeregowany zestaw co najmniej dwóch danych osobowych (art. 4 pkt 6 RODO), przykładowo dokumentacja medyczna. Zawartość dokumentacji medycznej, zasady jej prowadzenia, przechowywania i udostępniania zostały uregulowane odrębnie, w art. 23–30a u.p.p.r.p.p.

W tym kontekście istotna jest podstawa przetwarzania tzw. danych wrażliwych. Co do zasady zabrania się bowiem przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia, chyba że osoba, której dane dotyczą, wyraziła wyraźną zgodę albo przetwarzanie jest niezbędne do ochrony jej żywotnych interesów i jest ona fizycznie lub prawnie niezdolna do wyrażenia zgody (art. 9 ust. 2 lit. a i c RODO).

Odrębnymi wyjątkami umożliwiającymi przetwarzanie danych wrażliwych w kontekście udzielania świadczeń zdrowotnych są:

- przetwarzanie niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia, przy czym w takim przypadku dane osobowe mogą być przetwarzane przez lub na odpowiedzialność pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej (art. 9 ust. 2 lit. h i ust. 3 RODO);
- przetwarzanie niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową (art. 9 ust. 2 lit. i RODO).

Przy identyfikacji pacjenta pomocne mogą być wytyczne Kodeksu PZ odnośnie do źródeł weryfikacji tożsamości i problemów wideokonferencji. Przy założeniu, że pacjent jest znany świadczeniodawcy POZ, źródłem danych do weryfikacji jego tożsamości po stronie osoby udzielającej teleporady może być – w zależności od sytuacji – dokumentacja medyczna, deklaracja wyboru lekarza, pielęgniarki lub położnej POZ lub Internetowe Konto Pacjenta, zaś po stronie pacjenta takim źródłem jest jego dokument potwierdzający tożsamość, okazany w trakcie teleporady (jeśli teleporada odbywa się z wykorzystaniem połączenia wideo), lub sam pacjent, który przekazuje informacje na swój temat osobie udzielającej teleporady. Weryfikacja tożsamości pacjenta na podstawie okazania – w trakcie realizacji wideoporady – dokumentu potwierdzającego tożsamość nie jest dopuszczalna w sytuacji, gdy wideoporada jest nagrywana, ze względu na brak podstaw prawnych do utrwalania i przechowywania obrazu takiego dokumentu. Jeżeli warunki techniczne na to pozwalają, nagrywanie wideoporady należy przerwać na czas okazywania dokumentu potwierdzającego tożsamość (pkt 12.1.1. Kodeksu PZ).

Podsumowując, standard identyfikacji pacjenta obejmuje cztery sposoby potwierdzenia jego tożsamości:

- na podstawie przekazanych przez niego danych;
- na podstawie dokumentacji medycznej lub deklaracji wyboru;
- na podstawie elektronicznego konta pacjenta;
- w przypadku wideoporady – na podstawie okazanego dokumentu tożsamości.

W tym kontekście należy pamiętać, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane. Podmiot udzielający teleporady powinien podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (art. 5 ust. 1 lit. d RODO). Wiąże się to z prawami podmiotów, których dane dotyczą, a więc prawem dostępu do danych osobowych (art. 15 RODO), uprawnieniem do żądania od administratora sprostowania lub uzupełnienia danych (art. 16 RODO), czy też prawem do ograniczenia przetwarzania danych osobowych wówczas, gdy osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych jej dotyczących (art. 18 RODO). Administrator nie powinien przy tym odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, by ułatwić jej wykonanie jej praw (motyw 57 RODO), co jest pewną wskazówką przy podawaniu przez pacjentów danych nadmiarowych. Pamiętać jednak należy, że w świetle zasady minimalizacji danych dane osobowe muszą być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c RODO).

Standard poufności

Drugi standard organizacyjny teleporady obejmuje przeprowadzenie jej w warunkach gwarantujących poufność, w tym zapewnienie braku dostępu osób nieuprawnionych do informacji przekazywanych za pośrednictwem systemów teleinformatycznych lub systemów łączności w związku z udzieleniem teleporady. Świadczenie telemedyczne jest usługą, której właściwość wymaga wykonania jej w sposób uniemożliwiający dostęp osób nieuprawnionych do przekazywanej treści. Obowiązki w zakresie poufności i bezpieczeństwa informacji znajdują pokrycie w konieczności zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z wykonywaniem zawodu medycznego. Świadczeniodawca jest obowiązany zapewnić, aby w udzielaniu świadczenia telemedycznego nie uczestniczyły osoby postronne i aby informacje przekazywane przez pacjenta nie były słyszalne poza pomieszczeniem, w którym przebywa świadczeniodawca, a ponadto powinien on także wdrożyć mechanizmy ochrony przekazywanych danych cyfrowych przed nieuprawnionym dostępem osób trze-

cich. Z uwagi na brak fizycznego kontaktu stron celowe jest również wprowadzenie mechanizmów gwarantujących ich jednoznaczną identyfikację, do czego rekomendowana jest wymiana danych między indywidualnymi kontami [4]. Aktualne na tym tle pozostają wskazówki odnoszące się do aspektów zapewnienia poufności teleporady i weryfikacji tożsamości pacjenta, zawarte w wytycznych Prezydium Naczelnej Rady Lekarskiej w sprawie udzielania świadczeń telemedycznych [6]. Spójne są też wytyczne Kodeksu PZ wskazujące, aby teleporada odbywała się w miejscu, gdzie nie będzie możliwe podsłuchanie rozmowy telefonicznej lub wideorozmowy bądź podejrzenie ekranu przez osoby nieupoważnione. Zdalne udzielanie świadczeń powinno mieć miejsce w oddzielnym, zamykanym pomieszczeniu, do którego nie mają dostępu pacjenci lub inne osoby postronne. Jeżeli teleporada jest nagrywana, pacjent musi być o tym poinformowany przed jej rozpoczęciem, a przekazywanie informacji pocztą elektroniczną ma odbywać się za pośrednictwem skrzynki poczty elektronicznej, do której nie mają dostępu osoby nieupoważnione i której zabezpieczenia zostały uprzednio skonsultowane z informatykiem oraz inspektorem ochrony danych (pkt 12.2. Kodeksu PZ).

Standard poufności wiąże się zatem z koniecznością zapewnienia braku dostępu osób nieuprawnionych do informacji przekazywanych podczas teleporady, co pokrywa się z obowiązkiem zachowania w tajemnicy informacji związanych z pacjentem, uzyskanych w związku z wykonywaniem zawodu medycznego. Teleporada powinna odbyć się przy udziale wyłącznie osób uprawnionych, a więc bez osób postronnych. Przekazywane informacje nie powinny być słyszalne przez osoby trzecie poza pomieszczeniem, w którym przebywa świadczeniodawca, a dodatkowo należy zapewnić funkcjonowanie mechanizmów ochrony przekazywanych treści przed nieuprawnionym dostępem.

Standard bezpiecznych rozwiązań techniczno-organizacyjnych

Trzeci standard dotyczy przypadku przekazywania informacji dotyczącej stanu zdrowia pacjenta, w tym cyfrowego odwzorowania dokumentacji medycznej, za pośrednictwem systemów teleinformatycznych. Standard obejmuje stosowanie przez świadczeniodawcę POZ rozwiązań techniczno-organizacyjnych służących zapewnieniu transmisji dokumentów elektronicznych w postaci graficznej i tekstowej w sposób zapewniający ich integralność oraz ochronę przed nieuprawnionym wykorzystaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem. Świadczeniodawca POZ ma zatem zabezpieczyć pacjenta przed naruszeniem ochrony jego danych osobowych. Takim naruszeniem jest bowiem naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 4 pkt 12 RODO). Aby zrealizować ten standard, należy jednak uczynić zadość wszystkim obowiązkom świadczeniodawcy POZ jako administratora danych, niewyrażonym w rozporządzeniu. Równocześnie bowiem standard integralności i poufności danych osobowych wynika z RODO i zasady, wedle której dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO), z czym wiążą się liczne szczegółowe obowiązki administratora danych.

Pozostałe wymogi RODO

Analizując przepisy rozporządzenia, należy zauważyć, że skupiają się one na obowiązkach realizowanych w bezpośrednim związku z jednostkową teleporadą. To w jej trakcie trzeba zachować zasady poufności, tuż przed jej udzieleniem należy zidentyfikować pacjenta, jedynie kwestie zabezpieczeń technicznych dotyczą przekazywania informacji dotyczącej stanu zdrowia pacjenta, co może mieć miejsce zarówno przed teleporadą, jak i w jej trakcie oraz po niej. Chociaż granice czasowe teleporady nie zostały wyznaczone w rozporządzeniu, przez co nie można jednoznacznie przesądzić, kiedy dokładnie się ona zaczyna i z jakich elementów się składa, to w kontekście ochrony danych osobowych należy zwrócić uwagę, że standardy organizacyjne dotyczą czynności związanych z samym świadczeniem zdrowotnym, nie akcentując kwestii systemowych. Tymczasem, jak wskazuje orzecznictwo, na gruncie RODO prawodawca odszedł od statycznego określenia wymaganych od administratora środków technicznych i organizacyjnych na rzecz dynamicznej oceny przyjętych środków bezpieczeństwa. Oznacza to, że to na administratorze i podmiocie przetwarzającym dane spoczywa obowiązek przyjęcia odpowiednich (adekwatnych) środków bezpieczeństwa. Stosownie do treści art. 32 ust. 1 RODO ww. podmioty powinny ustalić odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko związane z przetwarzaniem, wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

W konsekwencji obowiązujące przepisy prawa nie określają katalogu odpowiednich środków bezpieczeństwa, zaś to na administratorze spoczywa obowiązek dokonania oceny w tym zakresie i wyboru środków adekwatnych m.in. do obecnego stanu wiedzy technicznej czy skali ryzyka naruszenia praw (wyrok NSA z 9 lutego 2023 r., III OSK 3945/21, CBOSA). W świetle RODO to do obowiązków świadczeniodawcy POZ jako administratora danych należy konieczność przeprowadzenia oceny ryzyka, zanim nastąpi przetwarzanie danych z wykorzystaniem odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z RODO i rozliczalność przetwarzania danych osobowych. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych (motyw 74 RODO), przy czym RODO nie wskazuje

konkretnych rozwiązań zapewniających odpowiednią ochronę danych osobowych. W zakresie stosowania tych środków także wytyczne Kodeksu PZ są bardzo ogólne. Wskazuje się jedynie, że w celu zapewnienia, by przekazywanie informacji w ramach teleporad odbywało się w sposób zapewniający ich integralność oraz ochronę przed nieuprawnionym wykorzystaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem, powinno się wykorzystywać rozwiązania techniczno-organizacyjne uprzednio konsultowane z informatykiem lub firmą IT pod względem zabezpieczeń technicznych, a także z inspektorem ochrony danych (dalej: IOD), w zakresie spełnienia wymagań związanych z ochroną danych osobowych i bezpieczeństwem informacji (pkt 12.3. Kodeksu PZ).

Dalsze obowiązki, nieujęte w rozporządzeniu, a dotyczące zapewnienia bezpieczeństwa przetwarzania danych, to konieczność prowadzenia rejestru czynności przetwarzania (art. 30 ust. 1 i 4 RODO), zgłaszania i dokumentowania naruszeń (art. 33 ust. 1, 2 i 5 RODO) oraz zawiadamiania podmiotu danych o naruszeniach (art. 34 ust. 1 RODO). Po stronie administratora leży też realizacja obowiązków informacyjnych (art. 13 i 14 RODO) oraz wykonywanie praw podmiotów danych (art. 15–22 RODO). Przygotowanie się administratora do realizacji tych obowiązków w zakresie udzielania teleporad wymaga wdrożenia systemu ochrony danych osobowych i odpowiedniej organizacji pracy na etapie poprzedzającym samo udzielanie teleporad.

Podmiot wykonujący taką działalność jako administrator ma także obowiązki spełnienia wymogów właściwego doboru podmiotu przetwarzającego (art. 28 ust. 1 i 5 oraz art. 32 ust. 1 i 2 RODO). Tworząc dokumentację medyczną, musi kierować się zasadami wskazanymi w RODO, choć w praktyce, w obliczu ogromnej ilości danych, prowadzeniem dokumentacji medycznej zajmują się nierzadko wyspecjalizowane firmy. W rozporządzeniu brakuje jednak w tym zakresie określenia wytycznych. W momencie zawierania umowy o świadczenie usług z taką firmą jednostka medyczna powinna zawrzeć umowę powierzenia przetwarzania danych osobowych, spełniającą wymagania z art. 28 RODO. Administrator zobowiązany jest przy tym do korzystania z usług podmiotu dającego gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą. Umowa powierzenia przetwarzania danych powinna zatem, zgodnie z RODO, obejmować między innymi przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych, kategorie osób, których dane dotyczą, obowiązki i prawa administratora oraz obowiązki zachowania w tajemnicy przez osoby upoważnione do przetwarzania danych [9]. W niektórych przypadkach administrator będzie miał obowiązek wyznaczenia IOD. Powołanie IOD jest obowiązkowe, gdy główna działalność administratora polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, w tym danych o stanie zdrowia. IOD będzie miał zadanie m.in. informować administratora, podmiot przetwarzający oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO, monitorowania przestrzegania RODO i współpracy z organem nadzorczym. Zadania IOD w RODO zostały sformułowane w sposób ogólny, bez wskazania trybu oraz terminów ich realizacji. IOD pełnić będzie funkcję doradczą i weryfikacyjną wobec działań administratora danych [10], także w zakresie świadczenia teleporad medycznych.

Wnioski

W założeniu ustawodawcy standardy organizacyjne mają określać wzajemne zależności oraz zakres i podział zadań (uprawnień i odpowiedzialności) związanych z udzielaniem świadczeń zdrowotnych. Może to oznaczać w szczególności kwalifikacje personelu medycznego uczestniczącego w wykonywaniu świadczeń zdrowotnych, kolejność wykonywania czynności medycznych w procesie diagnostyczno-terapeutycznym i relacje kompetencyjne występujące między personelem, jak również zakres jego odpowiedzialności [11]. W tym świetle standard organizacyjny teleporad, który w zakresie ochrony danych osobowych odnosi się wyłącznie do identyfikacji pacjenta oraz konieczności zapewnienia poufności i bezpieczeństwa rozwiązań techniczno-organizacyjnych, w istocie jedynie powiela w ograniczonym zakresie ogólne wymogi stawiane wszystkim administratorom danych osobowych. Nie wskazuje też na tych wąsko uregulowanych obszarach konkretnych rozwiązań praktycznych. Można stwierdzić, że standard organizacyjny teleporad w obszarze ochrony danych osobowych nie tylko nie uwzględnia zależności ani nie określa zadań, obowiązków i zakresu odpowiedzialności osób udzielających teleporad oraz świadczeniodawców POZ, ale również nie stanowi dla nich konkretnych i praktycznych wskazówek organizacyjnych. W tym zakresie większe znaczenie przypisać można Kodeksowi PZ czy wytycznym Naczelnej Rady Lekarskiej. Dlatego określony rozporządzeniem obligatoryjny standard organizacyjny dla teleporad zbyt nisko ustanowił wymogi minimalne. Nie są one wystarczające, aby uczynić zadość wszystkim obowiązkom administratora danych osobowych wynikającym z RODO. Przez to teleporady powinny być organizowane z założenia wedle wymogów ponadstandardowych względem tych, które przewidział prawodawca. Wymogi takie muszą uwzględnić wdrożenie procedur prowadzenia rozmów i udostępniania na odległość wrażliwych danych o stanie zdrowia pacjenta, zapewniających adekwatny stopień bezpieczeństwa oraz poufności. Uwzględnić w nich trzeba instrukcje korzystania ze sprzętu IT, wsparcie techniczne i zasady postępowania w przypadkach naruszenia ochrony danych osobowych, w tym informowanie IOD. Konieczne jest wdrożenie procedur na potrzeby realizacji indywidualnych praw podmiotów danych, w tym reguł informowania o tych prawach, zwłaszcza wobec szczególnych podstaw przetwarzania danych na potrzeby opieki zdrowotnej. W przyjmowanych procedurach należy uwzględnić sytuacje nagłe i wyjątkowe, jak zagrożenie życia i konieczność udzielenia natychmiastowej pomocy bądź brak współpracy lub inne nieprawidłowości w korzystaniu ze świadczenia.

W każdym przypadku przetwarzanie danych powinno odbywać się w zakresie niezbędnym. Dlatego mając na względzie zasadę minimalizacji danych, rozmowy z osobami dzwoniącymi powinny być nagrywane tylko wyjątkowo, z uwzględnieniem celu i analizy ryzyka.

W placówce powinna obowiązywać polityka bezpieczeństwa wraz z mechanizmami gwarantującymi jej przestrzeganie. Należy wprowadzić rejestry wymagane przez RODO, a także rejestr upoważnień dla osób działających w imieniu administratora i mających dostęp do danych osobowych, zapewniając przy tym przejrzyste sformułowanie poleceń przetwarzania danych dla pracowników (regulaminowych lub związanych z zakresem ich obowiązków), tak aby uczynić zadość wymogom art. 29 RODO.

Podejmując działania na rzecz ochrony danych osobowych podczas teleporad, warto sięgać do zatwierdzonych przez PUODO kodeksów postępowania. Obecnie, pomimo że RODO obowiązuje od ponad 5 lat, zatwierdzone zostały dwa takie krajowe kodeksy: Kodeks PZ oraz Kodeks postępowania dla sektora ochrony zdrowia, złożony przez Polską Federację Szpitali. Stosując obowiązujące standardy, wytyczne i zalecenia, należy jednak przede wszystkim przyjąć perspektywę systemową, aby stosowane środki ochrony danych osobowych były adekwatne do specyfiki teleporad medycznych i uwzględniały typowe ryzyka z nimi związane.

Piśmiennictwo

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. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z 4 listopada 2008 r. w sprawie korzyści telemedycyny dla pacjentów, systemów opieki zdrowotnej i społeczeństwa. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52008DC0689 (access: 31.05.2023)
6. Uchwała nr 89/20/P-VIII Prezydium Naczelnej Rady Lekarskiej z 24 lipca 2020 r. w sprawie przyjęcia wytycznych dla udzielania świadczeń telemedycznych. https://nil.org.pl/aktualnosci/4980-wytyczne-dla-udzielania-swiadczen-telemedycznych?previewmode=4ffbd5c8221d7c147f8363ccdc9a2a37 (access: 31.05.2023)
7. Kodeks postępowania dotyczącego ochrony danych osobowych przetwarzanych w małych placówkach medycznych (Porozumienie Zielonogórskie) z 9 listopada 2022 r., https://uodo.gov.pl/pl/426/1110 (access: 31.05.2023)
8. Wytyczne dotyczące realizacji prawa do informacji przez osoby uprawnione na odległość, Rzecznik Praw Pacjenta, Prezes Urzędu Ochrony Danych Osobowych, 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. Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia? Warszawa, Fundacja Telemedyczna Grupa Robocza, 2018: s. 86. http://telemedycyna-raport.pl/#raport (access: 31.05.2023)
11. Uzasadnienie do projektu ustawy o zmianie ustawy o działalności leczniczej oraz niektórych innych ustaw. Druk Sejmowy nr 562, Sejm VIII Kadencji. https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=562 (access: 31.05.2023)