Warszawa, dnia 13 listopada 2018 r.

Polska Federacja Szpitali

ul. Nowogrodzka 11

00-513 Warszawa

Organizacja pracodawców wpisana

pod numerem 402294

Krajowego Rejestru Sądowego

przez Sąd Rejonowy dla m.st. Warszawy,

XII Wydział Gospodarczy

Szanowna Pani

dr Edyta Bielak–Jomaa

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

Wniosek o zatwierdzenie kodeksu postępowania

Działając na podstawie udzielonego mi pełnomocnictwa (załącznik do wniosku), na podstawie art. 40 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(dalej: „RODO"), w związku z art. 27 ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (Dz.U.2018.1000 z dnia 2018.05.24) (dalej: „ustawa o ochronie danych osobowych"), w imieniu Polskiej Federacji Szpitali występującej jako wnioskodawca, o którym mowa w art. 27 ust. 5 ustawy o ochronie danych osobowych, niniejszym wnoszę o zatwierdzenie kodeksu postępowania pt. „Kodeks postępowania dla sektora ochrony zdrowia wydany zgodnie z art. 40 RODO dotyczący podmiotów wykonujących działalność leczniczą i podmiotów przetwarzających" (dalej: „Kodeks") stanowiący załącznik nr 1 do niniejszego wniosku.

Polska Federacja Szpitali należy do podmiotów, które są uprawnione zgodnie z art. 40 ust. 2 RODO do opracowania kodeksów postępowania. Zakres przedmiotowy Kodeksu jest zgodny wymogami określonymi w art. 40 RODO, a prace nad Kodeksem zostały poddane konsultacjom publicznym zgodnie z motywem 99 RODO oraz z art. 27 ust 2 ustawy o ochronie danych osobowych, a efekty przeprowadzonych konsultacji zostały przedstawione w załączniku 2, 3, 4 do wniosku, czyniąc tym samym zadość wymogom określonym w art. 27 ust. 3 ustawy o ochronie danych osobowych.

W związku z powyższym wnoszę jak na wstępie.

Ligia Kornowska,

dyrektor zarządzająca

Polskiej Federacji Szpitali

Spis załączników:

1. Projekt Kodeksu postępowania
2. Raport z przeprowadzonych konsultacji publicznych
3. Wyrazy poparcia i oświadczenia pozostałych członków Komitetu sterującego.
4. Wyrazy poparcia, pozostałe.
5. Pełnomocnictwo
6. Dowód wpłaty

Wersja: 22 przygotowana w celu przedłożenia do Prezesa Urzędu Ochrony Danych Osobowych (załącznik nr 1 do wniosku).

Data przygotowania: 13.11.2018

KODEKS POSTĘPOWANIA DLA SEKTORA OCHRONY ZDROWIA WYDANY ZGODNIE Z ART. 40 RODO DOTYCZĄCY PODMIOTÓW WYKONUJĄCYCH DZIAŁALNOŚĆ LECZNICZĄ I PODMIOTÓW PRZETWARZAJĄCYCH

Warszawa, dnia 13.11.2018

SPIS TREŚCI

1. WSTĘP

1.1. Celem Kodeksu jest zapewnienie adekwatnego poziomu ochrony Pacjentów, w związku z przetwarzaniem ich danych osobowych z uwzględnieniem ochrony zdrowia i życia Pacjentów będących dobrami nadrzędnymi. .

1.2. Kodeks postępowania został sporządzony z uwzględnieniem specyfiki funkcjonowania rynku podmiotów wykonujących działalność leczniczą.

1.3. Stosowanie Kodeksu postępowania stanowi okoliczność potwierdzającą wywiązywanie się z obowiązków nałożonych przez Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO) na administratorów danych oraz Podmioty przetwarzające, które działają na rynku podmiotów wykonujących działalność leczniczą. Kodeks służy tym samym realizacji zasady rozliczalności.

1.4. Kodeks postępowania zawiera zbiór zasad zgodnych z RODO i ustawodawstwem krajowym, w zakresie podnoszenia poziomu ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, obejmujących w szczególności:

1.4.1. realizację ogólnych zasad przetwarzania danych osobowych wskazanych w art. 5 RODO;

1.4.2. pseudonimizację danych osobowych;

1.4.3. informowanie opinii publicznej i osób, których dane dotyczą;

1.4.4. wykonywanie przez osoby, których dane dotyczą przysługujących im praw;

1.4.5. środki i procedury regulujące obowiązki Administratora oraz ochronę danych w fazie projektowania i domyślną ochronę danych;

1.4.6. środki i procedury zapewniające bezpieczeństwo przetwarzania;

1.4.7. zgłaszanie organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamianie o takich naruszeniach osoby, których dane dotyczą.

1.5. Mając na uwadze specyfikę działalności poszczególnych Podmiotów wykonujących działalność leczniczą oraz różnice w zakresie uwarunkowań, skali działalności i profili ryzyka, szczegółowe działania w zakresie ochrony danych osobowych mogą być realizowane odmiennie przy zachowaniu podstawowych wymagań opisanych w niniejszym Kodeksie postępowania oraz zgodnych z wymaganiami RODO.

1.6. Podmiotami tworzącymi kodeks w rozumieniu art. 40 RODO są: Polska Federacja Szpitali, Fundacja Telemedyczna Grupa Robocza, Pracodawcy Medycyny Prywatnej, Konfederacja Lewiatan, Polska Izba Informatyki i Telekomunikacji, Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie oraz inne podmioty tworzące Komitet sterujący. Podmioty te podejmują solidarne działania na rzecz opracowania, zmiany lub rozszerzenia zakresu Kodeksu oraz deklarują chęć wystąpienia o jego zatwierdzenie do Prezesa Urzędu Ochrony Danych Osobowych.

1.7. Kodeks postępowania powstawał przy aktywnym udziale m.in.:

1.7.1. strony publicznej - Centrum Systemów Informacyjnych Ochrony Zdrowia, Ministerstwo Zdrowia, Centrum Monitorowania Jakości w Ochronie Zdrowia;

1.7.2. podmiotów wspierających - Województwo Wielkopolskie, Naczelna Izba Lekarska, Naczelna Izba Pielęgniarek i Położnych, Fundacja My Pacjenci, Fundacja Urszuli Jaworskiej, Naczelna Izba Aptekarska, Krajowa Izba Diagnostów Laboratoryjnych, Krajowa Izba Fizjoterapeutów, Gdański Uniwersytet Medyczny, Kancelaria Domański Zakrzewski Palinka oraz wielu innych osób fizycznych, prawnych i jednostek organizacyjnych uczestniczących w pracach nad Kodeksem w ramach szeroko zakrojonych konsultacji.

1.8. Mając na uwadze znaczenie Kodeksu postępowania dla ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w działalności polskiego rynku podmiotów wykonujących działalność leczniczą, podmioty opracowujące Kodeks deklarują współpracę na rzecz:

1.8.1. podnoszenia poziomu ochrony danych osobowych w działalności polskiego rynku podmiotów wykonujących działalność leczniczą,

1.8.2. upowszechniania i jednolitego wdrażania zasad prawnej ochrony danych osobowych,

1.8.3. właściwego reagowania na zmiany w otoczeniu prawnym i instytucjonalnym, a także na oczekiwania i potrzeby Pacjentów, PWDL oraz innych podmiotów zaangażowanych w opracowanie i realizację postanowień Kodeksu – poprzez dokonywanie stosownych zmian lub rozszerzeń zakresu Kodeksu w celu doprecyzowania postanowień RODO.

1.9. Podmioty opracowujące Kodeks pragną także wyrazić nadzieję, że Kodeks postępowania przyczyni się do skutecznego rozwoju e-zdrowia w Polsce, z zachowaniem właściwych i aktualnych standardów bezpieczeństwa i poufności przetwarzania danych o stanie zdrowia Pacjentów.

1.10. PWDL oraz Podmioty przetwarzające, które podejmują się stosowania Kodeksu, zobowiązują się do realizowania niezbędnych działań mających na celu zapewnienie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

1.11. PWDL oraz Podmioty przetwarzające, które podejmują się stosowania Kodeksu, przykładają szczególną wagę do zapewnienia bezpieczeństwa przetwarzanych danych osobowych. W podmiotach tych ochronie podlegają w szczególności:

1.11.1. dane przetwarzane w celach zdrowotnych, których przetwarzanie nie wymaga zgody Pacjenta,

1.11.2. dane przetwarzane w celach innych niż zdrowotne, których przetwarzanie nie wymaga zgody Pacjenta,

1.11.3. dane przetwarzane na podstawie zgody Pacjenta w celach marketingowych, w związku z realizacją Badań klinicznych lub innych Badań naukowych, w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, przekazywaniem danych osobowych do państwa trzeciego gdy realizowane jest na podstawie zgody, lub innych celach wymagających zgody Pacjenta.

1.12. Podmioty, realizując postanowienia Kodeksu, uwzględniają ryzyko naruszenia praw lub wolności osób fizycznych i wdrażają odpowiednie środki techniczne i organizacyjne zapewniające stopień bezpieczeństwa odpowiadający temu ryzyku, między innymi poprzez:

1.12.1. zapewnienie ochrony danych osobowych w oparciu o obowiązujące przepisy prawa i postanowienia Kodeksu,

1.12.2. określenie zasad dostępu, przetwarzania i udostępniania danych osobowych,

1.12.3. minimalizowanie ryzyka w obszarze bezpieczeństwa fizycznego, teleinformatycznego, organizacyjno-prawnego oraz osobowego,

1.12.4. zaangażowanie wszystkich pracowników w ochronę danych osobowych oraz stałe podnoszenie umiejętności i kwalifikacji kadr w tej dziedzinie.

2. DEFINICJE I SKRÓTY

Administrator - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Badanie kliniczne - każde badanie prowadzone z udziałem ludzi w celu odkrycia lub potwierdzenia klinicznych, farmakologicznych, w tym farmakodynamicznych skutków działania jednego lub wielu badanych produktów leczniczych, lub w celu zidentyfikowania działań niepożądanych jednego lub większej liczby badanych produktów leczniczych, lub śledzenia wchłaniania, dystrybucji, metabolizmu i wydalania jednego lub większej liczby badanych produktów leczniczych, mając na względzie ich bezpieczeństwo i skuteczność, a także zaprojektowane i zaplanowane systematyczne badanie prowadzone na ludziach, podjęte w celu weryfikacji bezpieczeństwa lub działania określonego wyrobu medycznego, wyposażenia wyrobu medycznego albo aktywnego wyrobu medycznego do implantacji;

Badanie naukowe – badanie naukowe, którym mowa w recitalu 159 RODO, pojęcie to obejmuje również Eksperyment medyczny, w tym Badanie kliniczne;

Dokumentacja medyczna – dokumentacja medyczna, o której mowa w przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określona w przepisach odrębnych;

Eksperyment medyczny – eksperyment medyczny w rozumieniu ustawy o zawodach lekarza i lekarza dentysty, obejmujący eksperyment leczniczy i badawczy. Pojęcie to obejmuje również Badania kliniczne;

Kodeks – niniejszy dokument;

Opiekun faktyczny – opiekun faktyczny w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta;

Osoba bliska - małżonek, krewny lub powinowaty do drugiego stopnia w linii prostej, Przedstawiciel ustawowy, osoba pozostająca we wspólnym pożyciu lub osoba wskazana przez pacjenta[1];

Osoba wykonująca zawód medyczny[2] - osoba uprawniona na podstawie odrębnych przepisów do udzielania świadczeń zdrowotnych oraz osoba legitymująca się nabyciem fachowych kwalifikacji do udzielania świadczeń zdrowotnych w określonym zakresie lub w określonej dziedzinie medycyny, w tym m.in. lekarz, lekarz dentysta, pielęgniarka, położna, ratownik medyczny, diagnosta laboratoryjny, fizjoterapeuta, technik analityki medycznej i inne osoby wskazane w art. 6a ustawy o diagnostyce laboratoryjnej, farmaceuta, technik farmacji, psycholog, psychoterapeuta, fizjoterapeuta, logopeda, felczer, optometrysta, dietetyk, a także osoby wykonujące inne zawody wskazane w tabeli nr 1 załącznika nr 3 do rozporządzenia Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych;

Pacjent - osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub Osobę wykonującą zawód medyczny[3];

Podmiot monitorujący – podmiot odpowiedzialny za monitorowanie przestrzegania Kodeksu i akredytowany przez Prezesa Urzędu Ochrony Danych Osobowych, spełniający wymogi wskazane w art. 41 ust. 1 i 2 RODO;

Podmiot przestrzegający Kodeksu - PWDL lub Podmiot przetwarzający, który podjął się dobrowolnie przestrzegania postanowień Kodeksu poprzez złożenie oświadczenia o którym mowa w pkt. 7.3.1. Kodeksu lub wniosku, o którym mowa w pkt. 7.4.1., które zostały pozytywnie rozpatrzone zgodnie z procedurą wskazaną w Kodeksie.

Podmiot wykonujący działalność leczniczą (PWDL) – podmiot leczniczy oraz lekarz, pielęgniarka lub położna, fizjoterapeuta wykonujący zawód w ramach działalności leczniczej

---

[1]Definicja zgodna z definicją wskazaną w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta.
[2]W przypadku, gdy w Kodeksie mowa o pielęgniarce i lekarzu, rozumie się przez to również odpowiednio położną i lekarza dentystę.
[3]Pojęcie Pacjenta nie jest ograniczone jedynie do osób, które aktualnie ubiegają się o świadczenia bądź uzyskują świadczenia, lecz także do osób które uzyskiwały świadczenia zdrowotne w przeszłości. Można przyjąć zasadę, że „raz pacjent-zawsze pacjent".

jako praktykę zawodową[4], o których mowa w przepisach ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej;

Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora[5];

Profilaktyka zdrowotna - wszelkie działania mające na celu zapobieganie niekorzystnym zjawiskom w obszarze zdrowia Pacjenta;

Przedstawiciel ustawowy – osoba umocowana do działania w cudzym imieniu na podstawie ustawy zgodnie z art. 96 k.c.;

Świadczenie zdrowotne - działania służące zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działania medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich wykonywania;

Unikalny Pacjent – Pacjent którego tożsamość ustalana jest na podstawie unikalnego identyfikatora, zwłaszcza PESEL;

UODO – Urząd Ochrony Danych Osobowych;

RODO - Rozporządzenie 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).

Jeżeli w treści dokumentu nie wskazano inaczej, terminom pisanym wielką literą, które nie zostały należy zdefiniowane powyżej przypisać znaczenie nadane im w przepisach RODO.

[4]W odniesieniu do fizoterapeuty zapisy kodeksu uwzględniają projektowaną nowelizację u.d.l. https://legislacja.rcl.gov.pl/projekt/12312254/katalog/12513340#12513340.
[5]Definicja wynikająca wprost z RODO.

3. Zakres Kodeksu

3.1. Kryterium podmiotowe stosowania Kodeksu

3.1.1. Biorąc pod uwagę motywy powstania niniejszego Kodeksu, które opisane zostały w punkcie 1 dokumentu, Kodeks może regulować zasady przetwarzania danych osobowych przez wszystkie PWDL, bez względu na[6]:

3.1.1.1. formę prawną prowadzenia działalności;

3.1.1.2. strukturę właścicielską i podmiot tworzący;

3.1.1.3. uczestnictwo w systemie opieki zdrowotnej finansowanym ze środków publicznych;

3.1.1.4. zakres i rodzaj prowadzonej działalności leczniczej.

3.1.2. Z zastrzeżeniem pkt. 3.1.3. postanowienia Kodeksu mają również zastosowanie do Podmiotów przetwarzających, które przetwarzają na zlecenie PWDL dane osobowe pozyskane przez PWDL w celu prowadzenia działalności leczniczej.

3.1.3. Stosowanie postanowień Kodeksu w odniesieniu do Podmiotów przetwarzających ze względu na specyfikę ich działalności ogranicza się przede wszystkim do wymogów wskazanych w rozdziale 5 Kodeksu i oceniane jest w oparciu o zakres wskazany w załączniku nr 10 do Kodeksu.

3.1.4. Z zastrzeżeniem pkt. 3.1.2. Kodeks nie reguluje zasad przetwarzania danych przez. podmioty niebędące PWDL np. podmioty z branży lifestyle/fitness/ dietetycznej itp., nawet jeżeli podmioty te przetwarzają dane o stanie zdrowia.

3.2. Kryterium przedmiotowe stosowania Kodeksu

3.2.1. Kodeks zbudowany jest wokół poszczególnych procesów związanych z przetwarzaniem danych osobowych Pacjentów, do których dochodzi w Podmiotach wykonujących działalność leczniczą oraz wyznacza minimalne wymogi z nimi związane. Kodeks reguluje następujące procesy przetwarzania danych osobowych Pacjentów:

3.2.1.1. przetwarzanie danych w związku z prowadzoną działalnością leczniczą (zazwyczaj na podstawie RODO w związku z przepisem ustawy, bez konieczności uzyskania osobnej zgody na przetwarzanie);

3.2.1.2. przetwarzanie danych w innych celach (zazwyczaj na podstawie zgody Pacjenta).

---

[6]Z zastrzeżeniem, że monitorowanie przestrzegania Kodeksu zgodnie z art. 41 RODO nie będzie dotyczyć organów i podmiotów publicznych (art. 41 ust. 6 RODO). Stosowanie Kodeksu jest dobrowolne.

3.2.2. Kodeks nie reguluje czynności przetwarzania prowadzonych w kilku państwach członkowskich w rozumieniu art. 40 ust. 7 RODO. PWDL lub Podmiot przetwarzający zaangażowane w czynności przetwarzania w kilku państwach członkowskich w dalszym ciągu będą mogły uzyskać status Podmiotów przestrzegających Kodeksu, który dotyczyć będzie czynności przetwarzania, w zakresie w jakim nie są one realizowane w kilku państwach członkowskich[7][8].

3.2.3. Z zastrzeżeniem pkt. 3.2.2. rekomenduje się jako dobrą praktykę stosowanie postanowień Kodeksu również do czynności przetwarzania prowadzonych w kilku państwach członkowskich.

3.2.4. Kodeks nie reguluje przetwarzania danych o osobach zmarłych.

4. Podstawowe zasady przetwarzania danych osobowych przez PWDL

4.1. Podstawy przetwarzania danych

4.1.1. Podstawą prawną przetwarzania danych osobowych Pacjentów w celach zdrowotnych przez Podmioty wykonujące działalność leczniczą są bezpośrednio właściwe przepisy RODO pozostające w związku z przepisami krajowego prawa medycznego[9]. W przypadku realizacji praw wskazanych w art. 13, 14 oraz 15 RODO, Administrator w odniesieniu do podstawy prawnej przetwarzania podaje co najmniej przepis RODO i nazwę aktu prawnego [10], określonego
w szczególności w pkt. 4.1.4 i 4.1.5.

4.1.2. W szczególności PWDL mogą przetwarzać dane osobowe Pacjentów, w tym dotyczące zdrowia na podstawie:

4.1.2.1. art. 9 ust. 2 lit h) RODO, który wymienia cele zdrowotne przetwarzania[11] oraz

---

[7] Komitet Sterujący będzie podejmował dalsze działania zmierzające do rozszerzenia zakresu stosowania Kodeksu do operacji przetwarzania danych w kilku państwach członkowskich.

[8] Zakresem przedmiotowym Kodeksu może być objęta czynność przetwarzania w zakresie w jakim nie odnosi się do przetwarzania w kilku państwach członkowskich, np. udostępnianie danych z serwerów chmurowych położonych kilku państwach członkowskich w dalszym ciągu może być ocenione za zgodność z Kodeksem w szczególności pod kątem takich kwestii jak pkt. 4.8. Kodeksu.

[9] Co do zasady PWDL w związku z prowadzeniem działalności leczniczej nie będą musiały uzyskiwać zgody Pacjenta na przetwarzanie danych osobowych.

[10] Podawanie konkretnego przepisu prawa polskiego nie zawsze jest możliwe i nie zawsze dostarcza adekwatnych informacji na temat przetwarzania osobie której dane dotyczą.

[11] Pojęcie „cele zdrowotne" zostało użyte w pkt. 52 preambuły „cele zdrowotne", w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej, w szczególności zapewnianiem jakości i ekonomiczności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych. Przetwarzanie danych na podstawie art. 9 ust. 2 lit h RODO może się odbywać 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. Terminy te nie mają definicji w krajowym porządku prawnym. Jak

4.1.2.2. przepisów polskich ustaw z obszaru prawa medycznego, pozostających w związku z celami zdrowotnymi przetwarzania, mogących przy tym zawierać dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych dotyczących zdrowia.

4.1.3. Dane osobowe Pacjenta mogą być także przetwarzane na podstawie zgody, o której mowa w art. 9 ust. 2 lit a) RODO, a także na podstawie przesłanek wskazanych w pkt 4.3.1. Kodeksu.

4.1.4. Przetwarzanie danych osobowych Pacjenta w celach zdrowotnych na podstawie art. 9 ust. 2 lit h) RODO odbywa się co do zasady w związku z wykonywaniem działalności leczniczej zgodnie z ustawą o działalności leczniczej przy zachowaniu obowiązków wynikających z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.1.5. W sytuacji, gdy udzielenie Świadczenia zdrowotnego ze względu na swą specyfikę regulowane jest szczegółowo przepisami innych aktów prawnych, zastosowanie znajdą również odpowiednio właściwe przepisy szczegółowe, zawarte m.in. w:

4.1.5.1. ustawie z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (t.j. Dz.U. z 2018 r. poz. 1878);

4.1.5.2. ustawie z dnia 27 czerwca 1997 r. o służbie medycyny pracy (t.j. Dz.U. z 2018 r. poz. 1155);

4.1.5.3. ustawie z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (t.j. Dz.U. z 2017 r. poz. 2195);

4.1.5.4. ustawie z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz.U. z 2017 r. poz. 2217);

4.1.5.5. ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2018 r. poz. 1510);

4.1.5.6. ustawie z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (t.j. Dz.U. z 2017 r. poz. 1371);

---

wskazuje się w komentarzach do RODO „wydaje się, że pojęcie działalności leczniczej lub nawet pojęcie Świadczenia zdrowotnego (...) będzie obejmować zakresem pojęciowym terminy: Profilaktyka zdrowotna, leczenie, diagnoza medyczna i zapewnienie opieki zdrowotnej, zawarte w komentowanym przepisie" (*P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018). Co najmniej więc pomocniczo w zakresie interpretacji komentowanego przepisu można odwołać się do przepisów prawa krajowego. Przetwarzane danych osobowych w celu udzielania świadczeń i zarządzania udzielaniem świadczeń z zakresu medycyny estetycznej będzie również przetwarzaniem w celach zdrowotnych, jednak nie zawsze osoby korzystające z tego rodzaju świadczeń będą Pacjentami.

4.1.5.7. ustawie z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (t.j. Dz.U. z 2017 r. poz. 1000);

4.1.5.8. ustawie z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (t.j. Dz.U. z 2018 r. poz. 151);

4.1.5.9. ustawie z dnia 25 czerwca 2015 r. o leczeniu niepłodności (t.j. Dz.U. z 2017 r. poz. 865);

4.1.5.10. ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (t.j. Dz.U. z 2017 r. poz. 1845).

4.1.6. W przypadku udzielania świadczeń w ramach transgranicznej opieki zdrowotnej, podstawę prawną będą stanowiły także przepisy dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej

4.2. Przetwarzanie danych w celach zdrowotnych (niewymagające zgody Pacjenta)

4.2.1. Przepisy RODO określają katalog celów uzasadniających przetwarzanie danych przez PWDL bez konieczności uzyskania zgody Pacjenta, co uzasadnione jest ochroną innych praw podstawowych Pacjenta.

4.2.2. Nie jest wymagana zgoda Pacjenta, jeżeli przetwarzanie jego danych osobowych jest niezbędne do realizacji celów zdrowotnych przetwarzania, czyli:

4.2.2.1. Profilaktyki zdrowotnej,

4.2.2.1.1. Cel ten obejmuje m.in. przetwarzanie związane z procesem informowania Pacjenta o możliwości udzielenia świadczenia, w tym przesyłanie zaproszeń na badania przesiewowe, zaproszeń na wykonanie szczepień, przekazywanie materiałów edukacyjnych, przekazywanie informacji o wydarzeniach prozdrowotnych, udzielanie porad patronażowych, wykonywanie wizyt patronażowych, badań bilansowych i testów przesiewowych oraz uczestnictwo w profilaktycznych programach zdrowotnych;

4.2.2.1.2. Przetwarzanie danych osobowych Pacjenta do celów Profilaktyki zdrowotnej jest niezbędne wtedy, jeżeli jest uzasadnione stanem zdrowia Pacjenta lub czynnikami ryzyka lub rokowaniami co do niego zawartymi w Dokumentacji medycznej, którą dysponuje PWDL lub też jeżeli wynika ono z przepisów prawa dotyczących Profilaktyki zdrowotnej[12];

[12] Dotyczy to m.in. przepisów obejmujących szczepienia ochronne, czy też przepisów regulujących zasady prowadzenia profilaktyki chorób w ramach POZ, lub realizacji Narodowych Programów do Walki z Chorobami Nowotworowymi

4.2.2.1.3. Przetwarzanie danych w celu Profilaktyki zdrowotnej odbywa się zwykle na podstawie art. 9 ust. 2 lit h) RODO w związku z art. 3 ust. 2 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.2.2.2. **medycyny pracy, w tym oceny zdolności pracownika do pracy,**

4.2.2.2.1. Cel ten obejmuje w szczególności przetwarzanie związane z procesem realizacji zadań służby medycyny pracy, w tym badania wstępne, okresowe i kontrolne pracowników oraz inne świadczenia zdrowotne wykonywane na podstawie pisemnej umowy zawartej przez pracodawcę z podstawową jednostką służby medycyny pracy;

4.2.2.2.2. Przetwarzanie danych w tym celu odbywa się zwykle na podstawie art. 9 ust. 2 lit h) RODO w związku z art. 6 i 11 ustawy o służbie medycyny pracy.

4.2.2.3. **diagnozy medycznej i leczenia,**

4.2.2.3.1. Cel ten obejmuje w szczególności przetwarzanie związane procesem udzielania świadczeń zdrowotnych (diagnostycznych i leczniczych), w tym prowadzenie Dokumentacji medycznej;

4.2.2.3.2. Przetwarzanie danych w tym celu odbywa się zwykle na podstawie art. 9 ust. 2 lit h) RODO w związku z art. 3 ust. 1 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.2.2.4. **zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej,**

4.2.2.4.1. Cel ten obejmuje w szczególności przetwarzanie związane z:

a) rejestracją Pacjenta w PWDL,

b) zapewnieniem jakości udzielania świadczeń, m.in. poprzez badanie satysfakcji Pacjentów[13],

c) realizacją umowy z płatnikami, w szczególności z płatnikiem publicznym;

[13] badanie satysfakcji może być wykonywane w każdej formie (np. sms, e-mail, połączenie głosowe, ankieta w formie papierowej); warunkiem wykonywania badań satysfakcji w ramach przesłanki zarządzania systemami i usługami opieki zdrowotnej jest jego wykonanie w krótkim czasie po wykonaniu usługi i musi pozostawać z nią w związku a przystąpienie przez Pacjenta do badania satysfakcji ma w pełni dobrowolny charakter – nieprzystąpienie do badania satysfakcji nie może skutkować dla Pacjenta żadnymi negatywnymi konsekwencjami; nie może mieć ono również uporczywego charakteru, mogącego stworzyć po stronie Pacjenta poczucia nękania go; Pacjent powinien również zostać uprzednio poinformowany w obowiązku informacyjnym o wykonywaniu przez PWDL badań satysfakcji.

d) zapewnieniem ciągłości opieki zdrowotnej, w tym w procesie koordynacji udzielania świadczeń, co może obejmować m.in. przypomnienie o terminie realizacji świadczenia zdrowotnego, potwierdzenie wizyty, odwołanie wizyty, poinformowanie o zmianach organizacyjnych w PWDL, które mają wpływ na udzielenie oczekiwanego świadczenia;

e) komunikacją po udzieleniu świadczenia w celu oceny samopoczucia/stanu zdrowia pacjenta itp.;

f) odbieraniem i archiwizacją oświadczeń woli Pacjentów;

g) pozyskiwaniem informacji zarządczych/ zarządzaniem PWDL;

h) weryfikacją uprawnień do uzyskania świadczeń opieki zdrowotnej i rozliczaniem zrealizowanych świadczeń opieki zdrowotnej;

i) wykonywaniem innych czynności pomocniczych przy udzielaniu świadczeń zdrowotnych, a także czynności związanych z utrzymaniem systemu teleinformatycznego;

j) wymianą informacji o stanie zdrowia Pacjenta pomiędzy różnymi PWDL w celu zapewnia ciągłości opieki zdrowotnej (w oparciu o art. 26 ust. 3 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta);

k) przekazywaniem przez PWDL danych Pacjentów do rejestrów działających na podstawie ustawy o systemie informacji w ochronie zdrowia w zakresie rejestrów publicznych prowadzonych na podstawie w/w ustawy.

4.2.2.4.2. Przetwarzanie danych w tym celu odbywa się zwykle na podstawie art. 9 ust. 2 lit h) RODO w związku z art. 3 ust. 1 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.2.2.5. **zapewnienia zabezpieczenia społecznego oraz zarządzania systemami i usługami zabezpieczenia społecznego,**

4.2.2.5.1. Cel ten obejmuje w szczególności przetwarzanie związane z procesem wystawiania zaświadczeń lekarskich[14] oraz wykonywania zadań przez lekarzy orzeczników określonych w innych ustawach;

[14]Ustawa o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.

4.2.2.5.2. Przetwarzanie danych w tym celu odbywa się na podstawie art. 9 ust. 2 lit h) RODO, zwykle w związku z art. 54 ustawy o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa lub innych właściwych przepisów z zakresu prawa ubezpieczeń społecznych.

4.2.3. Do przetwarzania danych dotyczących zdrowia w celach medycznych upoważnione są osoby, o których mowa w art. 9 ust. 3 RODO. Osobami tymi będą osoby wskazane w pkt. 4.7. Kodeksu.

4.3. Przetwarzanie danych w celach innych niż zdrowotne (niewymagające zgody Pacjenta).

4.3.1. Dane osobowe Pacjenta, mogą być przetwarzane przez PWDL nie wymagając udzielania zgody przez Pacjenta także w innych wskazanych w RODO celach, w szczególności w celach określonych w art. 6 ust. 1 lit. b) – f) lub art. 9 ust. 2 lit. c), f), g), i), j)[15].

4.3.2. Możliwość powołania się na przesłankę art. 9 ust 2 lit. c) RODO opisana została w pkt. 4.10. Kodeksu.

4.4. Zakres przetwarzanych danych (niewymagające zgody Pacjenta).

4.4.1. Przetwarzane przez PWDL dane osobowe Pacjenta muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów w jakich są przetwarzane;

4.4.2. Z zastrzeżeniem pkt poprzedniego, PWDL przetwarzając dane osobowe w celach zdrowotnych może potencjalnie przetwarzać zakres danych osobowych wykraczający poza minimalny zakres danych obowiązkowo zawartych w Dokumentacji medycznej zgodnie z przepisami prawa polskiego[16]. Na przykład zazwyczaj adekwatne do celów zdrowotnych jest gromadzenie danych takich jak e-mail, czy telefon mimo że nie wchodzą w minimalny, wymagany ustawowo zakres danych zawartych w Dokumentacji medycznej[17].

---

[15]Do celów innych niż zdrowotne uzasadniających przetwarzanie danych o zdrowiu może należeć wystawianie niektórych zaświadczeń, a także dochodzenie roszczeń lub obrona przed roszczeniami.

[16]Art. 25 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

[17]Art. 9 ust. 2 lit h stanowi podstawę przetwarzania danych wrażliwych jak również danych „zwykłych" im towarzyszących. Zgodnie z motywem 35 preambuły RODO, 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. Dane dotyczące zdrowia powinny być więc rozumiane kontekstowo, jako wszelkie dane osobowe przetwarzane w związku z celami zdrowotnymi. Podobne rozważania prezentowane były w odniesieniu do ustawy o ochronie danych osobowych, która zawierała analogiczne rozwiązania prawne *„Art. 27 jest lex specialis względem art. 23. Wprawdzie także ustanawia zakaz przetwarzania danych osobowych, to jednak odmiennie reguluje przesłanki uchylające ten zakaz. Zakaz*

4.4.3. Zakwalifikowanie przetwarzanych przez PWDL danych osobowych Pacjenta jako niestanowiących Dokumentacji medycznej, np. danych zawartych w dokumentacji rozliczeniowej, raportach zarządczych[18], ankietach ds. jakości itp. nie przesądza o możliwości ich przetwarzania zgodnie z pkt. 4.2.2 Kodeksu. Oznacza to, iż dane osobowe Pacjenta nieujęte w Dokumentacji medycznej mogą również być przetwarzane w celach zdrowotnych.

4.5. Przetwarzanie danych na podstawie zgody Paejenta.

4.5.1. Przetwarzanie danych na podstawie zgody Pacjenta w praktyce funkcjonowania PWDL może mieć niekiedy miejsce w przypadku braku innych podstaw prawnych przetwarzania w szczególności w następujących sytuacjach[19]:

4.5.1.1. Przetwarzanie danych prowadzone jest w celu marketingowym PWDL, przy czym za przetwarzanie danych w celu marketingowym nie uznaje się przetwarzania służącego bezpośrednio realizacji celów zdrowotnych wskazanych w art. 9 ust. 2 lit h) RODO, nawet jeżeli skutkiem tego przetwarzania jest zwiększenie popytu na usługi świadczone przez PWDL[20];

---

przetwarzania wrażliwych danych osobowych zostaje uchylony w wyniku spełnienia przez administratora danych którejkolwiek z przesłanek wymienionych w art. 27 ust. 2. Ponadto przesłanki wymienione w art. 27 ust. 2 ***uchylają nie tylko zakaz przetwarzania wrażliwych danych osobowych, lecz również zakaz przetwarzania danych innych niż wrażliwe***" (Drozd Andrzej. art. 27. w: Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, wyd. IV. Wydawnictwo Prawnicze LexisNexis, 2008).

[18]Np. raporty dotyczące rachunku kosztów.

[19]Przetwarzanie danych przez PWDL na podstawie zgody będzie rzadką sytuacją i następować tylko w określonych przypadkach – co do zasady PWDL przetwarzają dane osobowe bez zgody Pacjenta (por. punkt 4.5.). Rekomenduje się prowadzenie rejestru udzielonych zgód. Dobra praktyką jest prowadzenie takiego rejestru w postaci elektronicznej, nawet gdy same zgody mają postać papierową. Taki rejestr powinien zawierać dane identyfikujące dokumenty zgód, co najmniej w zakresie: osoby której dotyczy zgoda, okresu obowiązywania zgody osoby przyjmującej zgodę, datę przyjęcia zgody.

[20] Zwracamy uwagę, że Administrator może przetwarzać dane osobowe zwykłe w celach marketingowych niekedy również w oparciu o uzasadniony interes, a nie tylko w oparciu o zgodę. Motyw 47 RODO określa cel marketingowy jako podstawę do opierania przetwarzania na art. 6 ust. 1 lit. f. W odniesieniu do problemu rozróżnienia celu marketingowego i celu zdrowotnego można wskazać następujący przykład: działaniem marketingowym PWDL będzie wysyłka wiadomości sms/e-mail z kodem rabatowym na świadczone przez PWDL usługi. Nie będzie natomiast działaniem marketingowym wysyłka zaproszeń w ramach działań służących profilaktyce zdrowotnej takich jak bezpłatne badania mammograficzne czy informacja z przypomnieniem o upływie rekomendowanego terminu kolejnego przeglądu higieny jamy ustnej (jeśli wynika to ze wskazań wiedzy medycznej).

4.5.1.2. Przetwarzanie danych realizowane jest w związku z realizacją Badań klinicznych[21], przy czym zgody nie będzie wymagało przetwarzanie przez PWDL danych na potrzeby udzielania świadczeń opieki zdrowotnej na rzecz pacjenta będącego uczestnikiem Badania klinicznego (np. leczenie skutków działań niepożądanych, leczenie towarzyszące itp.);

4.5.1.3. Przetwarzanie danych Pacjenta dokonywane jest przez PWDL w celu realizacji innych Badań naukowych;

4.5.1.4. Przetwarzanie danych osobowych odbywa się w związku ze zautomatyzowanym podejmowaniem decyzji w indywidualnych sprawach, przekazywaniem danych osobowych do państwa trzeciego, o ile Administrator nie posiada innej podstawy prawnej przetwarzania danych osobowych pacjentów zgodnie z RODO.

4.5.2. W przypadku, gdy podstawą przetwarzania danych osobowych ma być zgoda Pacjenta, zgoda powinna zostać wyrażona poprzez złożenie oświadczenia woli w formie ustnej lub pisemnej lub poprzez wyraźne działanie, w tym poprzez zaznaczenie okienka wyboru na formularzu lub w systemie informatycznym, przy którym są wskazane treści zgód[22].

4.5.3. Poprzez wyraźne działanie rozumie się, w szczególności, wybór przez Pacjenta określonych ustawień technicznych w systemie informatycznym, przekazanie danych osobowych przez Pacjenta w celu uzyskania odpowiedzi na zapytanie, wrzucenie wizytówki do wyznaczonego pojemnika w celu wzięcia udziału w losowaniu.

4.5.4. Zapytanie o zgodę powinno być sformułowane w jasny i przejrzysty sposób oraz odrębnie w odniesieniu do poszczególnych celów przetwarzania danych osobowych.

4.5.5. Relacja pomiędzy Pacjentem, a osobą wykonującą zawód medyczny/ osobami wykonującymi czynności pomocnicze przy udzielaniu świadczeń zdrowotnych/ PWDL ma charakter niesymetryczny i jest oparta na zaufaniu, zatem PWDL i jego personel zobowiązany jest do zapewnienia, że udzielona zgoda na przetwarzanie danych osobowych nie jest wyrażona na skutek błędu, przymusu, czy groźby. Pacjent powinien uzyskać informacje, jakie są konsekwencje niewyrażenia zgody na przetwarzanie danych na cele dodatkowe, w szczególności, że nie będzie to mieć wpływu na możliwość uzyskania świadczeń zdrowotnych i ich jakość.

---

[21] § 7 ust. 1 pkt 13 Dobrej Praktyki Klinicznej

[22] W przypadku upoważnienia do dostępu do dokumentacji medycznej, uwzględnia się dodatkowo przepisy dotyczące dokumentacji medycznej, por. §8 rozporządzenia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

4.5.6. Pacjent ma prawo wycofać zgodę w każdym momencie. Wycofanie zgody powinno następować w równie prosty sposób, jak jej wyrażenie. Wycofanie zgody może nastąpić, w szczególności, w formie ustnej lub pisemnej, poprzez zaznaczenie okienka wyboru na formularzu lub w systemie informatycznym, przy którym są wskazane treści zgód lub poprzez wybór przez Pacjenta określonych ustawień technicznych w systemie informatycznym, w zależności od rozwiązań przyjętych przez Administratora.

4.5.7. W związku z obowiązkiem zachowania zasady rozliczalności przez Administratora, za przestrzeganie ww. zasady w odniesieniu do przetwarzania danych osobowych na podstawie zgody Pacjenta należy uznać, w szczególności: archiwizowanie pisemnych oświadczeń woli Pacjenta[23], rejestrowanie rozmów telefonicznych lub posiadanie skryptów rozmów telefonicznych, dokonywanie kopii zapasowych (back-up'ów lub zrzutów z ekranu), odznaczenie odpowiednich symboli (tick'ów) w bazach danych, posiadanie stosownych polityk i procedur wewnętrznych oraz notatek z przebiegu spotkań.

4.5.8. Klauzula zgody na przetwarzanie danych osobowych powinna zawierać co najmniej nazwę i adres Administratora oraz cel (cele), w jakich Administrator będzie przetwarzać dane osobowe. Klauzula zgody może zawierać dodatkowe elementy.

4.5.9. Przykładowy wzór zgody na przetwarzanie danych osobowych stanowi załącznik nr 1 do Kodeksu.

4.6. Administrator

4.6.1. Administratorem danych osobowych Pacjentów przetwarzanych zgodnie z pkt. 4.1. Kodeksu, a także osób wskazanych w pkt. 6.4.2. jest PWDL.

4.6.2. Z zastrzeżeniem pkt. 4.6.3. każdy PWDL jest Administratorem danych Pacjentów, których dane przetwarza w celach zdrowotnych. Oznacza to w szczególności, że PWDL jest niezależnym Administratorem i nie jest zasadne na potrzeby realizacji celów zdrowotnych zawieranie z tym podmiotem jako Podmiotem przetwarzającym umowy powierzenia przetwarzania danych osobowych przekazywanych np. przez:

4.6.2.1. Pracodawcę przekazującego dane osobowe pracowników w celu objęcia ich opieką medyczną bez względu na okoliczność, czy opieka ta dotyczy świadczeń zdrowotnych z zakresu medycyny pracy, czy wykracza ona poza ten zakres (tzw. benefity pracownicze);

4.6.2.2. Organizatora udzielania świadczeń zdrowotnych lub zakład ubezpieczeń;

[23] Należy pamiętać, że RODO nie wymaga pobierania zgód na piśmie.

4.6.2.3. Inny PWDL udostępniający dane na potrzeby zachowania ciągłości usług medycznych, w tym w ramach podwykonawstwa udzielania świadczeń, w tym wykonywania badań diagnostyki laboratoryjnej i obrazowej oraz badań histopatologicznych (obejmuje to m.in. sytuacje, w których Pacjent uzyskuje świadczenia na podstawie skierowania w podmiocie, będącym podwykonawcą PWDL wydającego skierowanie na określony rodzaj badania, celem jego wykonania)[24];

4.6.2.4. Podmiot prowadzący szkołę, w celu udzielania świadczeń zdrowotnych z zakresu opieki profilaktycznej nad uczniami.

4.6.3. Pomimo przetwarzania danych Pacjentów w celach zdrowotnych, PWDL nie może być zakwalifikowany jako Administrator danych tych pacjentów, jeżeli nie jest prawnie obowiązany do prowadzenia, przechowania i udostępniania Dokumentacji medycznej, a także zapewnienia ochrony danych zawartych w tej Dokumentacji, w sposób określony w art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta we własnym imieniu i na własny rachunek, lecz działa na rzecz innego PWDL. W szczególności Administratorem danych osobowych Pacjentów nie jest Osoba wykonująca zawód medyczny, prowadząca jednoosobową działalność gospodarczą, pozostająca w stosunku prawnym
z innym PWDL, w zakresie w jakim wykonuje swoje zadania w ramach działalności leczniczej prowadzonej przez ten PWDL w miejscu pobytu Pacjenta, w tym[25]:

4.6.3.1. indywidualna praktyka lekarska wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład;

4.6.3.2. indywidualna specjalistyczna praktyka lekarska wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład;

4.6.3.3. indywidualna praktyka pielęgniarki wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład;

4.6.3.4. indywidualna specjalistyczna praktyka pielęgniarki wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład;

4.6.3.5. indywidualna praktyka fizjoterapeutyczna wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym prowadzącym ten zakład,;[26]

---

[24]Na podstawie art. 26 ust. 3 pkt. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

[25]W przypadku, gdy w Kodeksie mowa o pielęgniarce i lekarzu, rozumie się przez to również odpowiednio położną i lekarza dentystę.

[26] jeżeli taka bądź analogiczna forma prowadzenia działalności leczniczej zostanie wprowadzona przez obowiązujące przepisy prawa

4.6.3.6. PWDL w formie indywidualnej praktyki lub indywidualnej specjalistycznej praktyki lekarskiej, pielęgniarskiej lub fizjoterapeutycznej, w odniesieniu do danych Pacjentów przetwarzanych w związku z prowadzeniem działalności leczniczej w zakładzie innego podmiotu leczniczego.

4.6.4. Z podmiotami wskazanymi w pkt. 4.6.3 wykonującymi zawód medyczny, w tym w ramach praktyk zawodowych PWDL będący Administratorem na rzecz którego działają, a także z osobami wykonującymi zawód medyczny, świadczącymi pracę w innej formie na podstawie zawieranej przez nich umowy z PWDL (umowa o pracę, umowa cywilno-prawna, wolontariat), a także z osobami odbywającymi staże cząstkowe/staże kierunkowe (w ramach stażu podyplomowego lub odbywania specjalizacji) lub praktykę absolwencką nie zawiera umowy powierzenia przetwarzania, o której mowa w art. 28 RODO. [27]

4.6.5. Z PWDL innych niż określone w pkt. 4.6.4., udostępniającymi zatrudniony przez siebie personel medyczny na potrzeby udzielania świadczeń zdrowotnych w ramach innych PWDL w miejscu pobytu Pacjenta, podmioty te zobowiązane są do zawarcia umowy powierzenia przetwarzania, o której mowa w art. 28 RODO.

4.7. Dostęp do danych Pacjentów.

---

[27] Zgodnie z opinią Grupy Roboczej art. 29 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" należy wskazać dwa podstawowe warunki kwalifikowania się jako przetwarzający:

- posiadanie statusu osoby prawnej odrębnej od administratora danych,
- przetwarzanie danych osobowych w jego imieniu, przy czym działanie w czyimś imieniu oznacza działanie w interesie innego podmiotu i przypomina pojęcie prawne „przekazania uprawnień". Działania w zakresie przetwarzania danych mogą ograniczać się do ściśle określonego zadania lub kontekstu lub mieć bardziej ogólny charakter i szerszy zakres.

W związku z pierwszą przesłanką należy zauważyć, że działalność wykonywana w formie jednoosobowej działalności gospodarczej nie zapewnia statusu „osoby prawnej" odrębnej od administratora danych. Choć jest to forma prawna wyraźnie odrębna od administratora, nie stanowi ona oddzielnej osoby prawnej, lecz rodzaj wykonywania działalności przez osobę fizyczną. Jako że działalność ta może być wykonywana wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym, stanowi substytut zatrudnienia. Jednocześnie też zakres zadań osób wykonujących zawody medyczne w ramach praktyki zawodowej jest najczęściej tożsamy z zakresem zadań pracowników wykonujących ten sam zawód. W związku z tym procesy przetwarzania danych są analogiczne. W szczególności osoby wykonujące zawód w tej formie nie prowadzą własnej dokumentacji medycznej, lecz przetwarzają ją w imieniu administratora. Umowa z podmiotem leczniczym powinna zobowiązywać ich też do przestrzegania regulaminów podmiotu leczniczego i jego wewnętrznych procedur. Jak wskazano w przywołanej opinii „rola przetwarzającego nie wynika z charakteru osoby prawnej przetwarzającej dane, ale z jej konkretnej działalności w określonym kontekście". Uwzględniając powyższy kontekst, należy uznać, że praktyki zawodowe, a także osoby odbywające staże cząstkowe/kierunkowe powinny być traktowane na takich zasadach, jak pracownicy. W związku z tym nie jest potrzebne zawieranie umowy powierzenia przetwarzania z tymi podmiotami.

4.7.1. Do przetwarzania danych osobowych Pacjentów zawartych w szczególności w Dokumentacji medycznej w ramach działalności PWDL uprawnione są:

4.7.1.1. osoby wykonujące zawód medyczny;

4.7.1.2. inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych, a także czynności związane z utrzymaniem systemu teleinformatycznego, w którym przetwarzana jest Dokumentacja medyczna, i zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia Administratora[28].

4.7.2. W odniesieniu do osób wykonujących zawody medyczne PWDL stosuje następujące zasady przetwarzania:

4.7.2.1. Osoba wykonująca zawód medyczny przetwarzająca dane Pacjentów w ramach wykonywania zawodu medycznego nie musi uzyskać upoważnienia Administratora do przetwarzania danych osobowych.

4.7.2.2. Zakres przetwarzanych danych powinien być niezbędny do wykonywania zawodu medycznego, w szczególności do udzielania świadczeń opieki zdrowotnej lub musi być powiązany choćby z potencjalną możliwością udzielania świadczeń opieki zdrowotnej.

4.7.2.3. Osoba wykonująca zawód medyczny przetwarzająca dane w ramach czynności wykraczających poza wykonywanie zawodu medycznego powinna w tym zakresie uzyskać upoważnienie Administratora wskazane w art. 24 ust. 2 pkt. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

---

[28] Dobrą praktyką jest prowadzenie rejestru upoważnień w postaci elektronicznej, nawet gdy same upoważnienia mają postać papierową. Taki rejestr powinien zawierać dane identyfikujące dokumenty upoważnień, co najmniej w zakresie: osoby której dotyczy upoważnienie, okresu obowiązywania upoważnienia, osoby wydającej upoważnienie, datę wystawienia upoważnienia.

Zwracamy uwagę, że upoważnieniom do przetwarzania danych osobowych towarzyszą również zazwyczaj upoważnienia do dostępu/ przetwarzania danych w ramach systemów informatycznych. W przypadku tego rodzaju upoważnień rekomendowane jest, aby stosowane do przetwarzania systemy informatyczne odnotowywały historię zmian w zakresie uprawnień do przetwarzania nadawanych poszczególnym użytkownikom systemów, z uwzględnieniem czasu na jaki uprawnienie zostało nadane i osoby odpowiedzialnej za nadanie uprawnienia. Wskazane jeż również odnotowanie podstawy nadania i zmiany uprawnień poszczególnym użytkownikom systemów. Dobrą praktyką jest również, aby systemy informatyczne za pomocą których dokonuje się przetwarzania lub narzędzia uzupełniające ten system w zakresie monitorowania czynności przetwarzania danych umożliwiały włączenie informacji o uprawnieniach nadanych użytkownikom do analizy pozwalającej na zweryfikowanie czasu, zakresu i użytkownika systemu przetwarzającego dane. Dodatkowo w celu monitorowania dostępu do przetwarzanych danych w systemach IT, wskazane jest aby operacje przetwarzania wykonywane z użyciem systemu informatycznego były odnotowane automatycznie w dedykowanym rejestrze elektronicznym, a systemy informatyczne za pomocą których dokonuje się przetwarzania lub narzędzia uzupełniające te systemy w zakresie monitorowania czynności przetwarzania danych, umożliwiały wykonanie bieżącej analizy pozwalającej na zweryfikowanie czasu, zakresu i użytkownika systemu przetwarzającego dane.

4.7.3. Osoby wskazane w pkt. 4.7.1.2. przetwarzające dane wskazane w art. 9 ust. 1 RODO, w szczególności dane zawarte w Dokumentacji medycznej przetwarzają te dane na podstawie upoważnienia, o który mowa w art. 24 ust. 2 pkt. 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.7.4. Zakres danych wskazanych w upoważnieniu powinien być niezbędny do realizacji wykonywanych obowiązków pracownika (lub osoby świadczącej pracę na innej podstawie) i jego roli w pracy PWDL. Upoważnienie może być udzielone wyłącznie w celu wykonywania własnych obowiązków zawodowych pracownika (lub osoby świadczącej pracę na innej podstawie), nie w ramach upoważnienia zbiorczego[29].

4.7.5. Upoważnienie zawiera co najmniej następujące elementy:

4.7.5.1. Jednoznaczną identyfikację osoby, której jest udzielane;

4.7.5.2. Jednoznaczne określenie zakresu i celu przetwarzania danych w ramach upoważnienia, co może być dokonane w szczególności poprzez wskazanie umowy będącej podstawą współpracy z PWDL;

4.7.5.3. Wskazanie okresu obowiązywania poprzez oznaczenie konkretnego warunku lub terminu[30], w szczególności poprzez odwołanie się do okresu obwiązywania umowy będącej podstawą współpracy z PWDL.

4.8. Udostępnianie danych osobowych Pacjenta zawartych w dokumentacji medycznej zgodnie z art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.8.1. Z zastrzeżeniem pkt. 6.5. dane osobowe Pacjenta zawarte w Dokumentacji medycznej są udostępniane zazwyczaj na zasadach i w sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz w przepisach rozporządzeń wykonawczych wydanych na podstawie tej ustawy[31].

4.8.2. Podmiot, któremu udostępniane są dane osobowe Pacjenta w sposób wskazany w pkt. 4.8.1. jest bądź staje się ich Administratorem[32].

---

[29]Rekomendowanym rozwiązaniem przy udzielaniu upoważnień jest tworzenie profili stanowiskowych, które z uwzględnieniem zakresu czynności zawodowych, potrzebnych do ich wykonywania informacji oraz innych procesów wewnętrznych związanych z przetwarzaniem danych osobowych wskazywać będą zasadność upoważnienia.

[30]Pojęcia „warunek" lub „termin" należy definiować zgodnie z kodeksem cywilnym. Warunkiem w szczególności może być rozwiązanie umowy zawartej na czas nieokreślony lub nieoznaczony.

[31]Zwracamy uwagę na obowiązek prowadzenia przez PWDL ewidencji udostępniania dokumentacji medycznej. Forma tej ewidencji może być dowolna, jednak ze względów operacyjnych rekomenduje się prowadzenie w wersji elektronicznej jednolitego rejestru wniosków o udostępnienie dokumentacji medycznej wraz z informacjami o terminie i sposobie realizacji udostępnienia.

[32]Pod warunkiem, że zgodnie z RODO może być administratorem danych. W szczególności administratorem nie stanie się sam Pacjent, członkowie jego rodziny lub inne upoważnione osoby

4.8.3. PWDL może w celu udostępniania danych osobowych Pacjenta, zawartych w Dokumentacji medycznej prowadzonej w formie elektronicznej zgodnie z art. 26 ust 3 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta przenosić kopię tej Dokumentacji na odrębne serwery (własne lub należące do podmiotów trzecich) służące udostępnianiu danych (dla zapewnienia bezpieczeństwa i integralności danych oryginalnych) pod warunkiem zapewnienia odpowiednich środków bezpieczeństwa, w tym również zawarcia, jeśli charakter świadczonych usług tego wymaga, umowy powierzenia przetwarzania danych osobowych z podmiotami pośredniczącymi w wymianie danych[33]. Serwery te mogą w szczególności stanowić element platform wymiany danych obsługiwanych przez podmioty świadczące usługę prowadzenia repozytorium. Działania takie w przypadku przetwarzania danych na obszarze Europejskiego Obszaru Gospodarczego nie wymaga uzyskania od tych Pacjentów zgody na przetwarzanie danych osobowych.

4.8.4. W przypadku udostępniania Pacjentowi informacji zawartych w Dokumentacji medycznej dotyczących pojedynczego świadczenia zdrowotnego, PWDL może taką informację (w szczególności wynik badania lub konsultacji) udostępnić na podstawie indywidualnego numeru tego świadczenia (przekazanego wyłącznie samemu Pacjentowi lub Pacjentowi oraz PWDL wystawiającemu skierowanie). Udostępnianie informacji w wyżej wskazany sposób następuje w szczególności przy dostępie online lub przy wykorzystaniu stanowisk odbioru wyników badań (wynikomatów). Zastosowanie wyżej wskazanej metody udostępniania wymaga poinformowania Pacjenta o takiej możliwości oraz konsekwencjach przekazania indywidualnego numeru świadczenia osobie trzeciej. W przypadku udostępnienia danych z wykorzystaniem indywidualnego numeru świadczenia domniemywa się, że udostepnienie nastąpiło Pacjentowi.

4.8.5. Upoważnienie, o którym mowa w art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta:

4.8.5.1. może być udzielone w dowolnej formie[34];

4.8.5.2. upoważnienie złożone w jednym PWDL zachowuje moc w innym PWDL, chyba że coś innego wynika z treści upoważnienia.

4.8.6. Upoważnienie zawiera co najmniej następujące elementy:

4.8.6.1. Jednoznaczna identyfikacja Pacjenta;

---

najbliższe (czyli osoby fizyczne przetwarzające dane w ramach czynności o czysto osobistym lub domowym charakterze).

[33]Co do zasady udostępnianie danych osobowych Pacjenta zgodnie z art. 26 ust 3 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta za pośrednictwem tzw. platform regionalnych, nie wymaga dodatkowej zgody Pacjenta na przetwarzanie danych. Podobnie odrębnej zgody nie wymaga kopiowanie danych na serwery służące udostępnianiu danych Pacjentom lub innym podmiotom uprawnionym jako, że takie kopiowanie ma charakter czysto techniczny i służy zabezpieczeniu oryginalnej dokumentacji medycznej.

[34]Wyrok NSA sygn. II OSK 1134/16.

4.8.6.2. Jednoznaczna identyfikacja osoby udzielającej upoważnienia;

4.8.6.3. Jednoznaczna identyfikacja osoby, której udzielane jest upoważnienie, poprzez wskazanie co najmniej imienia i nazwiska tej osoby w przypadku osoby fizycznej bądź nazwy lub firmy i adresu jej siedziby (w przypadku osoby prawnej).

4.8.7. PWDL zobowiązany jest do ustalenia tożsamości Pacjenta, osoby udzielającej upoważnienia oraz osoby uzyskującej dostęp do Dokumentacji medycznej na podstawie upoważnienia. Do ustalenia tożsamości osób wskazanych w punkcie poprzednim przepisy pkt. 6.2. Kodeksu stosuje się odpowiednio.

4.8.8. W załączniku nr 2 do Kodeksu wskazano:

4.8.8.1. przykładowy katalog danych osobowych, które jednoznacznie identyfikują osoby wskazane w pkt. 4.8.6.1-3.;

4.8.8.2. przykładową treść upoważnienia, o którym mowa w art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta zgodną z przepisami obowiązującego prawa.

4.9. Wybrane zagadnienia dotyczące kwalifikacji danych, materiałów i próbek jako danych osobowych.

4.9.1. Dane i materiały poddane pseudonimizacji przez PWDL będący Administratorem, w taki sposób że ustalenie tożsamości Pacjentów, których one dotyczą przez podmioty trzecie nie jest w praktyce możliwe bez uzyskania dostępu do dodatkowych danych prawnie chronionych, jak również dane i materiały poddane anonimizacji, nie stanowią danych osobowych w odniesieniu do podmiotów trzecich nimi dysponujących nie będących Podmiotami przetwarzajacymi. Dotyczy to w szczególności:

4.9.1.1. danych zawartych w Dokumentacji medycznej bądź rozliczeniowej[35];

4.9.1.2. próbek materiału biologicznego, takich jak: komórki, tkanki, płyny ustrojowe wydzieliny i wydaliny[36];

4.9.1.3. wycisków protetycznych, modeli diagnostycznych.

4.10. Zasady przekazywania informacji dotyczących Pacjenta w stanach nagłych w oparciu o art. 9 ust. 2 lit c) RODO.

---

[35]Dotyczy to np. baz danych przekazywanych w celu realizacji badań naukowych, które nie zawierają danych „metryczkowych" takich jak imię, nazwisko czy PESEL, lecz dane dotyczące pomiarów np. wartość ciśnienia, masa ciała itp.

[36]Oznacza to, że co do zasady nie jest konieczne zawieranie umów powierzenia przetwarzania danych osobowych z podmiotami świadczącymi usługi utylizacji materiału biologicznego, chyba że próbki materiału zawierają oznaczenia zawierające dane osobowe (np. imię i nazwisko na probówce, PESEL).

4.10.1. W przypadku, w którym Pacjent nie jest fizycznie albo prawnie zdolny do wyrażenia zgody w odpowiednim czasie, w szczególności gdy:

4.10.1.1. Jest nieprzytomny,

4.10.1.2. Nie ma możliwości ustalenia nawiązania z nim kontaktu w wymaganym czasie.

PWDL może podjąć kontakt z osobą trzecią, nieupoważnioną przez Pacjenta zgodnie z przepisami prawa medycznego, w szczególności zgodnie z art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, w tym z osobą bliską w celu przekazania lub uzyskania danych, w tym danych o stanie zdrowia Pacjenta, niezbędnych dla ochrony żywotnych interesów Pacjenta lub innej osoby, w szczególności ochrony zdrowia lub życia tych osób.

4.10.2. Do sytuacji wskazanej w pkt. 4.10.1. może dojść w szczególności w następujących okolicznościach:

4.10.2.1. w przypadku nagłej utraty przytomności przez Pacjenta, gdy niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych;

4.10.2.2. w przypadku gdy Pacjent znajduje się w stanie uniemożliwiającym mu świadome wyrażenie zgody lub udzielenie wiarygodnych informacji a niezbędne jest uzyskanie dodatkowych informacji o stanie zdrowia Pacjenta w celu udzielania świadczeń zdrowotnych[37];

4.10.2.3. w przypadku uzyskania wyniku badania diagnostycznego (w szczegółowych przypadkach nawet wyniku jeszcze nie autoryzowanego), które wymaga podjęcia pilnych działań medycznych, przy braku możliwości kontaktu z Pacjentem w odpowiednim czasie przy wykorzystaniu standardowych środków komunikacji[38];

4.10.3. Wskazane wyżej działania podejmowane są zgodnie z następującymi zasadami:

4.10.3.1. PWDL odnotowuje każdorazowo okoliczności udostępnienia danych osobowych Pacjenta w oparciu o niniejszy punkt z uzasadnieniem zaistnienia stanu zagrożenia dla życia lub zdrowia Pacjenta;

---

[37]Np. stan upojenia alkoholowego czy stan po użyciu środków psychoaktywnych jak i np. afazja wywołana chorobą somatyczną.

[38]W przypadku wyników alarmowych standardową procedurą jest (o ile to możliwe) powtórzenie badania przed autoryzacją wyniku, natomiast dla ratowania zdrowia lub życia Pacjenta niekiedy nie można czekać na powtórny wynik.

4.10.3.2. PWDL podejmuje działania wskazane w pkt 4.10.1. jedynie w sytuacjach wyjątkowych, gdy nie jest możliwe udostępnienie lub uzyskanie danych od osób upoważnionych zgodnie z przepisami prawa medycznego bądź od innych PWDL, które uprzednio świadczyły usługi zdrowotne na rzecz Pacjenta w oparciu o art. 9 ust. 2 lit h RODO;

4.10.3.3. PWDL w miarę możliwości podejmuje działania w celu dostatecznego uprawdopodobnienia zasadności kontaktu z osobą trzecią w celu ochrony żywotnych interesów Pacjenta. Do działań takich można zaliczyć m.in.:

4.10.3.3.1. kontakt z Osobą bliską Pacjenta;

4.10.3.3.2. kontakt z osobą odbierającą telefon uprzednio wskazany przez Pacjenta w Dokumentacji medycznej;

4.10.3.3.3. kadawanie pytań kontrolnych dotyczących Pacjenta osobie trzeciej, która powinna znać na nie odpowiedź;

4.10.3.3.4. kontakt ze świadkiem zdarzenia w trakcie bądź w wyniku którego Pacjent został poszkodowany;

4.10.3.4. PWDL w miarę możliwości weryfikuje a także odnotowuje tożsamość osoby trzeciej, której udostępnia lub od której uzyskuje dane osobowe Pacjenta. Pkt. 6.2. stosuje się odpowiednio.

4.11. Zasady postępowania w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych

4.11.1. Załącznik nr 3 do Kodeksu zawiera zasady postępowania w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych[39].

5. Bezpieczeństwo przetwarzania danych osobowych

5.1. Pojęcie przetwarzania na dużą skalę szczególnych kategorii danych osobowych:

5.1.1. Przetwarzanie nie jest przetwarzaniem na dużą skalę, o którym mowa w art. 35 ust. 3 lit. b) RODO gdy:

5.1.1.1. Dotyczy PWDL będącego indywidualną praktyką zawodową, w odniesieniu do danych przetwarzanych w ramach wykonywanej przez osobę wykonującą zawód medycznych działalności leczniczej, w tym:

[39]Załącznik został przygotowany w oparciu o oficjalne stanowisko strony rządowej dostępne pod następującym adresem: https://www.gov.pl/cyfryzacja/rodo-w-sluzbie-zdrowia-po-pierwsze-pacjent (dostęp z dnia 26.10.2018.)

a) jednoosobowej działalności gospodarczej jako indywidualnej praktyki lekarskiej, indywidualnej praktyki lekarskiej wyłącznie w miejscu wezwania, indywidualnej specjalistycznej praktyki lekarskiej, indywidualnej specjalistycznej praktyki lekarskiej wyłącznie w miejscu wezwania;

b) jednoosobowej działalności gospodarczej jako indywidualnej praktyki pielęgniarki, indywidualnej praktyki pielęgniarki wyłącznie w miejscu wezwania, indywidualnej specjalistyczne praktyki pielęgniarki, indywidualnej specjalistycznej praktyki pielęgniarki wyłącznie w miejscu wezwania;

c) jednoosobowej działalności gospodarczej jako indywidualnej praktyki fizjoterapeutycznej, indywidualnej praktyki fizjoterapeutycznej wyłącznie w miejs cu wezwania[40].

5.1.1.2. Dotyczy PWDL udzielających ambulatoryjnych świadczeń zdrowotnych, w tym w ramach Ambulatoryjnej Opieki Specjalistycznej, które zrealizowały świadczenia dla nie więcej niż 600 Unikalnych Pacjentów miesięcznie, w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy) poprzedzających miesiąc, w którym złożony został wniosek wskazany w pkt. 7.4.1. bądź oświadczenie wskazane w pkt. 7.3.1 lub[41];

5.1.1.3. Dotyczy PWDL udzielających wyłącznie świadczeń POZ i nieposiadających więcej niż 6000 przypisanych Unikalnych Pacjentów miesięcznie, w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy według stanu na ostatni dzień miesiąca) poprzedzających miesiąc, w którym złożony został wniosek wskazany w pkt. 7.4.1. bądź oświadczenie wskazane w pkt. 7.3.1[42];

---

[40]W odniesieniu do fizjoterapeuty zapisy Kodeksu uwzględniają projektowaną nowelizację u.d.l. https://legislacja.rcl.gov.pl/projekt/12312254/katalog/12513340#12513340.

[41]Zgodnie ze sprawozdaniem NFZ za 2017 rok, średnia liczba Unikalnych Pacjentów przypadających na świadczeniodawcę AOS miesięcznie wynosiła 247 osób (6062 świadczeniodawców i 17948773 Unikalnych Pacjentów rocznie), podobnie kształtuje się obłożenie świadczeniodawców udzielających świadczeń POZ – średnio 242 Unikalnych Pacjentów miesięcznie (9560 świadczeniodawców i 27772345 Unikalnych Pacjentów rocznie). Autorzy Kodeksu nie posiadają informacji na temat kształtowania się rozkładu Unikalnych Pacjentów w stosunku do świadczeniodawców, w oparciu o wartość średnią, jednak ze względu na możliwe fluktuacje sezonowe i występowanie wielu bardzo małych świadczeniodawców (jeden lub kilku lekarzy) zaniżających wartość średnią autorzy Kodeksu postulują ustanowienie kryterium Unikalnych Pacjentów na poziomie 600 Unikalnych Pacjentów miesięcznie, co mogłoby odpowiadać w przybliżeniu obciążeniu pracą 2 pracujących w pełnym wymiarze czasu pracy lekarzy udzielających świadczeń AOS w placówce świadczeniodawcy – 30 pacjentów dziennie*20 dni roboczych*2 lekarzy.

[42]W oparciu o dane NFZ (za II półrocze 2017 roku), autorzy Kodeksu stwierdzili, że jedynie niecałe 7% lekarzy POZ ma przypisanych więcej niż 3000 pacjentów. W ocenie autorów zasadne jest uznanie, że przetwarzanie w ramach POZ danych osobowych nie jest przetwarzaniem na dużą skalę w przypadku, POZ w którym przyjmuje średnio nie więcej, niż 2 lekarzy obłożonych pracą.

5.1.1.4. Dotyczy PWDL udzielających stacjonarnych i całodobowych świadczeń zdrowotnych

a) szpitalnych, które udzielały świadczeń zdrowotnych dla nie więcej niż 200 Unikalnych Pacjentów[43];

b) innych niż szpitalne, które udzielały świadczeń zdrowotnych dla nie więcej niż 300 Unikalnych Pacjentów;

miesięcznie w ostatnich 3 miesiącach (średnia z 3 poprzednich miesięcy) poprzedzających miesiąc, w którym złożony został wniosek wskazany w pkt. 7.4.1. bądź oświadczenie wskazane w pkt. 7.3.1.

5.1.2. Wskazane w pkt. 5.1.1.2-4. progi ustalane są dla całego PWDL, po zsumowaniu wszystkich zakładów leczniczych oraz komórek organizacyjnych PWDL[44].

5.1.3. Zastosowanie monitoringu wizyjnego lub audio w placówkach PWDL, w których nie dochodzi do przetwarzania na dużą skalę, które nie wykorzystują elementów rozpoznawania cech lub właściwości obiektów, które znajdują się w monitorowanej przestrzeni, nie stanowi systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie zgodnie z art. 35 ust. 3 lit c. RODO.

5.1.4. PWDL wskazane w pkt. 5.1.1. nie są zobligowane do powoływania Inspektora Ochrony Danych na podstawie przesłanki wskazanej w art. 37 ust. 1 lit. c RODO.

5.1.5. PWDL weryfikuje co trzy miesiące począwszy od miesiąca w którym uzyskał status Podmiotu przestrzegającego Kodeksu progi wskazane w pkt. 5.1.1.2-4. W przypadku, gdy PWDL po dokonanej weryfikacji zostaje zobligowane do powoływania Inspektora Ochrony Danych na podstawie przesłanki wskazanej w art. 37 ust. 1 lit. c RODO, zobowiązany jest on do powołania Inspektora Ochrony Danych w terminie 30 dni od końca 3-miesięcznego okresu, dla którego ustalono przekroczenie progów

5.2. Bezpieczeństwo przetwarzania danych osobowych (art. 24 ust. 1, art. 28 ust. 1 i 4, art. 32 RODO)

Zwracamy uwagę, że prawie 91% lekarzy obsługuje mniej, niż 2750 pacjentów (próg zgodny z wymogami NFZ).

[43]Z danych uzyskanych z CSIOZ wynika że liczba hospitalizacji średnio miesięcznie w szpitalach posiadających co najmniej jedno łóżko wynosi ok. 960, natomiast w szpitalach które nie mają łóżek, zaledwie ok. 50 miesięcznie. Zaproponowany w Kodeksie limit oznaczać będzie w praktyce, że jedynie nieliczne, bardzo małe szpitale prowadzące działalność w niewielkiej skali, porównywalnej do skali działania przychodni, będą kwalifikować się do przetwarzania danych sensytywnych w niewielkiej skali.

[44]Sumowania należy dokonać niezależnie od tego, czy PWDL deklaruje przestrzeganie Kodeksu dla wszystkich zakładów leczniczych, czy dla niektórych zakładów leczniczych.

5.2.1. PWDL lub Podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne odpowiadające ryzyku naruszenia praw i wolności osób fizycznych, których dane są przetwarzane (podejście oparte na ryzyku).

5.2.2. Przyjmuje się, że PWDL lub Podmiot przetwarzający wdrażają w sposób właściwy podejście oparte na ryzyku na potrzeby art. 24 ust.1 oraz 32 ust 1 RODO, w przypadku stosowania metodyki stanowiącej załącznik nr 4 do Kodeksu. PWDL w stosunku do danych może stosować inne równoważne metodyki analizy ryzyka, zapewniającej nie mniejszą skuteczność w zarządzaniu ryzykiem, niż standardy zaproponowane w Kodeksie.

5.2.3. Przyjmuje się, że PWDL lub Podmiot przetwarzający stosują odpowiednie środki techniczne i organizacyjne, jeżeli:

5.2.3.1. wynikają one z przeprowadzonej właściwie analizy ryzyka oraz

5.2.3.2. PWDL i Podmiot przetwarzający dobrały i właściwie wdrożyły środki techniczne i organizacyjne spośród wskazanych w załączniku nr 5 do Kodeksu oraz stosują uznane normy/ standardy międzynarodowe wskazane w załączniku 6 do Kodeksu w odniesieniu do zagadnień objętych tymi normami/standardami.

5.2.4. Przyjmuje się, że warunek wskazany w pkt. 5.2.2. oraz wskazany w pkt. 5.2.3. może być w całości lub części spełniony poprzez wdrożenie alternatywnego (uproszczonego) podejścia wskazanego w załączniku nr 7 do Kodeksu w odniesieniu do PWDL, które:

5.2.4.1. nie przetwarzają danych na dużą skalę, o którym to przetwarzaniu mowa w art. 35 ust. 3 lit. b) RODO oraz jednocześnie

5.2.4.2. są prowadzone w formie indywidualnej lub grupowej praktyki zawodowej.

5.2.5. PWDL może stosować środki techniczne lub organizacyjne, inne niż wskazane w załącznikach nr 5, 6 lub 7, jeżeli są one adekwatne do ryzyka naruszenia praw i wolności osób fizycznych oraz zapewniają analogiczny poziom ochrony danych osobowych.

5.3. Ocena skutków dla ochrony danych (art. 35 RODO)

5.3.1. PWDL, które nie przetwarzają na dużą skalę danych zgodnie z pkt. 5.1. nie muszą przeprowadzać oceny skutków dla ochrony danych na podstawie art. 35 ust. 3 lit b RODO.

5.3.2. W przypadkach, w których nie jest jasne, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO lub gdy subiektywny osąd zawodowy i profesjonalny wskazuje na możliwość naruszenia praw i wolności osób fizycznych zaleca się jednak przeprowadzenie tej oceny, ponieważ stanowi ona narzędzie ułatwiające Administratorowi przestrzeganie przepisów o ochronie danych lub stosowanie wytycznych albo wymogów organów uprawnionych.

5.3.3. Niespełnienie warunków nakładających obowiązek przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 RODO nie narusza jednak ogólnego obowiązku wdrożenia przez PWDL środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia prawa i wolności osób, których dane dotyczą, zgodnie z pkt. 5.2. Kodeksu.

5.3.4. Ocena skutków dla ochrony danych może być przeprowadzona przez inny podmiot wybrany przez PWDL, jednak ostateczną odpowiedzialność za wykonanie tego zadania ponosi PWDL.

5.3.5. Jeżeli proces przetwarzania jest całkowicie lub częściowo realizowany przez Podmiot przetwarzający dane, Podmiot przetwarzający na mocy umowy powierzenia pomaga PWDL w przeprowadzeniu oceny skutków dla ochrony danych i dostarcza wszelkich niezbędnych informacji, mogących wpływać na ocenę poziomu ryzyka naruszenia praw i wolności osób fizycznych.

5.3.6. Przyjmuje się, że PWDL przeprowadza właściwą ocenę ryzyka na potrzeby art. 35 ust. 7 lit c RODO w przypadku stosowania metodyki stanowiącej załącznik nr 4 bądź 7 do Kodeksu. Administrator danych może stosować inne równoważne metodyki analizy ryzyka zapewniające nie mniejszą skuteczność w zarządzaniu ryzykiem, niż standardy zaproponowane w Kodeksie.

5.3.7. Przyjmuje się, że Administrator stosuje odpowiednie środki techniczne i organizacyjne na potrzeby art. 35 ust. 7 lit d RODO, jeżeli:

5.3.7.1. wynikają one z przeprowadzonej właściwie analizy ryzyka oraz

5.3.7.2. PWDL dobrał i właściwie wdrożył środki techniczne i organizacyjne spośród wskazanych w załączniku nr 5 lub 7 do Kodeksu oraz stosuje uznane normy/ standardy międzynarodowe wskazane w załączniku nr 6 do Kodeksu w odniesieniu do zagadnień objętych tymi normami/standardami.

5.3.8. Administrator może stosować środki techniczne lub organizacyjne, inne niż wskazane w załącznikach nr 5,6 lub 7, jeżeli są one adekwatne do ryzyka naruszenia praw i wolności osób fizycznych oraz zapewniają analogiczny poziom ochrony danych osobowych.

5.4. Powierzenie przetwarzania danych.

5.4.1. PWDL może powierzyć przetwarzanie danych osobowych, w tym danych zawartych w Dokumentacji medycznej, Podmiotom przetwarzającym.

5.4.2. PWDL może korzystać wyłącznie z usług takich Podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych chroniących prawa osób, których dane dotyczą oraz spełniają wymogi RODO (art. 28 ust. 1 RODO). Stosowane środki powinny zapewniać, że proces przetwarzania nie będzie powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.

5.4.3. PWDL, przed powierzeniem przetwarzania, ocenia, czy Podmiot przetwarzający zapewnia wystarczające gwarancje, o których mowa w punkcie poprzednim, w szczególności PWDL ocenia czy Podmiot przetwarzający spełnia wymogi określone w pkt. 5.2. Kodeksu. PWDL dokumentuje proces tej oceny.

5.4.4. Przyjmuje się, że Podmiot przetwarzający będący Podmiotem przestrzegającym Kodeksu spełnia wymogi określone w pkt. 5.2.

5.4.5. Kodeks nie ogranicza możliwości wyboru rozwiązań technicznych i organizacyjnych przy powierzeniu przetwarzania danych osobowych (zasada neutralności technologicznej) – Podmiot przetwarzający może wykorzystywać dowolne rozwiązania technologiczne, obejmujące również architekturę IT, w tym dowolne rozwiązania w zakresie chmury obliczeniowej[45], pod warunkiem spełnienia wymogów wskazanych w pkt. 5.4.2. Powyższe nie ogranicza wyboru przez Administratora konkretnych (preferowanych) rozwiązań technicznych i organizacyjnych wykorzystywanych przez Podmiot przetwarzający.

5.4.6. Podmiot przetwarzający może korzystać z usług innego Podmiotu przetwarzającego tylko po uzyskaniu uprzedniej szczegółowej lub ogólnej pisemnej zgody PWDL.

5.4.6.1. W przypadku ogólnej pisemnej zgody Podmiot przetwarzający informuje PWDL o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych Podmiotów przetwarzających. PWDL ma możliwość wyrażenia sprzeciwu wobec takich zmian.

5.4.6.2. Każdy Podmiot przetwarzający świadczący usługi innemu Podmiotowi przetwarzającemu zapewnia przetwarzanie zgodne z wymogami RODO, w tym wdrożenie odpowiednich środków technicznych i organizacyjnych zgodnie z pkt. 5.4.2.

5.4.7. Przetwarzanie przez Podmiot przetwarzający może odbywać się na podstawie umowy zawartej z PWDL, sporządzonej w formie pisemnej, w tym elektronicznej, której treść jest zgodna z postanowieniami RODO. Umowa powierzenia przetwarzania może również mieć postać klauzul umownych będących częścią umowy o szerszym zakresie np. umowy o świadczenie usług.

[45]np. hosting, chmura obliczeniowa (prywatna, hybrydowa, publiczna).

5.4.8. Podmiot przetwarzający umożliwia osobie lub podmiotowi upoważnionemu przez PWDL przeprowadzenie audytu w zakresie zgodności przetwarzania z postanowieniami umowy i przepisami prawa.

5.4.9. W przypadkach uzasadnionych zasadami ochrony danych osobowych przyjętych przez Podmiot przetwarzający i Administratora, prawo wskazane w pkt. 5.4.7. może zostać zrealizowane poprzez wskazanie w umowie powierzenia przetwarzania danych, iż audyt będzie przeprowadzany przez profesjonalnych, niezależnych audytorów, przy czym wyniki audytu muszą być udostępnione Administratorowi bez zbędnej zwłoki.

5.5. Szkolenia jako element zapewnienia bezpieczeństwa danych osobowych.

5.5.1. PWDL i Podmiot przetwarzający podejmują skuteczne działania mające na celu osiągnięcie i utrzymanie odpowiedniego poziomu kwalifikacji personelu w zakresie przetwarzania danych osobowych, w tym środowiska teleinformatycznego i bezpieczeństwa informacji przetwarzanych w tym środowisku.

5.5.2. PWDL i Podmiot przetwarzający utrzymują kwalifikacje całego personelu na poziomie odpowiednim dla zapewnienia bezpieczeństwa przetwarzanych danych osobowych, w tym danych przetwarzanych w środowisku teleinformatycznym i umożliwienia właściwego korzystania ze sprzętu i systemów informatycznych. Poziom ten powinien być zróżnicowany w zależności m.in. od ryzyka związanego z poziomem uprawnień i kompetencji poszczególnych pracowników oraz pełnionej przez nich roli przy przetwarzaniu danych osobowych, w tym w systemie zarządzania bezpieczeństwem środowiska teleinformatycznego.

5.5.3. W celu zapewnienia odpowiedniego poziomu kwalifikacji personelu w powyższym zakresie, PWDL i Podmiot przetwarzający stosuje adekwatne formy szkoleń, zapewnia właściwe materiały, jak również prowadzi różnorodne akcje edukacyjne mające na celu podniesienie kultury bezpieczeństwa informacji (np. z wykorzystaniem plakatów czy wygaszaczy ekranu).

5.5.4. Wskazane w poprzednim ustępie działania muszą mieć charakter cykliczny i być udokumentowane przez PWDL lub Podmiot przetwarzający, ponadto pierwsze szkolenie odbywa się przed rozpoczęciem przetwarzania danych przez personel lub niezwłocznie po rozpoczęciu przetwarzania danych.

6. Prawa Pacjentów

6.1. Ogólne zasady dotyczące realizacji praw pacjentów jako podmiotów danych.

6.1.1. Wszelką komunikację z Pacjentem w zakresie realizacji jego Praw jako podmiotu danych PWDL prowadzi:

6.1.1.1. w języku polskim;

6.1.1.2. w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem;

6.1.1.3. w formie pisemnej, ustnej lub elektronicznej;

6.1.1.4. w terminach określonych w art. 12 ust. 3 i 12 ust. 4 RODO.

6.1.2. W przypadku, w którym Pacjent nie posługuje się językiem polskim, PWDL – w miarę możliwości finansowych i organizacyjnych oraz przy uwzględnieniu dostępności tłumaczy danego języka - może podjąć działania w celu zapewnienia Pacjentowi możliwości otrzymania informacji również w języku znanym Pacjentowi.

6.1.3. Wszelką komunikację z Pacjentem w zakresie realizacji jego praw jako podmiotu danych należy podejmować po ustaleniu tożsamości Pacjenta na zasadach określonych w punkcie 6.2. Kodeksu.

6.1.4. Komunikacja z Pacjentem w zakresie realizacji jego praw jako podmiotu danych jest wolna od opłat.

6.1.5. W przypadku żądań Pacjenta podejmowanych na podstawie art. 15-22 RODO ewidentnie nieuzasadnionych lub nadmiernych, w szczególności ze względu na swój ustawiczny charakter, PWDL może pobrać opłatę lub odmówić podjęcia działań. Przy ustaleniu wysokości opłaty uwzględnia się administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań. Opłata może mieć charakter zryczałtowany i być ustalona w formie cennika dostępnego dla Pacjentów.

6.1.6. Za ewidentnie nieuzasadnione lub nadmierne żądania Pacjenta, które uzasadniają pobranie opłaty bądź odmowę podjęcia działań, uznaje się w szczególności skierowane do tego samego PWDL:

6.1.6.1. żądania o informacje częściej niż raz na 3 miesiące, jeżeli zakres danych przetwarzanych przez PWDL bądź inne okoliczności związane z przetwarzaniem nie ulegały zmianie od czasu złożenia poprzedniego żądania;

6.1.6.2. żądania o informacje dzielone sztucznie na kilka lub kilkanaście żądań;

6.1.6.3. żądanie szczególnego, niestandardowego formatu odpowiedzi;

6.1.6.4. żądanie udzielenia odpowiedzi w języku innym niż polski.

6.1.7. Za ewidentnie nieuzasadnione lub nadmierne żądania osoby, które uzasadniają odmowę ich zrealizowania, uznaje się w szczególności:

6.1.7.1. żądanie informacji, których przekazanie spowodowałyby nieuprawnione ujawnienie tajemnicy przedsiębiorstwa, tajemnicy zawodowej personelu medycznego lub danych osobowych innego Pacjenta lub innej tajemnicy prawnie chronionej;

6.1.7.2. składanie żądania częściej niż raz na miesiąc, jeżeli zakres danych przetwarzanych przez PWDL bądź inne okoliczności związane z przetwarzaniem istotne dla przedmiotu żądania nie ulegały zmianie od czasu złożenia poprzedniego żądania (ustawiczny charakter żądania);

6.1.8. PWDL zobowiązany jest do każdorazowego uzasadnienia i podania do wiadomości osoby zgłaszającej żądanie przyczyny pobrania opłaty lub odmowy podjęcia działań poprzez wskazanie, dlaczego w jego ocenie żądania są ewidentnie nieuzasadnione lub nadmierne.

6.2. Zasady weryfikacji tożsamości Pacjentów

6.2.1. PWDL zobowiązany jest do zweryfikowania tożsamości Pacjenta przed:

6.2.1.1. utrwaleniem danych osobowych zebranych bezpośrednio od Pacjenta, w szczególności w związku z udzielaniem świadczeń zdrowotnych, chyba że ustalenie tożsamości przed uzyskaniem świadczenia nie jest możliwe i mogłoby istotnie utrudnić lub uniemożliwić uzyskanie świadczenia[46];

6.2.1.2. realizacją żądań Pacjentów wynikających z art. 15-22 RODO;

6.2.1.3. udostępnieniem Pacjentowi informacji zawartych w Dokumentacji medycznej i/lub informacji objętych tajemnicą osób wykonujących zawody medyczne zgodnie z art. 13 Ustawy o prawach pacjenta w związku z realizacją prawa Pacjenta do informacji i prawa do Dokumentacji medycznej.

6.2.2. Weryfikacji tożsamości Pacjenta dokonuje się poprzez kontrolę okazanego przez Pacjenta dokumentu potwierdzającego tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny numer jednoznacznie identyfikujący Pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, legitymacja studencka, legitymacja szkolna, prawo jazdy, paszport lub inny dokument urzędowy ze zdjęciem.

6.2.3. PWDL może utrwalić informację o:

6.2.3.1. dacie dokonania weryfikacji tożsamości; oraz

6.2.3.2. dokumencie, na podstawie którego została ona dokonana, z jednoczesnym wskazaniem numeru/identyfikatora tego dokumentu (np. numer i seria dowodu osobistego)[47].

---

[46]np. osoba nieprzytomna lub wymagająca pilnej interwencji lekarskiej

[47]Co do zasady PWDL nie jest natomiast uprawniony do dokonywania kopii dokumentu potwierdzającego tożsamość.

6.2.4. W przypadku, jeżeli w imieniu Pacjenta małoletniego w okolicznościach wskazanych w pkt. 6.2.1. występuje Przedstawiciel ustawowy, to tożsamość Pacjenta może być potwierdzona również przez Przedstawiciela ustawowego w drodze oświadczenia i okazania dowodu tożsamości Przedstawiciela ustawowego zgodnie z pkt. 6.2.2. PWDL może utrwalić informację o dacie dokonania weryfikacji oraz dokumencie Przedstawiciela ustawowego, na podstawie którego została ona dokonana.

6.2.5. W przypadku, jeżeli Pacjentowi małoletniemu towarzyszy Opiekun faktyczny, który wyraża zgodę na badanie, to przed utrwaleniem danych w związku z tym badaniem, zgodnie z pkt 6.2.1.1. tożsamość Pacjenta może być potwierdzona również przez opiekuna faktycznego w drodze oświadczenia i okazania dowodu tożsamości opiekuna faktycznego zgodnie z pkt. 6.2.2. PWDL może utrwalić informację o dacie dokonania weryfikacji oraz dokumencie opiekuna faktycznego, na podstawie którego została ona dokonana.

6.2.6. W przypadku, gdy weryfikacja tożsamości na potrzeby realizacji czynności wskazanych w pkt. 6.2.1. realizowana jest w sposób inny niż osobiście (np. na odległość lub przy użyciu środków komunikacji elektronicznej) lub w sytuacji powzięcia przez PWDL wątpliwości co do tożsamości osoby zgłaszającej żądanie, PWDL uprawniony jest do żądania dodatkowych informacji lub podjęcia przez osobę zgłaszającą żądanie dodatkowych działań niezbędnych do potwierdzenia tożsamości tej osoby, takich jak:

6.2.6.1. podanie dodatkowych danych osobowych w celu ich porównania z posiadanymi przez PWDL; lub

6.2.6.2. dokonanie czynności weryfikacyjnych przy użyciu dostępnych PWDL oraz osobie zgłaszającej żądanie narzędzi, w tym przy wykorzystaniu kwalifikowanego podpisu elektronicznego lub podpisu potwierdzonego profilem zaufanym ePUAP, przelewu bankowego potwierdzającego zgodność danych, uwierzytelnianie za pośrednictwem systemów informatycznych udostępnianych w ramach systemu informacji w ochronie zdrowia, np. Internetowe Konto Pacjenta, dwu lub kilkustopniowe uwierzytelnianie w systemie teleinformatycznym, lub

6.2.6.3. kontrolę na odległość dokumentu potwierdzającego tożsamość analogicznie do pkt. 6.2.2[48].

[48] Takie okazanie może być dokonane np. w trakcie wideotransmisji.

6.2.7. W celu uniknięcia wątpliwości, zakres danych, jakich może żądać PWDL w celu potwierdzenia tożsamości zgodnie z pkt. 6.2.6. może być szerszy, niż wymagany ustawowo zakres danych identyfikujących Pacjenta zawartych w Dokumentacji medycznej, przy czym zakres danych, których PWDL żąda od Pacjenta lub jego Przedstawiciela ustawowego lub opiekuna faktycznego powinien być adekwatny do rodzaju przetwarzanych danych, rodzaju zgłaszanego żądania oraz sposobu kierowania żądania i udzielania odpowiedzi na to żądanie. PWDL dokonuje wyboru dodatkowych informacji lub działań niezbędnych do potwierdzenia tożsamości zgodnie z pkt. 6.2.6. w oparciu o przeprowadzoną analizę ryzyka mając na względzie zapewnienie realizacji praw przysługujących Pacjentom i innym osobom w sposób możliwie najmniej uciążliwy.

6.2.8. PWDL może utrwalić informację o dacie i sposobie przeprowadzenia weryfikacji dokonanej zgodnie z pkt. 6.2.6. w tym również utrwalić pozyskane na potrzeby weryfikacji dane.

6.3. Obowiązek informacyjny względem Pacjentów w przypadku zbierania danych bezpośrednio od nich (art. 13 RODO)

6.3.1. PWDL przekazuje Pacjentom informacje, o których mowa w art. 13 RODO w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie, a także jasnym i prostym językiem, w tym w formie graficznej.

6.3.2. Obowiązek informacyjny może być zrealizowany poprzez:

6.3.2.1. podjęcie co najmniej 2 ze wskazanych poniżej działań podjętych jednocześnie przez PWDL:

6.3.2.1.1. umieszczenie klauzul informacyjnych w dokumentach przekazywanych Pacjentowi (np. umowa o świadczenie usług medycznych); lub

6.3.2.1.2. umieszczenie klauzul informacyjnych na stronie internetowej PWDL lub w systemie informatycznym PWDL dostępnym dla Pacjenta (tzw. Portal Pacjenta) lub w formie nagrania na infolinii lub w formie wiadomości e-mail lub sms; lub

6.3.2.1.3. umieszczenie informacji na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez Pacjentów (w szczególności ciągi komunikacyjne lub izba przyjęć lub rejestracja lub poczekalnia); lub

6.3.2.2. umieszczenie klauzul informacyjnych w regulaminie organizacyjnym PWDL przy jednoczesnym zapewnieniu podania do publicznej wiadomości treści klauzul zgodnie z art. 24 ust. 2 lub 2a ustawy o działalności leczniczej.

6.3.3. W odniesieniu do Pacjentów, którym udzielane są świadczenia w miejscu wezwania, przyjmuje się, że dla zrealizowania obowiązku informacyjnego zgodnie z art. 13 RODO przez PWDL wystarczające jest podjęcie działania wskazanego w pkt. 6.3.2.1.1. lub jeżeli wizyta w miejscu wezwania została zamówiona za pomocą systemów teleinformatycznych lub systemów łączności, wystarczające jest umieszczenie klauzul informacyjnych zgodnie z pkt. 6.3.2.1.2.

6.3.4. W odniesieniu do Pacjentów, dla których świadczenie jeżeli odbywa się za pomocą systemów teleinformatycznych lub systemów łączności, do spełnienia obowiązku informacyjnego wskazany w art. 13 RODO wystarczające jest umieszczenie klauzul informacyjnych zgodnie z pkt. 6.3.2.1.2.

6.3.5. PWDL zobowiązany jest realizować zasadę rozliczalności w zakresie spełnienia obowiązku informacyjnego poprzez archiwizację plików (w tym wzorów i zdjęć) i dokumentów, które dowodzą że obowiązek informacyjny wobec Pacjentów został zrealizowany. Informacje udostępnione Pacjentowi w celu realizacji obowiązku informacyjnego zawierają datę ostatniej aktualizacji[49].

6.3.6. Obowiązku informacyjnego wobec Pacjentów nie trzeba realizować jeśli Pacjent posiada już stosowne informacje.

6.3.7. Przepisy pkt. 6.3.1-6.3.6. stosuje się odpowiednio do Przedstawicieli ustawowych lub innych osób o których PWDL pozyskuje bezpośrednio dane osobowe w związku z realizacją celów zdrowotnych wobec Pacjenta.

6.4. Obowiązek informacyjny względem Pacjentów w przypadku zbierania danych niebezpośrednio od nich (art. 14 RODO)

6.4.1. W przypadku, w którym PWDL wchodzi w posiadanie danych osobowych Pacjenta na potrzeby realizacji celów zdrowotnych przetwarzania, PWDL nie musi realizować wobec Pacjenta obowiązku informacyjnego w związku z wyłączeniem wskazanym w art. 14 ust. 5 lit c RODO[50].

6.4.2. W przypadku, w którym PWDL wchodzi w posiadanie danych osobowych Przedstawicieli ustawowych, osób upoważnionych do dostępu do Dokumentacji medycznej Pacjenta lub zasięgania informacji o jego stanie zdrowia lub też innych osób wskazanych przez Pacjenta w związku z udzielaniem mu świadczeń zdrowotnych i utrwalonych w Dokumentacji medycznej, PWDL nie musi realizować wobec tych osób obowiązku informacyjnego. Podstawą wyłączenia tego obowiązku jest art. 14 ust. 5 lit. c lub d RODO.

6.5. Prawo Pacjenta do dostępu do danych (art. 15 RODO)

---

[49]Wskazanie, że jest to wersja z dnia X itp.

[50]Taka okoliczność może wystąpić np. w przypadku udostępniania przez pracodawcę danych osobowych pracownika za jego zgodą placówce medycznej, która ma objąć go opieką np. w ramach abonamentów medycznych.

6.5.1. Prawo Pacjenta do dostępu do danych osobowych, o którym mowa w art. 15 RODO, jest prawem odrębnym od prawa Pacjenta do informacji o swoim stanie zdrowia, o którym mowa w art. 9 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz od prawa dostępu do Dokumentacji medycznej, o którym mowa w art. 23 ust. 1 ustawy o prawach pacjenta.[51].

6.5.2. Pacjent ma prawo swobodnego wyboru podstawy oraz zakresu żądania związanego z dostępem do informacji na jego temat przetwarzanych przez PWDL.

6.5.3. PWDL informuje Pacjenta o możliwości uzyskania nieodpłatnej pierwszej kopii przetwarzanych danych osobowych, w tym danych zawartych w Dokumentacji medycznej zgodnie z art. 15 ust. 3 RODO, w terminie wskazanym w art. 12 ust. 3 RODO ze wskazaniem zakresu tego prawa, w sposób wskazany w pkt. 6.3.2. Kodeksu lub w inny sposób, nie później niż na etapie ubiegania się o realizację tego prawa.

6.5.4. Skierowanie przez Pacjenta żądania udostępnienia informacji o stanie zdrowia bądź Dokumentacji medycznej, bez wskazania, że Pacjent zamierza zrealizować prawo dostępu do danych osobowych, o którym mowa w art. 15 RODO, rodzi obowiązki wskazane odpowiednio w art. 9 lub art. 23 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

6.5.5. W przypadku, w którym Pacjent jednoznacznie powołuje się na prawo dostępu do danych osobowych, o którym mowa w art. 15 RODO, w zależności od zakresu wskazanego w żądaniu, Pacjent jest uprawniony do:

6.5.5.1. uzyskania od PWDL potwierdzenia, czy PWDL przetwarza jego dane osobowe, a jeżeli ma to miejsce,

6.5.5.2. uzyskania dostępu do tych danych oraz informacji wskazanych w art. 15 ust. 1 lit. a – h oraz art. 15 ust. 2 RODO. Obowiązek informacyjny wynikający z art. 15 RODO powinien być realizowany na zasadach określonych w art. 6.1.Kodeksu;

6.5.5.3. uzyskania od PWDL kopii danych osobowych podlegających przetwarzaniu, w tym kopii danych zawartych w Dokumentacji medycznej oraz innych danych osobowych Pacjenta (ale nie wyciągu lub odpisu). Udostępnianie danych zawartych w Dokumentacji medycznej zgodnie z art. 15 ust. 3 nie jest równoznaczne z obowiązkiem udostępniania danych w formacie i strukturze właściwej dla Dokumentacji medycznej.

[51]O odrębności wskazanych praw świadczy m.in. ich cel i specyfika oraz ich zakres. W szczególności maksymalne terminy realizacji prawa z art. 15 RODO wskazane w art. 12 ust. 3 RODO, czy też odmowa udostępnienia dokumentacji medycznej na podstawie art. 12 ust. 5 RODO stanowiłyby jaskrawe naruszenie praw Pacjenta zgodnie z polskimi przepisami. W określonych sytuacjach, realizacja każdego z tych praw może jednak prowadzić do podobnych skutków.

6.5.6. Przed udostępnieniem Pacjentowi żądanych informacji, w szczególności zaś przed udzieleniem Pacjentowi dostępu do danych osobowych lub wydaniu Pacjentowi kopii danych osobowych, w tym w formie elektronicznej, PWDL weryfikuje tożsamość Pacjenta na zasadach określonych w punkcie 6.2.

6.5.7. Jeżeli wykonywanie prawa dostępu do danych osobowych na podstawie art. 15 RODO wiąże się z udostępnieniem Pacjentowi kopii Dokumentacji medycznej, fakt ten jest odnotowywany w wykazie wskazanym w art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wraz ze wskazaniem, że do udostępnienia doszło na podstawie tego artykułu.

6.5.8. W przypadku realizacji prawa do informacji zgodnie z art. 15 ust. 3 poprzez udostępnienie kopii Dokumentacji medycznej, przekazanie Pacjentowi zawartych w jego Dokumentacji medycznej danych osobowych innych osób, w szczególności osób wykonujących zawód medyczny, dokonujących wpisu do Dokumentacji medycznej bądź osób upoważnionych do dostępu do Dokumentacji medycznej jest dopuszczalne.

6.5.9. Upoważnienie, o którym mowa w art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta nie stanowi podstawy do realizacji przez osobę upoważnioną prawa Pacjenta do dostępu do danych zgodnie z art. 15 RODO.

6.5.10. Zgodnie z art. 15 ust. 3 RODO, nieodpłatnemu udostępnieniu podlega pierwsza kopia przetwarzanych danych. PWDL może pobierać opłatę od kolejnych kopii. Za kolejne kopie uznaje się w szczególności Dokumentację medyczną w zakresie w jakim była uprzednio udostępniona (uprzednio udostępnione i niezmienione dokumenty Dokumentacji medycznej)[52].

6.5.11. Za rozsądną wysokość opłaty, o której mowa w art. 15 ust. 3 RODO uznaje się opłatę nie wyższą, niż opłaty wskazane w art. 28 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. PWDL może pobrać opłatę wyższą jeżeli uzasadniają to udokumentowane, istotne koszty administracyjne.

6.5.12. Kopię danych, w tym kopię Dokumentacji medycznej, zgodnie z art. 15 ust. 3 można przekazać w postaci elektronicznej w szczególności poprzez przesłanie danych na adres e-mail wskazany przez Pacjenta lub inny powszechnie stosowany sposób transmisji danych. W przypadku niewskazania adresu e-mail lub innego sposobu transmisji elektronicznej PWDL zwraca się do Pacjenta o wskazanie adresu e-mail lub innego powszechnie stosowanego sposobu transmisji elektronicznej informując jednocześnie Pacjenta o najczęstszych zagrożeniach związanych z transmisją elektroniczną.

[52]Dokumentacja medyczna Pacjenta kumuluje się w czasie, w przypadku gdy Pacjent zwraca się o udostępnienie po raz kolejny kopii dokumentacji medycznej na podstawie art. 15 ust. 3 RODO, to nieodpłatne udostępnienie dotyczy wyłącznie części, która nie została udostępniona uprzednio.

6.5.13. PWDL dowolnie zabezpiecza transmisję danych w postaci elektronicznej zgodnie z przeprowadzoną analizą ryzyka, przy czym poziom bezpieczeczeństwa nie może być niższy od poziomu bezpieczeństwa gwarantowanego przez minimalne zabezpieczenie wskazane w pkt. 6.5.14:

6.5.14. Minimalnym zabezpieczeniem przekazania danych w postaci elektronicznej, przesłanych na adres e-mail wskazany przez Pacjenta lub inny powszechnie stosowany sposób transmisji elektronicznej, jest zabezpieczenie składające się z następujących elementów:

6.5.14.1. Uprzednie poinformowanie Pacjenta o zagrożeniach dotyczących ochrony danych osobowych związanych z proponowanym kanałem komunikacji;

6.5.14.2. utworzenie plików zawierających zaszyfrowane informacje za pomocą programu kompresującego 7-Zip[53];

6.5.14.3. podczas tworzenia pliku należy wprowadzić hasła zabezpieczające plik;

6.5.14.4. do odszyfrowania przez Pacjenta przekazanej w skompresowanym pliku informacji niezbędne jest wprowadzenie klucza kryptograficznego (hasła), który został użyty podczas jego tworzenia. Klucz taki powinien zostać przesłany do odbiorcy innym, bezpiecznym kanałem komunikacji.[54]

[53] Opinia GIODO w sprawie bezpieczeństwa danych przekazywanych przy użyciu poczty elektronicznej https://giodo.gov.pl/pl/222/9801.

[54] Bezpiecznym kanałem komunikacyjnym do przekazania hasła jest np. sms przesłany na telefon Pacjenta, przekazanie hasła pocztą tradycyjną, przekazanie hasła do rąk własnych Pacjenta lub osoby przez niego upoważnionej.

6.6. Prawo Pacjenta do sprostowania i uzupełnienia danych osobowych (art. 16 RODO)

6.6.1. Pacjent ma prawo zażądać w każdym momencie niezwłocznego sprostowania danych osobowych go dotyczących, które przetwarza PWDL. Pacjent ma również prawo żądania uzupełnienia niekompletnych danych osobowych na jego temat przetwarzanych przez PWDL, w tym poprzez przedstawienie dodatkowego oświadczenia.

6.6.2. Pacjent ma prawo zażądać niezwłocznego sprostowania lub uzupełnienia danych osobowych zawartych w Dokumentacji medycznej wyłącznie w zakresie w jakim nie będzie prowadzić to do naruszenia autonomii zawodowej osoby wykonującej zawód medyczny, która dokonywała wpisu do Dokumentacji medycznej[55].

6.6.3. Wraz z wykonaniem żądania Pacjenta dotyczącego sprostowania lub uzupełnienia danych osobowych, PWDL dokonuje oceny istotności i charakteru wprowadzonych sprostowań i uzupełnień:

6.6.3.1. jeżeli niepoinformowanie określonych odbiorców danych o zmianach będzie nieść za sobą zagrożenie dla życia lub zdrowia Pacjenta, PWDL niezwłocznie; informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16 RODO, każdego z tych odbiorców, którym ujawnił dane osobowe, chyba że okaże się to niemożliwe. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda;

6.6.3.2. jeżeli niepoinformowanie określonych odbiorców danych o zmianach nie będzie niosło za sobą zagrożenia dla życia i zdrowia Pacjenta, PWDL informuje każdego z tych odbiorców, którym ujawnił dane osobowe Pacjenta o zakresie dokonanych zmian, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Dla uniknięcia wątpliwości interpretacyjnych, za działania wymagające niewspółmiernie dużego wysiłku w sytuacji wskazanej w zdaniu poprzednim uważa się w szczególności następujące działania wobec odbiorców:

6.6.3.2.1. poinformowanie o zmianach odbiorców, z którymi nie jest możliwy kontakt drogą e-mailową, lub;

6.6.3.2.2. poinformowanie o zmianach odbiorców, których tożsamości PWDL nie zna w chwili dokonania sprostowania lub usunięcia zgodnie z art. 16 RODO, lub;

[55]Należy pamiętać, że jeżeli wykonanie żądania Pacjenta prowadzi do zmiany wpisów w dokumentacji medycznej go dotyczącej, zmiany te należy odnotowywać w sposób właściwy dla dokumentacji medycznej.

6.6.3.2.3. poinformowanie o zmianach odbiorców, którym udostępniono dane osobowe wcześniej, niż na rok od chwili dokonania sprostowania lub usunięcia danych.

6.7. Prawo Pacjenta do usunięcia danych - „bycia zapomnianym" (art. 17 RODO)

6.7.1. Prawo Pacjenta do bycia zapomnianym nie znajduje zastosowania wobec danych osobowych Pacjentów przetwarzanych na podstawie art. 9 ust. 2 lit h RODO, w szczególności wobec danych przetwarzanych w ramach Dokumentacji medycznej prowadzonej i przechowywanej przez okres wskazany w art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz innych przepisach dotyczących okresu przechowywania Dokumentacji medycznej.

6.7.2. PWDL odmawia zrealizowania prawa Pacjenta do bycia zapomnianym w odniesieniu do danych osobowych zawartych w Dokumentacji medycznej przez cały wymagany przepisami prawa okres archiwizacji Dokumentacji medycznej powołując się na przepis art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta lub inne przepisy dotyczące okresu przechowywania Dokumentacji medycznej w zw. z art. 17 ust. 3 lit. b) RODO.

6.7.3. W przypadku gdy przetwarzanie danych osobowych Pacjenta odbywa się na podstawie zgody Pacjent może zrealizować prawo do bycia zapomnianym (usunięcia danych) w zakresie celu, w którym dane osobowe Pacjenta są przetwarzane na podstawie tej zgody, pod warunkiem że zachodzi przynajmniej jedna z przesłanek wskazanych w art. 17 ust. 1 RODO.

6.7.4. W przypadku usunięcia przez PWDL danych zawartych w Dokumentacji medycznej w związku z żądaniem Pacjenta złożonym po upływie terminu przechowywania Dokumentacji medycznej wskazanego w przepisie art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta lub innych przepisach dotyczących okresu przechowywania Dokumentacji medycznej, przyjmuje się, że podmioty, którym dokumentacja ta została uprzednio udostępniona posiadają wiedzę o usunięciu zgodnie z art. 19 RODO[56].

6.7.5. W odniesieniu do osób wskazanych w pkt. 6.4.3. pkt. 6.7.1.-6.7.4. stosuje się odpowiednio.

6.8. Prawo Pacjenta do żądania ograniczenia przetwarzania danych (art. 18 RODO)

[56]Proponujemy przyjęcie takiej konstrukcji – zarówno czas wytworzenia dokumentacji medycznej, jak i okres jej ustawowego przechowywania są znane odbiorcom danych.

6.8.1. Pacjent ma prawo żądać ograniczenia przetwarzania danych zgodnie z przesłanką określoną w art. 18 ust. 1 lit a) RODO w odniesieniu do danych osobowych Pacjentów przetwarzanych na podstawie art. 9 ust. 2 lit h RODO w tym w szczególności wobec danych przetwarzanych w ramach Dokumentacji medycznej i innych przetwarzanych w oparciu o ww. przesłankę[57].

6.8.2. Ograniczenie przetwarzania ma na celu zabezpieczenie danych przed dalszą możliwością ich przetwarzania za wyjątkiem przechowywania. Ograniczenie przetwarzania może polegać m.in. na czasowym przeniesieniu wybranych danych osobowych do innego systemu przetwarzania lub uniemożliwieniu odbiorcom danych dostępu do wybranych danych.

6.8.3. Prawo Pacjenta do żądania ograniczenia przetwarzania danych nie jest jednak bezwzględne. PWDL może przetwarzać dane osobowe Pacjentów m.in. w celu realizacji ważnego interesu publicznego, za który uznaje się w szczególności:

6.8.3.1. wykonywanie zadań, obowiązków oraz realizacja usług wynikających z ustawy o systemie informacji w ochronie zdrowia, jeśli ograniczenie przetwarzania może zakłócić wykonywanie zapisów tej ustawy;

6.8.3.2. wykonywanie obowiązków wynikających z innych przepisów prawa medycznego, w przypadku gdy ograniczenie przetwarzania może stwarzać ryzyko naruszenia zdrowia publicznego;

6.8.3.3. wykonywanie zobowiązań wynikających z realizacji umowy z płatnikiem publicznym, w tym w szczególności prowadzenia sprawozdawczości;

6.8.3.4. udostępniania danych na potrzeby przeprowadzania kontroli przez uprawnione z mocy prawa organy lub podmioty;

6.8.3.5. realizacji celów archiwalnych, Badań naukowych, historycznych lub celów statystycznych.

6.8.4. W odniesieniu do osób wskazanych w pkt. 6.4.3. pkt. 6.8.3. stosuje się odpowiednio.

6.9. Prawo Pacjenta do przenoszenia danych (art. 20 RODO)

6.9.1. Prawo Pacjenta do przenoszenia danych nie znajduje zastosowania wobec danych osobowych przetwarzanych przez PWDL na podstawie art. 9 ust. 2 lit. h RODO, w tym w szczególności wobec danych przetwarzanych w ramach Dokumentacji medycznej i innych przetwarzanych w oparciu o ww. przesłankę.

[57] Art. 18 ust. 1 RODO.

6.9.2. W przypadku otrzymania żądania Pacjenta związanego z wykonywaniem prawa do przenoszenia danych w odniesieniu do danych osobowych zgromadzonych w Dokumentacji medycznej, PWDL ma obowiązek poinformować Pacjenta o braku podstawy prawnej tego prawa oraz poinformować o trybie w jakim Pacjent może uzyskać dostęp do Dokumentacji medycznej.

6.9.3. Prawo Pacjenta do przenoszenia danych znajduje zastosowanie wyłącznie wobec operacji przetwarzania danych osobowych prowadzonych przez PWDL, które mają charakter zautomatyzowany i które prowadzone są w oparciu o zgodę Pacjenta na przetwarzanie danych osobowych lub w oparciu o umowę, której Pacjent jest stroną.

6.9.4. Przetwarzanie danych w sposób zautomatyzowany ma miejsce wyłącznie gdy prowadzone jest ono z wykorzystaniem urządzeń i systemów informatycznych i nie obejmuje ono żadnych dokumentów w postaci papierowej.

6.9.5. W ramach realizacji prawa Pacjenta do przenoszenia danych Pacjent może:

6.9.5.1. otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe dotyczące Pacjenta, które Pacjent dostarczył PWDL (art. 20 ust. 1 RODO);

6.9.5.2. żądać, by dane osobowe dotyczące Pacjenta zostały przesłane bezpośrednio innemu Administratorowi (art. 20 ust. 2 RODO).

6.9.6. Przez pojęcie „format nadający się do odczytu maszynowego" należy w szczególności rozumieć powszechnie używane formaty plików[58].

6.9.7. Przez pojęcie danych osobowych dotyczących Pacjenta, które Pacjent dostarczył PWDL należy rozumieć dane aktywnie i świadomie podane PWDL przez Pacjenta, w szczególności zawarte w ankietach i kwestionariuszach oraz dane wygenerowane przez tą osobę (np. login ze stron internetowych).

6.9.8. Żądanie wykonania prawa do przenoszenia danych może być zrealizowane przez PWDL tylko po zweryfikowaniu tożsamości Pacjenta na zasadach określonych w punkcie 6.2. Kodeksu.

6.9.9. Prawo do przenoszenia danych nie może negatywnie wpływać na prawa i wolności innych. Ma to na celu uniknięcie uzyskiwania i przesyłania danych obejmujących dane osobowe innych osób, których dane dotyczą (tych które nie wyraziły zgody) do nowego Administratora w przypadkach, gdy istnieje prawdopodobieństwo, że dane te będą przetwarzane w sposób, który negatywnie wpłynie na prawa i wolności innych osób, których dane dotyczą.

6.10. Prawo Pacjenta do sprzeciwu wobec przetwarzania danych osobowych (art. 21 RODO).

[58] Np. txt, .pdf, .odt .sxw, .doc, .rtf, jpeg, xml, xls

6.10.1. Prawo Pacjenta do sprzeciwu wobec przetwarzania danych osobowych nie znajduje zastosowania wobec danych osobowych przetwarzanych przez PWDL na podstawie art. 9 ust. 2 lit. h RODO, w szczególności wobec danych przetwarzanych w ramach Dokumentacji medycznej i innych przetwarzanych w oparciu o ww. przesłankę.

6.10.2. Prawo Pacjenta do sprzeciwu wobec przetwarzania danych osobowych znajduje zastosowanie tylko i wyłącznie wobec danych osobowych przetwarzanych przez PWDL:

6.10.2.1. w celu wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi (art. 6 ust. 1 lit. e RODO);

6.10.2.2. w oparciu o przesłankę tzw. prawnie uzasadnionych interesów PWDL jako Administratora (art. 6 ust. 1 lit. f RODO).

6.11. Profilowanie

6.11.1. Na gruncie RODO można wyróżnić[59]:

6.11.1.1. profilowanie, które nie skutkuje podejmowaniem decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych wywołujących wobec Pacjentów skutki prawne lub w podobny sposób istotnie na nich wpływających.

6.11.1.2. profilowanie, które skutkuje podejmowaniem decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych wywołujących wobec Pacjentów skutki prawne lub w podobny sposób istotnie na nich wpływa.

6.11.2. Profilowanie wskazane w pkt. 6.11.1.1. jest dopuszczalne bez zgody Pacjenta i może być prowadzone również w oparciu o dane osobowe o stanie zdrowia i inne szczególne kategorie danych osobowych, które wskazano w art. 9 ust. 1 RODO.

6.11.3. W przypadku profilowania wskazanego w pkt 6.11.1.1. realizowanego w celach zdrowotnych zgodnie z pkt. 4.1.2.1. Pacjent nie może wykonać prawa do wniesienia sprzeciwu ze względu na odmienne podstawy przetwarzania danych przez PWDL niż wskazane w art. 21 RODO (por. punkt 6.10.1. Kodeksu dot. sprzeciwu wobec przetwarzania danych osobowych).

---

[59] „profilowanie" oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

6.11.4. Decyzja opierająca się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu wskazanym w pkt. 6.11.1.2. to decyzja, która spełnia następujące cechy:

6.11.4.1. jest podejmowana bez udziału personelu medycznego lub administracyjnego, co oznacza że personel na żadnym etapie procesu nie kontroluje ani nie monitoruje prowadzonych operacji, jak również nie podejmuje ostatecznych rozstrzygnięć wobec Pacjenta oraz;

6.11.4.2. wywołuje wobec Pacjenta skutki prawne, np. w postaci odmowy zawarcia umowy o świadczenie usług medycznych, lub

6.11.4.3. wpływa w inny, istotny sposób na sytuację Pacjenta, np. w sposób pozbawiony realnego wpływu człowieka powoduje odmowę objęcia Pacjenta programem profilaktycznym, skutkuje pozbawieniem Pacjenta możliwości dostępu do świadczenia zdrowotnego lub podjęcie innej decyzji terapeutycznej[60];

6.11.5. W celu uniknięcia wątpliwości, m.in. następujące jednostkowe działania PWDL nie będą zakwalifikowane jako podejmowanie decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych w rozumieniu art. 22 RODO:

6.11.5.1. automatyczne ustalanie wyników skal stosowanych w medycynie[61];

6.11.5.2. ocena wystąpienia mutacji/ ryzyka choroby na podstawie analizy genomu Pacjenta;

6.11.5.3. automatyczne klasyfikowanie wyniku jako „w normie" „ponad normę" i „poniżej normy" na podstawie zdefiniowanych przedziałów wyników (zależnych od czynników wynikających z danych Pacjenta takich jak m.in. płeć czy wiek)[62];

6.11.5.4. wspieranie, za pomocą algorytmów procesu terapeutycznego np. poprzez przedstawienie sugestii badania diagnostycznego, sugestii terapii farmakologicznej i podobnych przez system komputerowy, pod warunkiem, że ostateczną decyzję o sposobie leczenia podejmuje personel medyczny;

---

[60] W świetle powyższej definicji, decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, nie będą pojawiać się często w działalności PWDL. Aby dana operacja przetwarzania danych osobowych mogła zostać uznana za prowadzącą do podejmowania decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych w rozumieniu art. 22 RODO konieczne jest łączne spełnienie warunków wskazanego w lit. (a) oraz jednego z warunków w literze (b) i (c).

[61] np. Skala CHA2DS2–VASc.

[62] np. na potrzeby wykonywania badań diagnostycznych.

6.11.5.5. wspieranie, za pomocą algorytmów komputerowych, procesu selekcji Pacjentów do programów badań profilaktycznych i przesiewowych, pod warunkiem, że ostateczną decyzję o zakwalifikowaniu Pacjentów do udziału w programach podejmuje personel medyczny;

6.11.5.6. wspieranie, za pomocą algorytmów komputerowych, procesu zamawiania przez Pacjentów recept na produkty lecznicze przyjmowane przez dłuższy okres czasu np. poprzez automatyczne informowanie personelu medycznego o konieczności skierowania na wizytę kontrolną Pacjentów, którzy składają zapotrzebowanie na receptę ze względu na upływ określonego czasu od ostatniej wizyty;

6.11.5.7. procesy dotyczące badań profilaktycznych i medycyny pracy, gdzie decyzja o skierowaniu Pacjenta na określone badania opiera się o czynniki charakterystyczne dla danego stanowiska pracy (zdefiniowane przez pracodawcę), a nie czynniki charakterystyczne dla osoby Pacjenta;

6.11.5.8. działanie aplikacji i algorytmów będących wyrobami medycznymi lub częściami wyrobów medycznych, pod warunkiem że wyroby takie zostały dopuszczone do obrotu na terytorium Unii Europejskiej w zgodzie z obowiązującymi przepisami prawa, w zakresie dokonanej certyfikacji.

7. Przyjęcie oraz zmiany Kodeksu, stosowanie Kodeksu

7.1. Komitet sterujący

7.1.1. Zrzeszenia i inne podmioty reprezentujące PWDL oraz Podmioty przetwarzające wskazane w pkt. 1.6. tworzą Komitet sterujący.

7.1.2. Do zadań Komitetu sterującego należy:

7.1.2.1. przygotowanie projektu Kodeksu, zmiany zatwierdzonego Kodeksu lub jego rozszerzenia we współpracy z interesariuszami, w szczególności z podmiotami wskazanymi w pkt. 1.7. Kodeksu;

7.1.2.2. ustalenie podmiotu, który będzie wnioskodawcą występującym o zatwierdzenie tego projektu Kodeksu, zmianę zatwierdzonego Kodeksu lub jego rozszerzenie;

7.1.2.3. przedstawianie Prezesowi Urzędu Ochrony Danych Osobowych opinii w przedmiocie zasadności udzielenia akredytacji podmiotowi ubiegającemu się o akredytację w zakresie monitorowania przestrzegania Kodeksu w oparciu o:

a) wymogi wskazane w art. 41. Ust. 1 i 2 RODO, w tym w szczególności wiedzę fachową w obszarze działalności leczniczej;

b) potencjał techniczny i organizacyjny umożliwiający sprawne prowadzenie procesu monitorowania przestrzegania Kodeksu;

c) cenę usług monitorowania, gwarantującą dostęp do usługi monitorowania PWDL i Podmiotów przetwarzających bez względu na wielkość.

7.1.2.4. Przedstawianie opinii Prezesowi Urzędu Ochrony Danych Osobowych w przedmiocie spełniania, niespełniania, zaprzestania spełniania warunków akredytacji przez Podmiot monitorujący lub jeżeli działania przez niego podejmowane nie są zgodne z RODO, w szczególności w oparciu o skargi i wnioski składane przez Podmioty przestrzegające Kodeksu lub inne osoby składające skargi zgodnie z pkt. 7.4.16.5 Kodeksu.

7.1.2.5. Rozstrzyganie sporów dotyczących stosowania i interpretacji zapisów Kodeksu, w szczególności między Podmiotami monitorującymi, PWDL oraz Podmiotami przetwarzający;

7.1.2.6. Okresowy przegląd stosowania Kodeksu, zgodnie z pkt. 7.5. Kodeksu;

7.1.2.7. Promowanie stosowania Kodeksu oraz podejmowanie innych działań zwiększających poziom ochrony danych osobowych w sektorze medycznym

7.1.2.8. Przyjmowanie bądź odwoływanie nowych członków Komitetu sterującego.

7.1.3. Komitet sterujący podejmuje rozstrzygnięcia w drodze uchwały.

7.1.4. Komitet sterujący przy podejmowaniu rozstrzygnięć, zwłaszcza dotyczących wyboru bądź odwoływania nowych członków Komitetu sterującego działa w drodze konsensusu. W przypadku braku możliwości osiągnięcia konsensusu, rozstrzygnięcia następują w drodze głosowania zwykłą większością głosów członków Komitetu sterującego z zastrzeżeniem pkt. 7.1.6.. Każdy z członków Komitetu sterującego ma jeden głos.

7.1.5. Głosowania Komitetu sterującego mogą być dokonywane na odległość w tym za pomocą środków komunikacji elektronicznej.

7.1.6. W przypadku glosowania w sprawie odwołania członka Komitetu sterującego, głosowanie to realizowane jest na następujących zasadach:

7.1.6.1. ma charakter tajny;

7.1.6.2. w głosowaniu nie uczestniczy członek Komitetu sterującego, który ma zostać odwołany

7.1.6.3. wymaga co najmniej 2/3 głosów wszystkich pozostałych członków Komitetu sterującego

7.1.6.4. głosowanie nie może dotyczyc członka Komitetu, który złożył wniosek o zatwierdzenie Kodeksu zgodnie z pkt. 7.1.2.2.

7.1.6.5. podstawą do dokonania głosowania może być naruszenie przez członka Komitetu sterującego zapisów Kodeksu bądź naruszenie zaufania pozostałych członków Komitetu sterującego, w szczególności poprzez prowadzenie lub promowanie działalności sprzecznej z działalnością Komitetu sterującego.

7.1.7. Komitet sterujący może zlecić wykonanie części swoich zadań lub zadań swoich członków wskazanych w Kodeksie któremuś z członków lub podmiotowi trzeciemu.

7.2. Podmiot monitorujący

7.2.1. Podmiotem monitorującym może być podmiot powołany do tego celu przez Komitet sterujący bądź inny podmiot, który uzyskał pozytywną opinię Komitetu sterującego, o której mowa w pkt. 7.1.2.3. oraz uzyskał akredytację Prezesa Urzędu Ochrony Danych Osobowych, spełniający również wymogi wskazane w art. 41 ust. 1 i 2 RODO.

7.2.2. Może zostać powołany więcej niż jeden Podmiot monitorujący.

7.2.3. Zadania i obowiązki Podmiotu monitorującego.

7.2.4. Do podstawowych zadań i obowiązków Podmiotu monitorującego należy:

7.2.4.1. ocena zdolności PWDL i Podmiotów przetwarzających do stosowania Kodeksu;

7.2.4.2. monitorowanie przestrzegania przepisów Kodeksu;

7.2.4.3. okresowy przegląd funkcjonowania Kodeksu, zgodnie z pkt. 7.5. Kodeksu;

7.2.4.4. rozpatrywanie wniosków i skarg na naruszenie Kodeksu przez PWDL lub Podmiot przetwarzający;

7.2.4.5. rozpatrywanie wniosków i skarg na sposób wdrożenia lub wdrażania Kodeksu przez PWDL lub Podmiot przetwarzający;

7.2.4.6. podejmowanie odpowiednich działań w przypadku naruszenia Kodeksu przez PWDL lub Podmiot przetwarzający, w tym zawieszanie lub wykluczanie PWDL lub Podmiotu przetwarzającego spośród stosujących Kodeks;

7.2.4.7. informowanie UODO o działaniach wymienionych w pkt wskazanych wyżej i powodach ich podjęcia;

7.2.4.8. promowanie stosowania Kodeksu oraz podejmowanie innych działań zwiększających poziom ochrony danych osobowych w sektorze medycznym.

7.2.5. Szczegółowy zakres zadań i obowiązków Podmiotu monitorującego zawarte są w innych punktach Kodeksu, umowach wskazanych w pkt. 7.4.7. Kodeksu oraz w procedurach wskazanych w art. 41 ust. 2 pkt. b i c RODO.

7.2.6. Jeżeli jest to celowe ze względu na ograniczenie kosztów działania Podmiotu monitorującego i przyspieszenie realizowanych przez ten Podmiot działań, Podmiot monitorujący może zlecić na postawie umowy wykonanie części czynności o charakterze techniczno – organizacyjnym związanych z wykonaniem jego zadań podmiotom trzecim, w tym w szczególności członkom Komitetu sterującego.

7.3. Podjęcie się stosowania Kodeksu przez organy i podmioty publiczne w rozumieniu art. 41 ust. 6 RODO

7.3.1. PWDL oraz Podmioty przetwarzające wskazane w pkt. 3.1. będące organami lub podmiotami publicznymi mogą podjąć się stosowania Kodeksu, poprzez złożenie oświadczenia składanego co najmniej w formie elektronicznej, skierowanego do Komitetu sterującego, zgodnie z którym PWDL lub Podmiot przetwarzający oświadczają, że spełniają wymogi wnikające z Kodeksu.

7.3.2. Oświadczenie, o którym mowa w punkcie poprzednim zawiera:

7.3.2.1. kwestionariusz odnoszący się do poszczególnych obowiązków wynikających z Kodeksu;

7.3.2.2. w przypadku PWDL, wskazanie, czy oświadczenie dotyczy całego PWDL, czy też wybranego bądź wybranych zakładów leczniczych ze wskazaniem tych zakładów;

7.3.2.3. Pozytywną opinię wydaną przez Inspektora Ochrony Danych (jeśli został powołany) lub inny podmiot dysponujący odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem Kodeksu, stwierdzającą spełnianie przez PWDL lub Podmiot przetwarzający wymogów Kodeksu.

7.3.3. Wzór oświadczenia stanowi załącznik nr 8 do Kodeksu, wzór kwestionariusza stanowi załącznik nr 10 do Kodeksu.

7.3.4. Kwestionariusz określa zakres wymogów nałożonych przez Kodeks na PWDL oraz Podmioty przetwarzające.

7.3.5. W przypadku braku sprzeciwu ze strony któregokolwiek z członków Komitetu sterującego złożonego w terminie 21 dni, PWDL lub Podmiot przetwarzający uzyskują status Podmiotu przestrzegającego Kodeksu.

7.3.6. W przypadku złożenia umotywowanego sprzeciwu przez jednego z członków Komitetu sterującego przed upływem 21 dni od dnia dokonania zgłoszenia, Komitet sterujący w terminie 7 dni przeprowadza głosowanie co do zasadności przyznania statusu Podmiotu przestrzegającego Kodeksu i niezwłocznie przekazuje PWDL lub Podmiotowi przetwarzającemu wynik głosowania.

7.3.7. Do przesłanek uzasadniających złożenie sprzeciwu przez członka Komitetu i jego przyjęcie przez Komitet sterujący należy w szczególności:

7.3.7.1. podejrzenie lub stwierdzenie podania nieprawdziwych lub niekompletnych informacji w oświadczeniu złożonym przez PWDL lub Podmiot monitorujący;

7.3.7.2. wątpliwości co do zdolności przestrzegania postanowień Kodeksu przez PWDL lub Podmiot przetwarzający;

7.3.7.3. wątpliwości co do wiedzy fachowej podmiotu wskazanego w pkt. 7.3.2.3.

7.3.8. Podmiot przestrzegający Kodeksu podaje do wiadomości publicznej[63]:

7.3.8.1. Informację o uzyskaniu statusu Podmiotu przestrzegającego Kodeksu;

7.3.8.2. Treść oświadczenia wraz z informacjami wskazanymi w pkt. 7.3.3. z wyłączeniem informacji których ujawnienie może stanowić naruszenie tajemnicy przedsiębiorstwa lub stwarza ryzyko naruszenia ochrony danych osobowych;

7.3.8.3. Informację o możliwości złożenia skargi na naruszenie Kodeksu na Podmiot przestrzegający Kodeksu;

7.3.8.4. Informację o utracie statusu Podmiotu przestrzegającego Kodeksu.

7.3.9. Komitet sterujący podaje do publicznej wiadomości informacje wskazane w punkcie 7.3.8.

7.3.10. Podmiot przestrzegający Kodeksu informuje Komitet sterujący bez zwłoki, lecz nie później niż w terminie 7 dni o decyzjach Prezesa Urzędu Ochrony Danych Osobowych w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych w rozumieniu rozdziału 7 Ustawy o ochronie danych osobowych, a także o zmianie danych identyfikujących Podmiotu przestrzegającego Kodeksu podanych w oświadczeniu o którym mowa w pkt. 7.3.1., jak również o istotnych dla ochrony danych osobowych zmianach stanu faktycznego opisanych w załącznikach do oświadczenia z dodatkową opinią dotyczącą tych zmian wydana przez podmiot o którym mowa w pkt. 7.3.2.4.

---

[63]Przewiduje się ustanowienie rejestru umieszczonego na dedykowanej stronie internetowej zawierającego wskazane informacje – rejestr będzie dotyczył podmiotów publicznych i niepublicznych.

7.3.11. PWDL lub Podmiot przetwarzający mogą w każdym czasie zostać pozbawione statusu Podmiotów przestrzegających Kodeksu w odniesieniu do całości lub części zakresu wskazanego w pkt. 7.3.3.2. Kodeksu w następujących sytuacjach:

7.3.11.1. zmiany stanu faktycznego wskazanego w oświadczeniu, o którym mowa w pkt. 7.3.1.;

7.3.11.2. niewywiązywaniu się przez Podmiot przestrzegający Kodeksu ze zobowiązań wynikających z Kodeksu, w szczególności w związku z wydaniem decyzji wskazanej w pkt.7.3.10. lub otrzymaniem skarg na naruszenie Kodeksu przez Podmiot przestrzegający Kodeksu, a także w związku z nieprzestrzeganiem umowy o której mowa w pkt.7.3.15.1. lub nieregulowania zobowiązań finansowych wskazanych w pkt. 7.3.15.3.

7.3.12. Pozbawienie statusu Podmiotu przestrzegającego Kodeksu następuje na wniosek członka Komitetu sterującego. Wniosek powinien wskazywać uzasadnienie pozbawienia statusu Podmiotu przestrzegającego Kodeksu wraz z prezentacją dowodów potwierdzających okoliczności uzasadniające pozbawianie statusu.

7.3.13. Komitet sterujący w terminie 7 dni przeprowadza głosowanie co do:

7.3.13.1. zasadności pozbawienia statusu Podmiotu przestrzegającego Kodeksu bądź;

7.3.13.2. wezwania Podmiotu przestrzegającego Kodeksu do usunięcia naruszeń lub wskazania dodatkowych wyjaśnień wraz z wyznaczeniem terminu na usunięcie naruszeń lub przedstawienie dodatkowych wyjaśnień;

7.3.13.3. Po upływie terminu wskazanego w pkt. 7.3.13.2. Komitet sterujący przeprowadza głosowanie zgodnie z pkt. 7.3.13.1.;

7.3.13.4. Komitet sterujący niezwłocznie przekazuje PWDL lub Podmiotowi przetwarzającemu wynik głosowania.

7.3.14. PWDL oraz Podmioty przetwarzające niezwłocznie po potrzymaniu informacji o pozbawieniu statusu Podmiotu przestrzegającego Kodeks, dokonują stosownej zmiany informacji wskazanych w pkt. 7.3.8.

7.3.15. Komitet sterujący może przyjąć dodatkowe zasady dotyczące podjęcia się stosowania Kodeksu przez organy lub podmioty publiczne, dotyczące w szczególności:

7.3.15.1. wzoru i trybu zawarcia umowy zawieranej przez PWDL lub Podmiot przetwarzający z członkiem Komitetu sterującego lub podmiotem trzecim wyznaczonym przez Komitet sterujący, której zawarcie stanowić może warunek otrzymania statusu Podmiotu przestrzegającego Kodeksu;

7.3.15.2. ustalenia oznaczenia słownego lub graficznego statusu Podmiotu przestrzegającego Kodeksu;

7.3.15.3. ustalenia opłaty za uzyskanie statusu Podmiotu przestrzegającego Kodeksu, przy czym opłata ta za rok nie może przekroczyć ogłaszanej przez GUS wartości przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku za ostatni kwartał roku po którym ustalana jest opłata. Przychody z opłat mogą być wykorzystane na pokrycie kosztów administracyjnych oraz na promowanie Kodeksu i przestrzegania danych osobowych;

7.3.15.4. ustalenia trybu zgłaszania skarg, o którym mowa w pkt. 7.3.8.3. oraz ustalenia szczegółowych zasad składania i publikowania oświadczeń złożonych przez PWDL lub Podmioty przetwarzające ubiegające się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu, w szczególności przy wykorzystaniu dedykowanego systemu teleinformatycznego;

7.3.15.5. ustalenia szczegółowych zasad składania oświadczenia, o którym mowa w pkt. 7.3.1. Kodeksu.

7.4. Podjęcie się stosowania Kodeksu przez PWDL oraz Podmioty przetwarzające inne, niż organy i podmioty publiczne w rozumieniu art. 41 ust. 6 RODO

7.4.1. PWDL oraz Podmioty przetwarzające wskazane w pkt. 3.1. niebędące organami lub podmiotami publicznymi mogą podjąć się stosowania Kodeksu, poprzez złożenie wniosku składanego co najmniej w formie elektronicznej skierowanego do Podmiotu monitorującego.

7.4.2. Wniosek, o którym mowa w punkcie poprzednim zawiera:

7.4.2.1. kwestionariusz odnoszący się do poszczególnych obowiązków wynikających z Kodeksu;

7.4.2.2. w przypadku PWDL, wskazanie, czy wniosek dotyczy całego PWDL, czy też wybranego bądź wybranych zakładów leczniczych, ze wskazaniem tych zakładów;

7.4.2.3. fakultatywnie: pozytywną opinię wydaną przez Inspektora Ochrony Danych (jeśli został powołany) lub inny podmiot dysponujący odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem Kodeksu, stwierdzającą spełnianie przez PWDL lub Podmiot przetwarzający wymogów Kodeksu.

7.4.3. Wzór wniosku stanowi załącznik nr 9 do Kodeksu, wzór kwestionariusza stanowi załącznik nr 10 do Kodeksu.

7.4.4. Kwestionariusz określa zakres wymogów nałożonych przez Kodeks na PWDL oraz Podmioty przetwarzające.

7.4.5. Warunkiem uzyskania statusu Podmiotu przestrzegającego Kodeksu jest poddanie się audytowi wstępnemu przeprowadzonemu przez Podmiot monitorujący i uzyskanie pozytywnej oceny zdolności PWDL lub Podmiotu przetwarzającego do stosowania zapisów Kodeksu.

7.4.6. Metodyka przeprowadzania audytu wstępnego określona jest w sposób wskazany w pkt. 7.2.5., przy czym powinna ona uwzględniać co najmniej ocenę spełnienia poszczególnych obowiązków wynikających z Kodeksu, których zakres wskazany został w kwestionariuszu, o którym mowa w pkt. 7.4.2.1. Kodeksu.

7.4.7. Metodyka przeprowadzania audytu wstępnego uwzględnia w szczególności specyfikę funkcjonowania niewielkich PWDL, które nie przetwarzają na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, RODO, w tym poprzez zapewnienie racjonalizacji kosztów przeprowadzenia audytu wstępnego w przypadku tych podmiotów.

7.4.8. Audyt wstępny, a także dalsze monitorowanie przestrzegania zapisów Kodeksu realizowany jest na podstawie umowy zawartej między Podmiotem monitorującym, a:

7.4.8.1. Samorządami zawodowymi – w odniesieniu do PWDL w formie praktyk zawodowych prowadzonych przez zrzeszone w ramach tych samorządów osoby;

7.4.8.2. Członkami Komitetu sterującego – w odniesieniu do PWDL lub Podmiotów przetwarzających będących ich członkami;

7.4.8.3. Bezpośrednio PWDL lub Podmiotami przetwarzającymi, ubiegającymi się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu.

7.4.9. Audyt wstępny przeprowadzany jest niezwłocznie. W przypadku złożenia przez PWDL lub Podmiot przetwarzający wniosku zawierającego pozytywną opinię o której mowa w pkt. 7.4.2.3., podmiot ten do czasu przeprowadzenia audytu wstępnego uzyskuje tymczasowo status Podmiotu przestrzegającego Kodeksu – przepisy pkt. 7.3. w tym okresie stosuje się odpowiednio, przy czym tymczasowy status Podmiotu przestrzegającego Kodeksu nie może trwać dłużej, niż 24 miesiące od dnia złożenia wniosku.

7.4.10. Podmiot monitorujący niezwłocznie informuje PWDL lub Podmiot przetwarzający, a także Komitet sterujący o wynikach audytu wstępnego. W przypadku pozytywnego wyniku audytu wstępnego Podmiot monitorujący wydaje stosowne zaświadczenie. W przypadku negatywnego wyniku audytu wstępnego, Podmiot monitorujący wydaje zalecenia dla PWDL lub Podmiotu przetwarzającego. PWDL lub Podmiot przetwarzający może zostać ponownie poddany audytowi po upływie co najmniej 31 dni od przekazania zaleceń. PWDL lub Podmiot przetwarzający mogą skrócić wskazany termin i wystąpić o wcześniejsze przeprowadzenie audytu.

7.4.11. Podmiot przestrzegający Kodeksu, Podmiot monitorujący, a także Komitet sterujący podają do publicznej wiadomości informacje:

7.4.11.1. informację o uzyskaniu statusu Podmiotu przestrzegającego Kodeksu oraz treść zaświadczenia wskazanego w pkt. 7.4.11.;

7.4.11.2. treść wniosku z pkt. 7.4.1. wraz z towarzyszącymi mu infomacjami, z wyłączeniem informacji których ujawnienie może stanowić naruszenie tajemnicy przedsiębiorstwa lub stwarza ryzyko naruszenia ochrony danych osobowych;

7.4.11.3. informację o możliwości złożenia i zasadach rozpatrywania wniosku lub skargi na naruszenie Kodeksu przez Podmiot przestrzegający Kodeksu w sposób wskazany przez Podmiot monitorujący zgodnie z pkt. 7.4.16.;

7.4.11.4. informację o utracie statusu Podmiotu przestrzegającego Kodeksu.

7.4.12. Podmiot przestrzegający Kodeksu informuje Komitet sterujący oraz Podmiot monitorujący bez zwłoki, nie później niż w terminie 7 dni, o decyzjach Prezesa Urzędu Ochrony Danych Osobowych w postępowaniu w sprawie naruszenia przepisów o ochronie danych osobowych w rozumieniu rozdziału 7 Ustawy o ochronie danych osobowych, a także o zmianie danych identyfikujących Podmiot przestrzegający Kodeksu podanych we wniosku o którym mowa w pkt. 7.4.1., jak również o istotnych dla ochrony danych osobowych zmianach stanu faktycznego opisanych w załącznikach do wniosku.

7.4.13. Podmiot monitorujący prowadzi obowiązkowe monitorowanie przestrzegania przepisów Kodeksu przez Podmioty przestrzegające Kodeksu.

7.4.14. Szczegółowe zasady prowadzenia monitorowania przestrzegania przepisów Kodeksu określa Podmiot monitorujący w sposób wskazany w pkt. 7.2.5., przy czym obejmują one co najmniej następujące postanowienia:

7.4.14.1. wykonywanie czynności sprawdzających w sposób cykliczny, nie rzadziej, niż raz do roku;

7.4.14.2. wykonywanie czynności sprawdzających w związku z uzyskaniem uprawdopodobnionej informacji, co do naruszenia zasad przestrzegania Kodeksu przez Podmiot przestrzegający Kodeksu;

7.4.14.3. wykonywanie czynności sprawdzających przez osobę posiadającą imienne upoważnienie, której przysługują uprawnienia analogiczne do wskazanych w art. 25 ust. 1 i 2 ustawy o ochronie danych osobowych.

7.4.15. W ramach monitorowania przestrzegania przepisów Kodeksu oraz okresowego przeglądu funkcjonowania Kodeksu, Podmiot monitorujący zbiera wnioski oraz skargi na naruszenie Kodeksu lub na sposób wdrożenia lub wdrażania Kodeksu przez Podmiot przestrzegający Kodeksu. Szczegółową procedurę zbierania i rozpatrywania skarg i wniosków określa Podmiot monitorujący w sposób wskazany w pkt. 7.2.5., przy czym, procedura ta:

7.4.15.1. musi być prosta i przejrzysta;

7.4.15.2. musi zapewnić sprawne rozpatrywanie skarg i wniosków z podaniem maksymalnego czasu odpowiedzi na skargę lub wniosek, nie dłuższy jednak niż miesiąc. Termin na rozpatrzenie skargi lub odpowiedzi na wniosek może ulec wydłużeniu o kolejne 2 miesiące ze względu na skomplikowany charakter skargi lub wniosku lub liczbę skarg lub wniosków, o czym Podmiot monitorujący informuje osobę składającą skargę lub wniosek, z podaniem przyczyny opóźnienia;

7.4.15.3. powinna zawierać możliwość składania skarg i wniosków w formie elektronicznej, telefonicznej, na piśmie i ustnie w siedzibie Podmiotu monitorującego bez konieczności dopełnienia szczególnej formy;

7.4.15.4. nie może przewidywać pobierania opłat od osoby składającej skargę lub wniosek;

7.4.15.5. zawiera informację o możliwości złożeniu skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz Komitetu sterującego na działania bądź zaniechania Podmiotu monitorującego.

7.4.16. W przypadku ustalenia wysokiego prawdopodobieństwa naruszenia przepisów Kodeksu bądź stwierdzenia naruszania przepisów Kodeksu przez Podmiot przestrzegający Kodeksu, Podmiot monitorujący, który aktualnie monitoruje przestrzeganie stosowania Kodeksu w tym Podmiocie, przekazuje Podmiotowi przestrzegającemu Kodeksu informację o możliwych lub stwierdzonych naruszeniach, w tym ze wskazaniem wagi naruszenia, z wyznaczeniem terminu 14 dni na ustosunkowanie się do informacji a także ewentualnie na podjęcie działań zaradczych, a następnie po przeanalizowaniu odpowiedzi przesłanej przez Podmiot przestrzegający Kodeksu oraz podjętych działań zaradczych może:

7.4.16.1. zawiesić posiadanie statusu Podmiotu przestrzegającego Kodeksu, z jednoczesnym wskazaniem naruszeń i terminu usunięcia naruszeń – w przypadkach naruszeń mniejszej wagi. Termin na usunięcie naruszeń nie może być dłuższy, niż 14 dni;

7.4.16.2. pozbawić PWDL lub Podmiot przetwarzający statusu Podmiotu przestrzegającego Kodeksu z jednoczesnym wskazaniem naruszeń – w przypadkach istotniejszych naruszeń lub w przypadku nieusunięcia przez PWDL lub Podmiot przetwarzający w wymaganym terminie naruszeń wskazanych w pkt. 7.4.16.1.;

7.4.16.3. zawieszenie posiadania statusu lub pozbawienie posiadania statusu podmiotu przestrzegającego Kodeksu może dotyczyć w całości lub części zakresu wskazanego w pkt. 7.4.2.2. Kodeksu.

7.4.17. Informacja o działaniach podjętych zgodnie z pkt. 7.4.16. przekazywana jest Komitetowi sterującemu bez zbędnej zwłoki.

7.4.18. Informacja o zawieszeniu wskazana w pkt. 7.4.16.1. nie jest podawana do wiadomości publicznej.

7.4.19. Podmiot monitorujący, Komitet sterujący, PWDL oraz Podmiot przetwarzający niezwłocznie po potrzymaniu informacji o pozbawieniu statusu Podmiotu przestrzegającego Kodeks, dokonują stosownej zmiany informacji wskazanych w pkt. 7.4.11.

7.4.20. Komitet sterujący może przyjąć dodatkowe zasady dotyczące podjęcia się stosowania Kodeksu przez PWDL lub Podmioty przetwarzające, inne niż organy lub podmioty publiczne w rozumieniu art. 41 ust. 7 RODO, dotyczące w szczególności:

7.4.20.1. wzoru i trybu zawarcia umów wskazanych w pkt. 7.4.9. Kodeksu;

7.4.20.2. ustalenia oznaczenia słownego iub graficznego statusu Podmiotu przestrzegającego Kodeksu oraz wzoru zaświadczenia, o którym mowa w pkt. 7.4.11.;

7.4.20.3. ustalenia trybu zgłaszania skargi na działanie Podmiotu monitorującego w szczególności przy wykorzystaniu dedykowanego systemu teleinformatycznego;

7.4.20.4. ustalenia szczegółowych zasad składania i publikowania wniosków złożonych przez PWDL lub Podmioty przetwarzające ubiegające się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu, informacji o uzyskaniu zaświadczenia, o którym mowa w pkt. 7.4.11. oraz innych informacji w szczególności przy wykorzystaniu dedykowanego systemu teleinformatycznego;

7.4.20.5. pokrywania kosztów administracyjnych funkcjonowania Komitetu sterującego, przy czym nie mogą być one wyższe niż wysokość oplaty określonej pkt. 7.3.14.3 Kodeksu, dodatkowo koszty powinny być uzależnione od rodzaju i wielkości PWDL lub Podmiotu przetwarzającego.

7.5. Współpraca na rzecz okresowego przeglądu stosowania Kodeksu

7.5.1. Okresowy przegląd stosowania Kodeksu dokonywany jest przez Komitet sterujący oraz Podmioty monitorujące.

7.5.2. Przegląd stosowania Kodeksu polega w szczególności na analizie jego stosowania w praktyce, a także na bieżącej analizie otoczenia regulacyjnego, w celu ustalenia konieczności dokonania ewentualnej zmiany lub rozszerzenia Kodeksu.

7.5.3. W ramach okresowego przeglądu stosowania Kodeksu Podmioty monitorujące przekazują Komitetowi sterującemu oraz Prezesowi Urzędu Ochrony Danych osobowych informacje dotyczące stosowania Kodeksu:

7.5.3.1. nie rzadziej niż, co 2 miesiące oraz;

7.5.3.2. na każde żądanie Komitetu sterującego lub Prezesa Urzędu Ochrony Danych Osobowych.

7.5.4. Komitet sterujący oraz Podmioty monitorujące zapewniają udział innych interesariuszy w procesie przeglądu stosowania Kodeksu, w szczególności:

7.5.4.1. PWDL oraz Podmiotów przetwarzających;

7.5.4.2. Podmiotów wskazanych w pkt. 1.7. Kodeksu;

7.5.4.3. Pacjentów i organizacji zrzeszających Pacjentów;

7.5.4.4. Podmiotów z sektora administracji publicznej;

7.5.5. Udział innych interesariuszy wymienionych w punkcie poprzednim odbywać się może m.in. poprzez:

7.5.5.1. udostępnienie systemu teleinformatycznego do zgłaszania uwag i wymiany doświadczeń związanych ze stosowaniem Kodeksu;

7.5.5.2. organizowanie wydarzeń poświęconych stosowaniu Kodeksu.

7.5.6. Komitet sterujący nie rzadziej niż raz na 6 miesięcy dokonuje oceny zasadności złożenia do Prezesa Urzędu Ochrony Danych Osobowych wniosku o zmianę lub rozszerzenie Kodeksu.

7.5.7. Informacje wskazane w pkt. 7.5.3., wnioski i propozycje uzyskane od podmiotów wskazanych w pkt. 7.5.4., informacje o aktywnościach podejmowanych zgodnie z pkt. 7.5.5. oraz ocena dokonana zgodnie z pkt. 7.5.6. podawane są do wiadomości publicznej przez Komitet sterujący.

7.6. Zapobieganie konfliktom interesów

7.6.1. Podmiot monitorujący jest zobowiązany zapewnić zachowanie niezależności i bezstronności w realizacji zadań i obowiązków.

7.6.2. Do osoby wykonującej zadania i obowiązki w imieniu lub z upoważnienia Podmiotu monitorującego stosuje się odpowiednio przepisy Kodeksu postępowania administracyjnego dotyczące wyłączenia pracownika.

7.6.3. Osoba, o której mowa w punkcie poprzednim może być wyłączona również w przypadku stwierdzenia innych przyczyn, które mogłyby wywołać wątpliwości co do jej bezstronności.

7.6.4. Komitet sterujący w ramach współpracy z Podmiotem monitorującym nie podejmuje działań stwarzających ryzyko konfliktu interesów, w szczególności:

7.6.4.1. nie wydaje Podmiotowi monitorującemu wiążących poleceń;

7.6.4.2. opinia udzielona przez Komitet sterujący, o której mowa w pkt. 7.1.2.3. i 71.2.4. może być oparta wyłącznie na merytorycznych przesłankach.

7.7. Stosowanie Kodeksu w przypadku braku Podmiotu monitorującego

7.7.1. Przed powołaniem Podmiotu monitorującego w odniesieniu do PWDL oraz Podmiotów przetwarzających innych, niż organy i podmioty publiczne w rozumieniu art. 41 ust. 7 RODO, przepisy pkt. 7.3. Kodeksu stosuje się odpowiednio.

7.7.2. W przypadku powołania Podmiotu monitorującego, Podmioty o których mowa w pkt. 7.7.1. utrzymują status Podmiotów przestrzegających Kodeksu w oparciu o przepisy pkt. 7.3. nie dłużej niż do dnia uzyskania informacji, o której mowa w pkt. 7.4.11., jednak nie dłuzej niż w terminie 24 miesięcy od dnia uzyskania przez Podmiot monitorujący certyfikatu akredytacyjnego, o którym mowa w art. 31 ustawy o ochronie danych osobowych.

7.7.3. W przypadku cofnięcia akredytacji Podmiotu monitorującego, a następnie powołania nowego Podmiotu monitorującego przepisy pkt. 7.7.1. oraz 7.7.2. stosuje się odpowiednio.

8. Spis załączników

1. Załącznik nr 1: Wzór zgody na przetwarzanie danych osobowych.
2. Załącznik nr 2: Katalog danych jednoznacznie identyfikujących daną osobę wraz ze wskazaniem przykładowego wzoru upoważnienia z art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, które spełnia wymogi prawa.
3. Załącznik nr 3: Zasady postępowania w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych.
4. Załącznik nr 4: Przykładowa procedura analizy ryzyka, której wdrożenie i stosowanie zapewnia realizację podejścia opartego na ryzyku.
5. Załącznik nr 5: Wykaz zabezpieczeń systemów IT.
6. Załącznik nr 6: Wykaz norm mających zastosowanie w obszarze bezpieczeństwa informacji i ochrony danych osobowych.
7. Załącznik nr 7: Rekomendacje w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania danych w Podmiotach wykonujących działalność leczniczą w których przetwarzanie danych nie jest uznane za przetwarzanie na dużą skalę.
8. Załącznik nr 8: Wzór oświadczenia o spełnieniu wymogów wynikających z Kodeksu.
9. Załącznik nr 9: Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu.
10. Załącznik nr 10: Wzór kwestionariusza, który dołącza się do oświadczenia, o którym mowa w załączniku nr 8 lub wniosku, o którym mowa w załączniku nr 9.

Załącznik nr 1

8.1. Wzór zgody na przetwarzanie danych osobowych

Ja, niżej podpisany [____][64], wyrażam zgodę na przetwarzanie moich danych osobowych [____][65] w celu [____][66] przez Administratora, tj. [____][67].

_____

Podpis i data[68]

W przypadku kilku celów, należy pobierać zgodę osobno dla każdego z celów, rekomendujemy ich umieszczenie w osobnych checkboxach, zgodnie z poniższym wzorem:

Ja, niżej podpisany [____][69], wyrażam zgodę na przetwarzanie moich danych osobowych w celach:

- ☐ [*cel nr 1*], zakres danych [____][70]
- ☐ [*cel nr 2*], zakres danych [____][71]

przez Administratora, tj. [____][72].

_____

Podpis i data[73]

W CELU ZAPEWNIENA, ŻE ZGODA UDZIELANA JEST W SPOSÓB ŚWIADOMY, NALEŻY PRZED JEJ UDZIELENIEM PRZEKAZAĆ PACJENTOWI TREŚĆ OBOWIĄZKU INFORMACYJNEGO O KTÓRYM MOWA W ART. 13 RODO.

---

[64]Imię i nazwisko osoby udzielającej zgody, a także dodatkowe informacje pozwalające na jednoznaczne ustalenie tożsamości osoby: rekomendujemy datę urodzenia lub PESEL lub adres miejsca zamieszkania.

[65]Do uzupełnienia kategorie danych osobowych, które będą przetwarzane w oparciu o zgodę. Można wskazać kategorie bezpośrednio (np. imię, nazwisko, adres email) lub w przypadku, w którym zgoda umieszczana jest pod formularzem zawierającym dane osobowe można dodać wzmiankę: „zawartych w niniejszym formularzu".

[66]W tym miejscu konieczne jest zaznaczenie w sposób precyzyjny celu, w którym dane osobowe mają być przetwarzane (np. w celu marketingowym, w celu wysyłania newslettera, w celu zapraszania na wydarzenia promocyjne).

[67]W tym miejscu należy podać nazwę Administratora danych osobowych oraz jego adres.

[68]Podpis osoby udzielającej zgody.

[69]Imię i nazwisko osoby udzielającej zgody a także dodatkowe informacje pozwalające na jednoznaczne ustalenie tożsamości osoby: rekomendujemy PESEL lub serię i numer dowodu tożsamości.

[70]Do uzupełnienia kategorie danych osobowych, które będą przetwarzane w oparciu o zgodę. Można wskazać kategorie bezpośrednio (np. imię, nazwisko, adres email) lub w przypadku, w którym zgoda umieszczana jest pod formularzem zawierającym dane osobowe można dodać wzmiankę: „zawartych w niniejszym formularzu".

[71]J.w.

[72]W tym miejscu należy podać nazwę Administratora danych osobowych oraz jego adres.

[73]Podpis osoby udzielającej zgody.

Załącznik nr 2

8.2. Katalog danych jednoznacznie identyfikujących daną osobę wraz ze wskazaniem przykładowego wzoru upoważenia z art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, które spełnia wymogi prawa

PRZYKŁADOWY ZAKRES DANYCH, CO DO KTÓRYCH PRZYJMUJE SIĘ ŻE JEDNOZNACZNIE IDENTYFIKUJĄ PACJENTA

Zakres danych wynikający z art. 25 ust. 1 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (z wyłączeniem danych o płci):

1) nazwisko i imię (imiona);
2) data urodzenia (fakultatywnie, choć rekomendowane zbieranie w przypadku osób nieposiadających nr PESEL);
3) adres miejsca zamieszkania;
4) 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.

W przypadku gdy Pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody, dodatkowo należy wskazać dane Przedstawiciela ustawowego:

1) nazwisko i imię (imiona);
2) adres jego miejsca zamieszkania;
3) *Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne ale zalecane):PESEL, seria i numer dowodu tożsamości.*

PRZYKŁADOWY ZAKRES DANYCH IDENTYFIKUJĄCYCH OSOBĘ UPOWAŻNIONĄ, CO DO KTÓREJ PRZYJMUJE SIĘ ŻE JEDNOZNACZNIE IDENTYFUKUJĄ WSKAZANĄ OSOBĘ

Zgodnie z §8 ust. 1 Rozporządzenia w sprawie rodzajów, zakresu i wzorów Dokumentacji medycznej oraz sposobu jej przetwarzania niezbędnymi danymi osoby upoważnionej, które muszą zostać podane jest imię i nazwisko.

Dodatkowo rekomenduje się zebranie, o ile Pacjent posiada takowe informacje, dodatkowych danych osoby upoważnionej, które pozwolą na jej jednoznaczną identyfikację ze względu na to, że imię i nazwisko zazwyczaj nie pozwalają na jednoznaczną identyfikację danej osoby. Pozyskanie tych danych przez Administratora danych jest adekwatne dla celów

przetwarzania. Nie można jednak uzależnić możliwości złożenia upoważnienia od podania dodatkowych informacji o osobie upoważnionej wykraczających poza imię i nazwisko.

Przykładowy zakres danych pozwalających na jednoznaczną identyfikację osoby upoważnionej:

1) numer PESEL;
2) numer dokumentu tożsamości (dowodu osobistego, paszportu, prawa jazdy legitymacji szkolnej.

PRZYKŁADOWA TREŚĆ OŚWIADCZEŃ ZGODNA Z PRZEPISAMI PRAWA

Imię osoby upoważnionej:*
Nazwisko osoby upoważnionej:*
Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne, ale zalecane)
Działając na podstawie art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta w związku z §8 ust. 1 Rozporządzenia w sprawie rodzajów, zakresu i wzorów Dokumentacji medycznej oraz sposobu jej przetwarzania:

JEŻELI UPOWAŻNIA PACJENT

□ *upoważniam wyżej wymienioną osobę*
□ *nie upoważniam nikogo*

do dostępu do mojej Dokumentacji medycznej:

a) w pełnym zakresie/ w zakresie ograniczonym do.....
b) wyłącznie w [nazwa PWDL] / w [PWDL] oraz w innych podmiotach wykonujących działalność leczniczą.

Imię Pacjenta
Nazwisko:
PESEL:
Data złożenia oświadczenia:.....

Imię osoby upoważnionej:*
Nazwisko osoby upoważnionej:*
Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne, ale zalecane):

JEŻELI UPOWAŻNIA PRZEDSTAWICIEL USTAWOWY

Działając jako Przedstawiciel ustawowy, na mocy art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta:

□ *upoważniam wyżej wymienioną osobę*
□ *nie upoważniam nikogo*

do dostępu do Dokumentacji medycznej dotyczącej pacjenta pozostającego pod moją opieką:

Imię Pacjenta
Nazwisko:
PESEL:

W pełnym zakresie/ w zakresie ograniczony do.....
Wyłącznie w [nazwa PWDL] / w [PWLD] oraz w innych podmiotach wykonujących działalność leczniczą.

nazwisko i imię (imiona) Przedstawiciela ustawowego:*
miejsca zamieszkania Przedstawiciela ustawowego:*
Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne, ale zalecane):PESEL, seria i numer dowodu tożsamości Przedstawiciela ustawowego.

Data złożenia oświadczenia:.....

Załącznik nr 3

8.3. Zasady postępowania w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych

Pytanie	Odpowiedź
W jaki sposób zapewnić anonimowość Pacjentów w trakcie rejestracji przed wizytą lekarską?	Dążyć należy do minimalizacji ryzyka ujawnienia informacji osobom postronnym, w szczególności danych o stanie zdrowia, z uwzględnieniem konkretnych uwarunkowań technicznych. Zastosowane rozwiązania nie mogą jednak w żadnym zakresie zakłócać udzielania świadczeń opieki zdrowotnej, ani narażać zdrowia lub życia Pacjentów. Należy również pamiętać, że podmiot leczniczy ma obowiązek i prawo ustalenia tożsamości osoby ubiegającej się o świadczenie. Możliwe sposoby dokonania rejestracji Pacjenta w podmiocie leczniczym z potwierdzeniem tożsamości: 1. W podmiocie powinno zostać wyznaczone miejsce do realizacji procesu rejestracji, oznaczenia miejsca powinny w wyraźny sposób wskazywać obszar, w którym może znajdować się wyłącznie obsługiwany Pacjent oraz ewentualnie osoba towarzysząca, Przedstawiciel ustawowy, opiekun faktyczny lub członek rodziny, Osoba bliska. Pozostałe osoby przebywające w podmiocie leczniczym (inni Pacjenci osoby towarzyszące tym Pacjentom) powinny pozostawać poza tym obszarem. Powyższe zrealizować można poprzez przyjęcie wybranych z poniższej listy przykładowych rozwiązań: a) naklejenie na podłodze przed stanowiskiem rejestracji taśmy w jaskrawych barwach wyznaczając obszar, w którym przebywa tylko osoba obsługiwane przez rejestrację; b) zamieszczenie komunikatu o konieczności przebywania przy jednym stanowisku recepcyjnym tylko jednego Pacjenta; c) oddzielenie strefy rejestracji ścianką, płytą plexi, szybą - w strefie pojedyncze miejsce siedzące lub stojące, osoby nieuprawnione pozostają poza barierą fizyczną; d) oddzielenie strefy rejestracji barierką - osoby nieuprawnione pozostają poza strefą rejestracji za barierką; e) wprowadzenie odpowiedniej odległości między

	stanowiskami; f) wprowadzenie stref rejestracji w osobnym pomieszczeniu poza korytarzem/miejscem dla oczekujących; g) wprowadzenie możliwości rejestracji elektronicznej/ telefonicznej; h) możliwe wyznaczenie odrębnego od recepcji głównej odizolowanego stanowiska do rejestracji telefonicznej, w ramach której czasami dochodzi do odczytywania danych osobowych. 2. Weryfikacja tożsamości Pacjenta powinna odbywać się w sposób nieutrudniający dostępu do uzyskania świadczenia zdrowotnego z ograniczeniem ryzyka uzyskania danych osobowych przez osobę trzecią. Powyższe zrealizować można poprzez zastosowanie poniższych przykładowych środków: a) osoba rejestrująca prosi Pacjenta o okazanie dokumentu weryfikującego tożsamość; b) jeżeli Pacjent odmawia okazania dokumentu weryfikującego tożsamość można poprosić go o podanie danych identyfikacyjnych tj. PESEL lub inny numer identyfikacji wskazany w przepisach prawa - ustnie lub w sposób wskazany w pkt. c; c) możliwe jest zastosowanie kartek/formularzy, na których Pacjent wpisuje wymagane dane identyfikacyjne. Kartki muszą być zniszczone niezwłocznie po wykorzystaniu (wprowadzeniu danych do systemu rejestracyjnego), w sposób uniemożliwiający odtworzenie zapisanej treści. Jeżeli nie ma możliwości ich natychmiastowego zniszczenia należy odkładać w bezpiecznym miejscu i niszczyć niezwłocznie po zakończeniu pracy; d) jeżeli Pacjent dobrowolnie bez wezwania okazuje dokument weryfikujący tożsamość lub przekazuje ustnie informacje, umożliwiające ustalenie tożsamości nie należy odmawiać przyjęcia dobrowolnie podanych danych (RODO w motywie 57 stanowi: „Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji od osoby której dane dotyczą by ułatwić jej wykonanie i praw." Wskazanie to można zastosować także do obszaru ochrony zdrowia i praw związanych z dostępem do świadczeń); e) wprowadzenie możliwości bezpiecznej rejestracji elektronicznej. Uwagi dodatkowe:

	Ustalenie tożsamości Pacjenta jest elementem wymaganym przepisami prawa zarówno na gruncie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (art. 25 ust. 1), jak również ustawy o świadczeniach opieki zdrowotnej, finansowanych ze środków publicznych (art. 20) oraz ustawy o systemie informacji w ochronie zdrowia. Na gruncie RODO ustalenie tożsamości osoby, która składa wniosek z żądaniem wykonania prac wskazanych w art. 15-22 RODO także ma istotne znaczenie. Nie ulega wątpliwości, że Podmiot wykonujący działalność leczniczą zobowiązany jest do potwierdzenia tożsamości osoby zgłaszającej się do podmiotu - zarówno w zakresie uprawnień do udzielania świadczenia, prawidłowego udzielenia świadczenia i prowadzenia Dokumentacji medycznej, jak i w zakresie spełnienia wymogów RODO w stosunku do osoby, której dane dotyczą i ochrony jej praw.
W jaki sposób w czasie wzywania Pacjentów do gabinetów lekarskich można zapewnić im anonimowość, gdy placówka nie ma środków na wdrożenie elektronicznego systemu identyfikacji Pacjentów (numerki wyświetlane nad gabinetami), a na korytarzu przebywa czasami ogromna ilość Pacjentów?	Dążyć należy do minimalizacji ryzyka ujawnienia informacji osobom postronnym, w szczególności danych o stanie zdrowia, z uwzględnieniem konkretnych uwarunkowań technicznych, organizacyjnych i lokalowych w placówce. Zastosowane rozwiązania nie mogą w żadnym zakresie zakłócać udzielania świadczeń opieki zdrowotnej ani narażać zdrowia lub życia Pacjentów. Możliwe przykładowe sposoby wywoływania Pacjenta w podmiocie leczniczym: 1. Wezwanie z wykorzystaniem numeru identyfikacyjnego nadanego zgodnie ze wskazaniami art. 36 ust. 5 ustawy o działalności leczniczej znaku/pseudonimu numerycznego wpisanie tych numerów do Dokumentacji medycznej następuje z jednoczesnym przekazaniem ich Pacjentowi. Pacjent wzywany jest wówczas do gabinetu po tym unikalnym numerze. 2. Wezwanie po numerze nadanym podczas rejestracji. Takie rozwiązania nie wymaga nakładów finansowych, a wiążę się jedynie z nadawaniem unikalnego numeru podczas rejestracji w sposób, zapewniający przekazanie numeru lekarzowi w gabinecie oraz Pacjentowi (dopięty do karty, wpisany w dokumentację w systemie, przekazany Pacjentowi). 3. Wezwanie po godzinie wizyty. Wizyty umawiane są na konkretną godzinę w sposób uniemożliwiający pokrywanie się tych godzin.

	4. Wezwanie po imieniu, gdy jest to wystarczające np. gdy w kolejce oczekujących jest tylko jedna osoba o danym imieniu. 5. Rozwiązania mieszane łączące wskazane wyżej informacje i lub inne szczegóły: a) jak w punkcie trzecim z dodatkowym wezwaniem po imieniu - np. Pan Michał z godziny 11:30; b) dodanie numeru gabinetu, np. Pan Jan z godziny X proszony do gabinetu Y. 6. Jeżeli podmiot ma możliwość wdrożenia elektronicznego systemu identyfikacji Pacjentów (numerki wyświetlane nad gabinetami) stosowanie takiego systemu. 7. Gdy jest kilka kategorii Pacjentów lub rodzajów poradni możliwe jest przydzielanie numerów w różnych kolorach (np. czerwona jedynka, żółta trójka itp.). 8. Jeśli jest to możliwe, w szczególności gdy osoba wykonująca zawód medyczny zna Pacjenta, można zrezygnować ze wskazanych wyżej sposobów wezwań. Niezależnie od powyższego, możliwe jest zastosowanie metody identyfikacji tożsamości z wykorzystaniem nazwiska bądź imienia i nazwiska oraz innych niezbędnych danych osobowych Pacjenta w przypadku Szpitalnych Oddziałów Ratunkowych, Izb Przyjęć pełniących funkcję SOR oraz jednostek ratownictwa medycznego oraz w każdej sytuacji, w której istnieje zagrożenie zdrowia bądź życia, a nie jest możliwe zastosowanie metod wskazanych powyżej w punktach 1-8.
Czy placówka zdrowia może na drzwiach gabinetów lekarskich zamieszczać imiona, nazwiska oraz specjalizacje lekarzy przyjmujących Pacjentów?	Tak. Zamieszczenie imion i nazwisk oraz specjalizacji lekarza na drzwiach gabinetów lekarskich nie narusza RODO. Informacje o imieniu i nazwisku lekarza oraz jego specjalizacji są jego zwykłymi danymi osobowymi. Zgodnie z art. 6 ust. 1 lit. c RODO podstawą przetwarzaniem zwykłych danych osobowych jest realizacja obowiązku wynikającego z przepisów prawa. Zgodnie z art. 31 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych świadczeniobiorca/ Pacjent ma prawo wyboru lekarza, a zgodnie z art. 36 ustawy o działalności leczniczej osoby zatrudnione w szpitalu bądź pozostający w stosunku

	cywilnoprawnym z podmiotem leczniczym, którego zakładem leczniczym jest szpital, są obowiązane nosić w widocznym miejscu identyfikator zawierający imię i nazwisko oraz funkcję tej osoby. Dane lekarza, w tym w szczególności imię nazwisko, rodzaj i stopień posiadanej specjalizacji, czy też umiejętności z zakresu węższych dziedzin medycyny lub udzielania określonych świadczeń zdrowotnych zawarte są w rejestrze lekarzy prowadzoną przez właściwą okręgową radę lekarską, o którym mowa w art. 8 ust. 1 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty. Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2012 roku w sprawie szczegółowych wymagań jakim powinny odpowiadać pomieszczenia i urządzenia Podmiotu wykonującego działalność leczniczą przesądza o obowiązku oznaczenia gabinetów lekarskich.
Czy lekarz może na Sali chorych rozmawiać z Pacjentem o jego chorobie, gdy nie ma gwarancji czy nie słyszą tego inni Pacjenci, a stan zdrowia Pacjenta pozwala na przeprowadzenie takiej rozmowy poza salą chorych?	Co do zasady, przekazywanie przez personel medyczny Pacjentowi informacji ujawniających dane o stanie jego zdrowia, na sali wieloosobowej, powinny być ograniczone do minimum niezbędnego do realizacji celu, w którym są przetwarzane („minimalizacja danych" – art. 5 ust. 1 lit. c RODO). W odpowiedzi na pytanie wyodrębnić należy dwie sytuacje: 1. Komunikacja z Pacjentem niezwiązana z realizacją codziennych czynności medycznych. Chodzi tutaj zwłaszcza o działania nie będące monitorowaniem stanu zdrowia, pytaniami o samopoczucie, czy uzyskiwaniem i przekazywaniem informacji związanych z procesem leczenia. Bez wątpienia mogą należeć do nich: informowanie o pobieraniu świadomej zgody na procedury medyczne, informacja o diagnozie i sposobie leczenia, itp. Jeżeli stan zdrowia Pacjenta na to pozwala, przekazanie Pacjentowi takich informacji powinno nastąpić w gabinecie lekarskim, pokoju badań lub innym ustronnym miejscu, tj. w miejscu, w którym nie przebywają inne nieuprawnione osoby, np. inni Pacjenci (dotyczy to zarówno sali chorych, jak i np. korytarza szpitalnego). Przy rozmowie może być obecna, za zgodą Pacjenta, np. Osoba bliska/członek rodziny. 2. Komunikacja z Pacjentem związana bezpośrednio z realizacją bieżącego monitorowania stanu zdrowia

	Pacjenta, w tym pytanie o samopoczucie, uzyskanie i przekazanie podstawowych informacji związanych z procesem leczenia. Chodzi tutaj również o czynności w ramach obchodu lekarskiego lub pielęgniarskiego - podstawowa komunikacja z Pacjentem, przekazanie informacji o zmianie leków, przekazanie informacji o planowanych badaniach, itp. W takich przypadkach możliwe jest przekazanie informacji o stanie zdrowia Pacjenta na sali chorych. W trakcie wykonywania bieżących czynności medycznych, w tym w trakcie obchodu lekarskiego/pielęgniarskiego, na sali mogą przebywać wyłącznie osoby uprawnione, tj. personel medyczny, opiekun faktyczny, opiekunowie ustawowi Pacjenta małoletniego, całkowicie ubezwłasnowolnionego lub niezdolnego do świadomego wyrażenia zgody. Na życzenie Pacjenta w trakcie udzielania świadczenia może być obecna Osoba bliska z zastrzeżeniem, że w przypadku obchodu opuszcza salę chorych, jeżeli omawiany jest stan zdrowia innego Pacjenta. Powinni móc zostać tylko rodzice lub opiekunowie osób niesamodzielnych. W przypadku, gdy rozmowa o stanie zdrowia Pacjenta związana jest bezpośrednio z ratowaniem życia bądź zdrowia i nie przeprowadzenie rozmowy w trybie natychmiastowym mogłoby narazić Pacjenta na uszczerbek, możliwe jest przeprowadzenie rozmowy w każdym miejscu. Jeżeli sytuacja wskazane w pytaniu nie dotyczy bieżących czynności medycznych lub obchodu, rozmowa taka powinna być przeprowadzona w miejscu, w którym nie przebywają inne nieuprawnione osoby np. inni Pacjenci (dotyczy to zarówno sali chorych jak i korytarza szpitalnego). W myśl ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, lekarz podczas udzielania świadczeń zdrowotnych ma obowiązek poszanowania intymności i godności osobistej Pacjenta, w szczególności w czasie udzielania świadczeń zdrowotnych. Nakłada to na podmiot leczniczy obowiązek wdrożenia takich procedur organizacyjnych, zgodnie z którymi prowadzona rozmowa dotycząca stanu zdrowia Pacjenta będzie prowadzona na osobności. Przy rozmowie może być natomiast obecna, za zgodą Pacjenta, np. Osoba bliska/ członek rodziny. W sytuacjach, w których stan Pacjenta uniemożliwia przeprowadzenie takiej rozmowy poza salą chorych, przewagę ma prawo Pacjenta do uzyskania informacji

	o swoim stanie zdrowia. W czasie takiej rozmowy osoby odwiedzające powinny opuścić salę chorych. Jeżeli u Pacjenta, któremu przekazujemy informacje są osoby odwiedzające, to także powinny opuścić salę chorych chyba, że Pacjent wyraża zgodę na ich pozostanie. Jeżeli na sali pozostają inni Pacjenci to przekazywanie informacji powinno odbywać się w jak najbardziej dyskretny sposób - zastosowanie parawanu, przyciszenie głosu. Zastosowanie znajdzie w tym przypadku również zamieszczona poniżej informacja o zapewnieniu organizacyjnych, technicznych i lokalowych środków organizacyjnych ryzyko ujawnienia danych osobowych dotyczących Pacjenta. W przypadku obchodów lekarskich odbywających się w bezpośrednim miejscu hospitalizacji Pacjenta, należy wdrożyć odpowiednie środki zapewniające poszanowanie intymności Pacjenta: 1. Osoby nieuprawnione, tj. osoby odwiedzające innych Pacjentów, powinny w czasie obchodu opuścić salę chorych, a drzwi od sali, jeżeli to możliwe powinny zostać zamknięte tak, aby osoby nieuprawnione nie mogły usłyszeć informacji przekazywanych podczas obchodu. 2. Jeżeli u Pacjenta, któremu przekazujemy informacje, są osoby odwiedzające, to także powinny opuścić salę chorych chyba, że są to osoby bliskie wskazane w art. 21 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a Pacjent wyraża życzenie ich pozostania w sali. Pozostać na sali chorych mogą także Przedstawiciele ustawowi Pacjenta małoletniego, całkowicie ubezwłasnowolnionego lub niezdolnego do świadomego wyrażenia zgody. 3. Osoby biorące udziału w obchodzie inne niż udzielające świadczeń zdrowotnych np. inni lekarze, pielęgniarki, fizjoterapeuci, biorą udział w obchodzie bez zgody Pacjenta, jeżeli są osobami wykonującymi zawód medyczny, tylko wtedy, gdy jest to niezbędne ze względu na rodzaj świadczenia. Jeżeli nie spełniają tego wymogu, to mogą brać udział w obchodzie wyłącznie za zgodą Pacjenta, chyba że ma do nich zastosowanie przepis art. 36 ust. 4 ustawy o zawodach lekarza i lekarza dentysty. Do klinik i szpitali akademii medycznych, medycznych jednostek badawczo-rozwojowych i innych jednostek uprawnionych do kształcenia studentów nauk medycznych, lekarzy oraz innego personelu medycznego w zakresie niezbędnym

	do celów dydaktycznych nie stosuje się art. 22 ust. 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Natomiast biorąc pod uwagę obowiązki lekarza wynikające z Kodeksu Etyki Lekarskiej, niezależnie od tego, lekarz powinien uzyskać zgodę Pacjenta na udział studentów w udzielaniu świadczeń zdrowotnych (może to być zgoda w formie ustnej). 4. Jeżeli podczas obchodu lekarze zamierzają dokonać obserwacji miejsc intymnych Pacjenta, wyniki obserwacji Pacjenta nie powinny być wypowiadane na głos na sali wieloosobowej, a jedynie wpisywane do Dokumentacji medycznej.
Czy RODO znajduje zastosowanie do wszelkich przypadków rozmów prowadzonych z Pacjentem zarówno przez personel medyczny, jak i administrację szpitala?	Nie. RODO znajduje zastosowanie do każdej rozmowy z Pacjentem, której przedmiotem są dane osobowe. RODO znajduje więc zastosowanie do rozmów Pacjenta z personelem medycznym i administracją szpitala w każdym przypadku, gdy rozmowa dotyczy danych osobowych gromadzonych przez placówkę leczniczą co najmniej w sposób częściowo zautomatyzowany oraz w zbiorach danych. Nie znajdzie więc zastosowania do rozmów do momentu, gdy ograniczają się one wyłącznie do informowania Pacjenta na przykład o jego prawach, organizacji placówki czy zasadach świadczenia usług medycznych. RODO znajdzie jednak zastosowanie do przypadku, gdy dyrektor lub inna osoba z administracji szpitala w rozmowie z Pacjentem ustosunkuje się do złożonej przez niego skargi w zakresie leczenia. Nawet zastosowanie RODO nie przesądza jednak o niemożności prowadzenia takich rozmów. Muszą być one jednak przeprowadzone z poszanowaniem prywatności Pacjenta.
Czy lekarz i personel medyczny na sali chorych może zwracać się do Pacjentów po imieniu i nazwisku?	Lekarz nie powinien na sali chorych zwracać się po imieniu i nazwisku do Pacjenta. Można natomiast zwracać się do Pacjenta używając chociażby zwrotu „Pan/Pani" wraz z dodaniem imienia, co jednocześnie zagwarantuje poszanowanie godności Pacjenta. Wyjątkiem są przypadki, gdy lekarz nie może zidentyfikować Pacjenta w inny sposób niż poprzez użycie jego nazwiska, bądź gdy jest to konieczne dla podejmowania nagłych czynności ratowania życia bądź zdrowia. Zgodnie z art. 9 ust. 2 lit. h RODO przetwarzanie danych osobowych dotyczących stanu zdrowia możliwe jest, gdy jest niezbędne do celów Profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki zdrowotnej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa państwa

	członkowskiego. Należy w tym zakresie zwrócić szczególną uwagę, że zgodnie z art. 36 ust. 3 i 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej, Pacjentów zaopatruje się w znaki identyfikacyjne. Znak identyfikacyjny zawiera informacje pozwalające na ustalenie m.in. imienia i nazwiska oraz datę urodzenia Pacjenta. Jedynie w przypadku uzasadnionym stanem zdrowia Pacjenta kierownik może podjąć decyzję o odstąpieniu od zaopatrywania tego Pacjenta w znak identyfikacyjny. Informacje w tym zakresie wraz z podaniem przyczyny odstąpienia zamieszcza się w Dokumentacji medycznej Pacjenta (art. 36 ust. 3a ustawy o działalności leczniczej). Zatem zasadą powinna być identyfikacja Pacjenta na podstawie ww. znaku np. wskazanego na opasce. Informacje na ww. znaku mają być tak zapisane, żeby uniemożliwić jego identyfikację przez osoby nieuprawnione. Warunki, sposób i tryb zaopatrywania Pacjentów szpitala w znaki identyfikacyjne oraz sposób postępowania w razie stwierdzenia braku są określone w rozporządzeniu Ministra Zdrowia z dnia 20 września 2012 r. wydanego na podstawie art. 36 ust. 6 ustawy o działalności leczniczej. Celem ww. przepisów jest zatem uniemożliwienie identyfikacji Pacjenta przez osoby postronne. Tym samym przyjęcie jako zasady zwracania się do Pacjenta przez personel medyczny po imieniu i nazwisku byłoby niezgodne z celem jaki wynika z ww. przepisów.
Czy możliwe jest oznaczanie produktów leczniczych imieniem i nazwiskiem Pacjenta?	Tak. Ze względu na ograniczenie ryzyka pomyłek, oznaczenie imieniem i nazwiskiem Pacjenta, gdy korzysta ze świadczenia w podmiocie leczniczym jest dopuszczalne. Dotyczy to wszystkich produktów leczniczych (w tym podawanych w kroplówkach), wyrobów medycznych i innych środków podawanych Pacjentowi. Podstawą prawną przetwarzania danych osobowych w powyższym zakresie jest art. 9 ust. 2 lit. h RODO. Jeżeli oznaczenie imieniem i nazwiskiem nie będzie wystarczające dla zapewnienia minimalizacji ryzyka pomyłem PWDL może wykorzystać dodatkowe dane identyfikujące Pacjenta. Zgodnie z art. 9 ust. 2 lit. c RODO przetwarzanie danych osobowych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba której dane dotyczą jest fizycznie lub prawnie niezdolna do wyrażenia zgody. Nie ulega wątpliwości, że z uwagi na ogromne ryzyko związane z podaniem niewłaściwego produktu medycznego osobie, której on nie przysługuje oraz konsekwencje mogące mieć poważny wpływ na zdrowie, a nawet życia Pacjentów, powyższa przesłanka stanowi bezpośrednio podstawę

	prawną do imiennego oznaczenia produktów medycznych. Nie ulega również wątpliwości, że podawanie produktów medycznych w postaci chociażby kroplówek, czy krwi do transfuzji następuje w sytuacji, w której niemal niemożliwym jest odbieranie zgód od Pacjentów na przetwarzanie ich danych. Uznanie, że podstawą prawną przetwarzania w takim przypadku danych osobowych jest zgoda doprowadziłoby do ogromnych problemów po stronie placówek medycznych w przypadku, gdyby ktoś taką zgodę odwołał. Świadczenie usług opieki medycznej byłoby w takich przypadkach niemożliwe.
Czy podmiot leczniczy może uzależnić wgląd do Dokumentacji medycznej osoby trzeciej od posiadania upoważnienia udzielonego przez Pacjenta, którego dotyczy dokumentacja, opatrzonego własnoręcznym podpisem albo złożonym w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym?	Zgodnie z obowiązującymi przepisami ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta upoważnienie w danej placówce może być udzielone w dowolnej formie, a ograniczenie formy upoważnienia w regulaminach stanowi naruszenie zbiorowych praw Pacjentów. Należy jednak pamiętać, że placówka powinna mieć pewność w zakresie tożsamości osoby udzielającej upoważnienie. W związku z powyższym, w przypadku gdy Pacjent upoważnienia udziela bezpośrednio w obecności personelu, dopuszczalna powinna być każda forma takiego oświadczenia. W przypadku złożenia upoważnienia przy braku obecności personelu medycznego dopuszczalne powinny być różne alternatywne sposoby upoważnienia, które jednak w dostateczny sposób potwierdzają tożsamość Pacjenta. Mogą być to chociażby przykładowo: a) upoważnienie podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym; b) upoważnienie udzielone za pośrednictwem systemów informatycznych np. Internetowe Konto Pacjenta, uwierzytelniające osobą upoważniającą.
Czy podmiot leczniczy może wykorzystywać utrwaloną już metodę ujawniania informacji o stanie zdrowia w zakresie temperatury Pacjenta na tzw. kartach przyłóżkowych (kartach zamieszczonych przy łóżkach szpitalnych Pacjentów)?	Tak. Podmiot medyczny może wykorzystywać w swojej praktyce karty przyłóżkowe. Rezygnacja z nich jest natomiast dobrą praktyką. Należy zwrócić szczególną uwagę, że istotą działań wszystkich placówek medycznych jest ochrona życia bądź zdrowia Pacjenta. W bardzo wielu przypadkach nagłe pogorszenie się stanu zdrowia Pacjenta może wymagać natychmiastowego dostępu do jego danych identyfikacyjnych. Powyższe dotyczy niemal wszystkich kategorii oddziałów, na których przebywają Pacjenci. Karty przyłóżkowe dają taką gwarancję. Podmiot leczniczy może natomiast całkowicie zrezygnować z kart przyłóżkowych z uwzględnieniem obowiązków wynikających z przepisów art. 36 ust. 3, 5 i 6 ustawy z dnia

	15 kwietnia 2011 r. o działalności leczniczej. Jest to również dobra praktyka rynkowa i standard wynikający również z wymogów akredytacyjnych. W przypadku, gdy stosowanie kart jest konieczne, w szczególności na oddziałach ratunkowych, konieczne jest ich zabezpieczenie poprzez: a) zastosowanie ramek na kartę przyłóżkowe chroniących dane osobowe zawarte w kartach; b) konstrukcja ramki powinna uniemożliwiać odczytanie danych; c) zastosowanie nakładki zabezpieczające i dane Pacjenta na karcie przyłóżkowej; d) odwrócenie kart przy łóżkowych.
Czy podmiot leczniczy może udostępniać telefonicznie informacje o fakcie hospitalizacji Pacjentów o wskazanej przez rozmówcę tożsamości, gdy nie ma pewności co do tożsamości rozmówcy, ale udzielenie takich informacji może mieć wpływ na stan zdrowia bądź życie Pacjenta?	Tak, ale może to mieć miejsce w wyjątkowych przypadkach. Często pojawiające się w tym zakresie problemy wynikają z braku wdrożenia odpowiednich procedur postępowania w placówce i braku świadomości pracowników w zakresie swoich obowiązków i zasad udostępniania danych w takich sytuacjach. Niemniej nie wszystko jest możliwe do uregulowania. Dlatego bardzo ważne jest odwołanie się do kategorii zdrowego rozsądku i doświadczenia życiowego. W przypadku, kiedy odmowa udzielenia informacji o pobycie Pacjenta w szpitalu może uniemożliwiać realizację prawa członków rodziny bądź osób bliskich do informacji o stanie zdrowia Pacjenta, podmiot powinien udzielić takiej informacji w sytuacjach nagłych (np. wypadek drogowy klęska żywiołowa) oraz stanach zagrożenia dla życia Pacjenta. Placówka powinna jednak dostatecznie uprawdopodobnić, że rozmówca jest osobą uprawnioną do uzyskania tej informacji poprzez zadanie pytań kontrolnych np. zapytanie o PESEL Pacjenta lub adres jego miejsca zamieszkania (jeśli podmiot leczniczy dysponuje takimi informacjami). Dodatkowo należy kierować się zasadą minimalizacji i przekazywać telefonicznie jedynie te informacje, które są niezbędne do działania w stanie wyższej konieczności. Dodatkowych informacji udziela się po ustaleniu tożsamości osoby uprawnionej (np. Przedstawiciela ustawowego). Podstawą prawną może być zarówno art. 9 ust. 2 lit. h RODO jak również w niektórych sytuacjach art. 9 ust. 2 lit. c, czyli gdy przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba której dane dotyczą jest fizycznie lub pragnienie zdolna do wyrażenia zgody. W sytuacjach kryzysowych często nie ma też potrzeby udzielania szczegółowych informacji o stanie zdrowia.

Załącznik nr 4

8.4. Przykładowa metodyka analizy ryzyka, której wdrożenie i stosowanie zapewnia realizację podejścia opartego na ryzyku

Ocena ryzyka naruszenia praw i wolności osób fizycznych

Przeprowadzenie oceny ryzyka ma na celu:

a) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania danych osobowych;
b) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniający adekwatny stopień bezpieczeństwa odpowiadający ryzyku;
c) ocenę, czy stopień bezpieczeństwa jest odpowiedni, uwzględniając ryzyko wiążące się z przetwarzaniem, w szczególności 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.

Ocena ryzyka jest procesem ciągłym, monitorującym adekwatność oraz skuteczność stosowanych zabezpieczeń organizacyjnych i technicznych, ma na celu utrzymanie ryzyka na akceptowalnym poziomie.

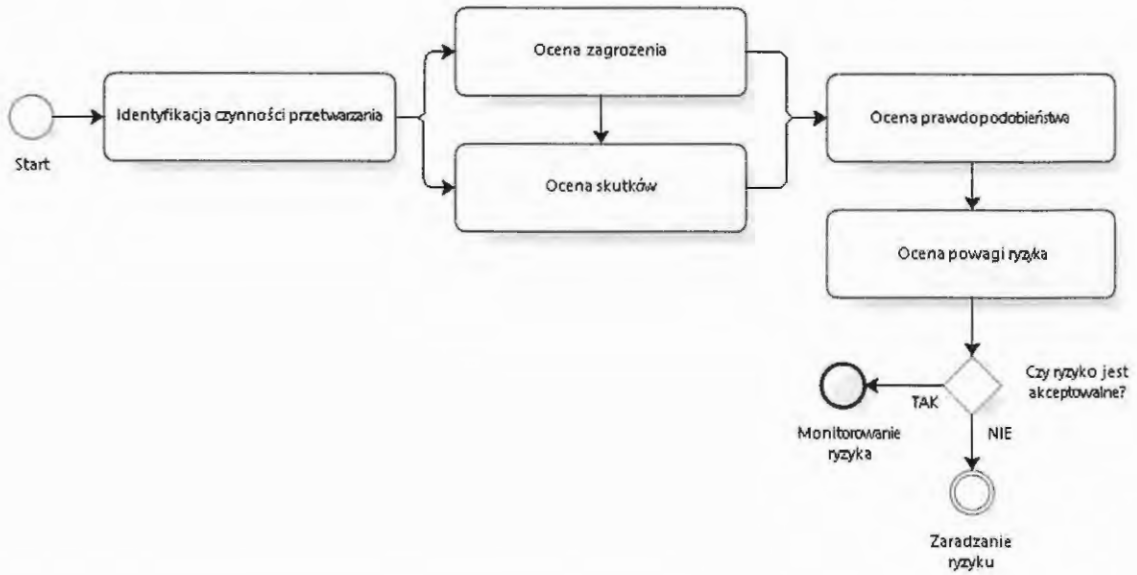
Powinno się badać oddzielnie ryzyko związane z prywatnością z punktu widzenia osoby której dane dotyczą oraz ryzyko związane z prywatnością z punktu widzenia organizacji.

Ocena ryzyka powinna być uruchamiana na etapie projektowania czynności przetwarzania, nawet jeśli niektóre czynności przetwarzania są wciąż nieznane. Konieczne może być powtórzenie poszczególnych etapów oceny ryzyka w miarę postępu procesu projektowania, ponieważ wybór niektórych środków technicznych lub organizacyjnych może mieć wpływ na wagę lub prawdopodobieństwo wystąpienia zagrożeń związanych z przetwarzaniem danych osobowych.

Wymaganie cyklicznej aktualizacji przeprowadzonej oceny ryzyka naruszenia praw i wolności osób fizycznych po rozpoczęciu procesu przetwarzania jest ważnym mechanizmem weryfikującym adekwatność i skuteczność zastosowanych środków technicznych i organizacyjnych względem identyfikowanej powagi ryzyka.

Poniższy schemat prezentuje etapy przeprowadzenia oceny ryzyka naruszenia praw i wolności osób fizycznych:

1. Identyfikacja czynności przetwarzania;
2. Ocena zgodności czynności przetwarzania z prawem
3. Ocena zagrożeń;
4. Ocena skutków (konsekwencji);
5. Ocena prawdopodobieństwa wystąpienia zagrożeń;
6. Ocena powagi ryzyka.



Identyfikacja czynności przetwarzania (procesów)

Czynności przetwarzania zgodnie z wytycznymi polskiego organu nadzorczego oraz w kontekście obowiązku określonego w art. 30 ust. 1 RODO należy rozumieć jako zespół powiązanych ze sobą działań, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane. Na podstawie analizy czynności przetwarzania należy zidentyfikować procesy, w których dane są przetwarzane. Procesy są zestawem powiązanych ze sobą lub oddziałujących ze sobą działań, które przekształcają dane wejściowe w dane wyjściowe.

Możemy wyróżnić dwie główne kategorie procesów – procesy operacyjne związane z obsługą świadczeniobiorców oraz procesy wspomagające procesy operacyjne.

Dla uproszczenia można przyjąć, że czynności przetwarzania zidentyfikowane na potrzeby stworzenia rejestru czynności przetwarzania są równoważne z procesami przetwarzania i mogą być przedmiotem oceny ryzyka naruszenia praw i wolności osób fizycznych.

Poniżej przedstawiono przykładowe listy procesów zidentyfikowanych w podmiotach wykonujących działalność leczniczą[74]:

- procesy operacyjne – dotyczące obsługi Pacjentów (przykłady):
  a) Profilaktyki zdrowotnej;
  b) medycyny pracy, w tym oceny zdolności pracownika do pracy;
  c) diagnozy medycznej i leczenia;
  d) zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej – opieka szpitalna;
  e) zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej – opieka ambulatoryjna;

[74]Procesy będą różne w zależności od placówek np. w niektórych placówkach można wyróżnić proces opieki duszpasterskiej, czy osobne procesy przetwarzania dla laboratorium lub zakładu diagnostyki obrazowej.

f) zapewnienia zabezpieczenia społecznego oraz zarządzania systemami i usługami zabezpieczenia społecznego;
g) przetwarzanie danych w celach marketingowych;
h) przetwarzanie danych w celach prowadzenia badań klinicznych;
i) przetwarzanie w celach profilowania i automatycznego podejmowania decyzji.

- Procesy wspomagające (przykłady):
  a) kadry – przetwarzanie w celach rekrutacyjnych, zatrudnienia pracownika;
  b) księgowość – przetwarzanie w szczególności w celach prowadzenia sprawozdawczości finansowej;
  c) IT – przetwarzanie w celach zapewnienie ciągłości działania oraz bezpieczeństwa danych (w pewnym zakresie), obsługi zgłoszeń, serwisowania urządzeń i systemów;
  d) zarządzanie jakością - np. w ramach stanowiska audytu wewnętrznego, czy kierownika ds. jakości;
  e) ochrona fizyczna - przetwarzanie w celach zapewnienie bezpieczeństwa osób, danych i mienia w obszarze objętym ochroną fizyczną;
  f) monitoring wizyjny - przetwarzanie w celach zapewnienie bezpieczeństwa osób, danych i mienia w obszarze objętym monitoringiem[75].

W celu identyfikacji zagrożeń można posłużyć się poniżej przedstawionymi pytaniami:
- jaka jest podstawa przetwarzania danych osobowych?
- Jakie jest źródło pozyskiwania danych osobowych?
- jakie posiadamy aktywa wspierające procesy przetwarzania?
- kto jest odpowiedzialny w podmiocie za przetwarzanie danych osobowych?
- jakie dane osobowe są przetwarzane i jaki jest ich zakres?
- jaki jest cel przetwarzania?
- jakie są główne korzyści płynące z przetwarzanych danych osobowych dla osoby fizycznej, grupy osób lub ogółu społeczeństwa?
- kim są odbiorcy danych osobowych i w jakim celu udostępnia się im dane osobowe?
- jak są skonstruowane procesy, które są realizowane dzięki przetwarzaniu tych danych osobowych?
- w jaki sposób będą realizowane prawa osób, których dane dotyczą, wynikające z RODO (zawiadomienie, cofnięcie zgody, dostęp, sprostowanie, usuwanie, etc.)?
- w jaki sposób osoby, których dane dotyczą, będą powiadamiane np. o incydentach bezpieczeństwa?

Analizując aktywa wspierające procesy należy uwzględnić:
- jaki sprzęt i oprogramowanie jest użytkowane obecnie;

[75]Proces ten może być analizowany w ramach szerszego procesu ochrony fizycznej lub jako odrębny proces.

- jaki rodzaj sprzętu komputerowego podmiot posiada (komputery, routery, inne media elektroniczne biorące udział w procesie przetwarzania np. urządzenia diagnostyczne);
- jakiego rodzaju oprogramowanie jest użytkowane w podmiocie (systemy operacyjne, systemy powiadamiania, bazy danych itp. –należy wskazać jakie to aktywa i ile jest tych aktywów);
- jakie rodzaje sieci komputerowych użytkowane są w podmiocie (kable, WiFi, światłowody itp.);
- jakie rodzaje nośników informacji w postaci papierowej są stosowane (wydruki, ksero itp.);
- jakie istnieją w podmiocie kanały przesyłu informacji, zarówno papierowej jak i elektronicznej (EMAIL, systemy obiegu dokumentów elektronicznych, karty Pacjenta przekazywane pomiędzy pracownikami w procesie);
- jacy pracownicy (grupy pracowników) będą uczestniczyć w przetwarzaniu danych w analizowanym procesie?;
- jacy dostawcy będą przetwarzać dane w procesie.

W odniesieniu do zidentyfikowanych systemów informacyjnych i aktywów wspierających, osoba przeprowadzająca ocenę wpływu powinna uwzględnić w tym procesie następujące kwestie:

- sposób zarządzania tożsamością i uprawnieniami użytkowników;
- jakie prace wykonywane są w podmiocie a jakie poza nim;
- wykorzystywanie wykonawców i podwykonawców oraz stopień dostępu jaki posiadają do danych osobowych;
- procedury stosowane w zakresie logowania, wykonywania kopii zapasowych, odzyskiwania danych, przekazywania nośników danych do Wykonawców, niszczenia danych;
- likwidacja systemów np. wycofanie z użytkowania.

Krok ten powinien zostać przeprowadzony podczas wykonywana procedury analizy zgodnie z załącznikiem nr 1.
Jeżeli jest to uzasadnione, do prac nad oceną wpływu, zaangażowane mogą zostać następujące osoby:

- pracownicy podmiotu, tacy jak: personel medyczny bezpośrednio związani z wykonywaniem czynności przetwarzania, pracownicy działów informatycznych, administratorzy aplikacji i baz danych, operatorzy sieci komputerowej, pracownicy odpowiedzialni za bezpieczeństwo, osoby odpowiedzialne za audyty wewnętrzne, osoby odpowiedzialne za finanse podmiotu, osoby odpowiedzialne za ochronę fizyczną podmiotu;
- wykonawcy i podwykonawcy;
- partnerzy biznesowi;
- niezależni eksperci w obszarze analizy ryzyka;

- inne osoby z innych organizacji, które mają uzasadnione wątpliwości związane z oceną wpływu na prywatność.

Ocena zgodności realizowanej lub planowanej czynności przetwarzania z RODO

W ramach tego kroku rekomenduje się dokonanie analizy prawnej czynności przetwarzania, m.in. poprzez odpowiedź na następujące kluczowe pytania:

- Czy istnieje ważna podstawa prawna przetwarzania?
- Czy realziowana jest zasada minimalizacji danych?
- Czy administrator danych realizuje/jest w stanie realizować prawa osób, których dane dotyczą?

W przypadku, gdyby okazało się, że dana czynność w swoich podstawowych założeniach nie jest zgodna z RODO, przed dalszą analizą należałoby:

- przemodelować wskazaną czynność bądź;
- zrezygnować z realizacji tej czynności.

Dodatkowo na tym etapie rekomenduje się również weryfikację, w oparciu o oficjalny wykaz opublikowany przez Prezesa Urzędu Ochrony Danych Osobowych, zasadności przeprowadzenia oceny skutków dla ochrony danych. W przypadku konieczności przeprowadzenia oceny skutków dla ochrony danych, należy przeprowadzić ją zgodnie z art. 35 RODO.

Ocena zagrożeń

Zagrożenie należy rozumieć jako potencjalną przyczynę niepożądanego incydentu, która może wywołać naruszenie praw lub wolności osób fizycznych.
Każde zidentyfikowane czynność przetwarzania należy rozważyć w kontekście możliwości wystąpienia zagrożenia, na zasadnie TAK/NIE (może wystąpić/ nie występuje).

Przykładowy katalog zagrożeń naruszenie praw lub wolności osób fizycznych
Przypadkowe lub niezgodne z prawem zniszczenie danych
Utracenie danych
Nieuprawnione zmodyfikowanie danych
Nieuprawnione ujawnienie danych
Nieuprawniony dostęp do danych osobowych przesyłanych
Nieuprawniony dostęp do danych przechowywanych
Nieuprawniony sposób przetwarzania danych
Brak podstawy prawnej do przetwarzania danych osobowych lub wskazana podstawa prawna nie jest jednoznaczna.

Wskazany katalog zagrożeń nie jest listą zamkniętą, w zależności od rodzaju, wielkości i natury prowadzonej działalności, w tym realizowanych czynności przetwarzania danych osobowych, należy rozważyć rozszerzenie katalogu. W przypisie wskazano na bardziej szczegółowy katalog zagrożeń dla przetwarzania danych w systemie informatycznym, który mógłby zostać wykorzystany przez organizacje, które ze względu na specyfikę działalności i przetwarzania danych osobowych i na posiadane zasoby realizują złożoną, szczegółową analizę ryzyka[76].

Ocena skutków (konsekwencji)

Dla każdej pary „czynność przetwarzania – zagrożenia" należy ocenić skutki (tj. konsekwencje) zmaterializowania się zagrożeń naruszenia praw lub wolności osób fizycznych w kontekście realizowanej czynności przetwarzania danych osobowych.

---

[76]**Poszerzony katalog zagrożeń występujących przy przetwarzaniu danych osobowych:**

- niewłaściwe uwierzytelnienie użytkowników w systemach teleinformatycznych;
- nieuprawniony dostęp przez użytkowników;
- nieuprawniony dostęp przez osoby z zewnątrz organizacji;
- nieuprawnione wykorzystanie aplikacji przetwarzającej dane osobowe;
- możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub inne "złośliwe oprogramowanie;
- nadużywanie zasobów;
- infiltracja komunikacji elektronicznej;
- przechwycenie komunikacji;
- brak niezaprzeczalności;
- błąd połączenia;
- osadzanie kodu złośliwego;
- niewłaściwe przekierowanie połączenia;
- awaria techniczna systemu lub infrastruktury sieciowej;
- awaria środowiska wsparcia;
- awaria systemu lub oprogramowania sieciowego;
- awaria oprogramowania aplikacji;
- błędne operacje przetwarzania danych.
- niewłaściwe odzyskiwanie po awarii (w tym tworzenia kopii zapasowych i przywracania systemów);
- błąd konserwacji;
- kradzież przez użytkowników w tym kradzież sprzętu lub danych;
- samowolne uszkodzenia przez użytkowników;
- terroryzm.

Szczegółowy opis wskazanych zagrożeń zawarty został w Rekomendacjach CSIOZ https://csioz.gov.pl/fileadmin/user_upload/rekomendacje_csioz_bezpieczenstwo_wrzesien2017_59cd1e951e9ba.pdf oraz w normie PN-EN ISO/IEC 27799:2016.

Lp.	Katalog skutków naruszenia praw lub wolności osób fizycznych, podlegający ocenie
1	Dyskryminacja
2	Kradzież tożsamości lub oszustwo dotyczące tożsamości
3	Strata finansowa osoby fizycznej
4	Naruszenie dobrego imienia osoby fizycznej
5	Naruszenie poufności danych osobowych chronionych tajemnicą zawodową (naruszenie godności i prywatności), w tym na skutek nieuprawnionego odwrócenia pseudonimizacji
6	Uszczerbek na zdrowiu lub śmierć
7	Wszelka inna znacząca szkoda gospodarcza lub społeczna osoby fizycznej

Tabela 1. Przykładowy katalog skutków naruszenia praw lub wolności osób fizycznych

Dla czynności przetwarzania, należy dokonać oceny skutków na podstawie przyjętej metodyki nadawania wartości np. ocena 4-stopniowa (pomijalne, niskie, średnie, wysokie). Dla każdego stopnia oceny przypisana jest wartość od 1 do 4.

Kategoria skutków	Skala poziomu skutków			
	1 – pomijalne	2 – niskie	3 – średnie	4 – wysokie

Ocena skutków naruszenia praw i wolności osób fizycznych	Osoba, której dane dotyczą nie będzie ponosić negatywnych skutków, bądź też dozna niewielkich niedogodności, które z łatwością pokona (np. strata czasu, drobne nieprzyjemności). Przykład: ujawnienie imion i nazwisk osób przypisanych do lekarza POZ.	Osoba, której dane dotyczą może mieć istotne niedogodności, które uda jej się przezwyciężyć pomimo pewnych trudności (dodatkowe koszty, stres, obawa, niewielkie niedogodności fizyczne).	Osoba, której dane dotyczą może być narażona na poważne skutki, które będzie w stanie z dużą trudnością odwrócić (strata pracy, pogorszenie stanu zdrowia, uszczerbek majątkowy).	Osoba, której dane dotyczą może być narażona na poważne, a wręcz nieodwracalne skutki (śmierć, długutrwałe pogorszenie zdrowia fizycznego lub psychicznego, spirala długów, brak zdolności do pracy).

Dla każdego zestawienia „czynność przetwarzania – zagrożenia - skutek" należy ocenić prawdopodobieństwo wystąpienia zagrożeń umożliwiające urzeczywistnienie się skutków.

Skutki należy ocenić na podstawie przyjętej metodyki nadawania wartości np. ocena 5-stopniowa (Mało prawdopodobne, Średnio prawdopodobne, Bardzo prawdopodobne, Wysoce prawdopodobne, Niemal pewne).

Ocena prawdopodobieństwa wystąpienia zagrożenia		
Wartość (*P*)	**Nazwa**	**Opis**
5	Niemal pewne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie zmaterializuje się w najbliższym czasie (prawie na 90%).
4	Wysoce prawdopodobne	Istnieją racjonalne przesłanki by ocenić, że zagrożenie raczej się zmaterializuje, istnieje więcej niż połowa szans na wystąpienie. Materializowało się w przeciągu ostatniego roku.
3	Prawdopodobne	Wystąpienie zagrożenia jest realne, lecz nie przekracza 50% prawdopodobieństwa. Materializowało się w przeszłości (w ciągu ostatnich 2 lat)
2	Średnio prawdopodobne	Zagrożenie może wystąpić sporadycznie (nie przekracza 25%). Materializowało się sporadycznie w przeszłości (w ciągu ostatnich 3 lat).
1	Mało	Zagrożenie raczej nie wystąpi lub możliwość jego

	prawdopodobne	wystąpienia jest znikoma (bliska zeru). Zagrożenie nie materializowało się w przeszłości.

Ocena powagi ryzyka (wartości oczekiwanej)

Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych oblicza się na podstawie niniejszego wzoru:

$$R = S * P$$

gdzie:

R – Ocena powagi ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania

S – Ocena skutków naruszenia praw lub wolności osób fizycznych

P – Ocena prawdopodobieństwa urzeczywistnienia się skutków

Uwaga, w kontekście ochrony dany osobowych nie priorytetyzuje się istotności czynności przetwarzania danych osobowych między sobą.

Poziom akceptacji

Otrzymane wyniki powagi ryzyka naruszenia praw lub wolności osób fizycznych należy przedstawić w postaci rankingu ryzyka, czyli od największej do najmniejszej wartości.

Poziom akceptacji ryzyka definiowany jest na podstawie przyjętej metodyki i wskazuje jaka wartość powagi ryzyka wymaga wdrożenia planu zaradzeniu ryzyka.
Poniższe tabele przedstawiają macierz ryzyka dla prywatności i poziom jego akceptacji.

		Ocena prawdopodobieństwa				
		1	**2**	**3**	**4**	**5**
Ocena skutków	**1**	1	2	3	4	5
	2	2	4	6	8	10
	3	3	6	9	12	15
	4	4	8	12	16	20

Powaga ryzyka	Sposób postępowania (decyzję podejmuje kierownik PWDL lub Podmiotu przetwarzającego)
1-6	Wskazane skutki w kontekście urzeczywistnienia się analizowanego zagrożenia nie występują. Ryzyka akceptowane, niewymagające dalszego postępowania (poza cyklicznym monitorowaniem).
8-20	Ryzyka nieakceptowane, wymagające zastosowania postępowania z ryzykiem. Ryzyka, które powinny być kompensowane wszystkimi możliwymi zabezpieczeniami, adekwatnie do potencjalnych kosztów rekompensaty. Powinno być możliwe stałe monitorowane w całym okresie przetwarzania danych.

5.2.7. Postępowanie z ryzykiem

Wybór najwłaściwszej opcji postępowania w przypadku wystąpienia nieakceptowalnego ryzyka dla praw i wolności osób fizycznych polega na przyjęciu przez Administratora sposobu postępowania z nim.
Istnieją cztery warianty postępowania z ryzykiem dla praw i wolności osób fizycznych:

- Redukcja ryzyka – redukcję ryzyka można osiągnąć poprzez wybór odpowiednich zabezpieczeń w warstwach organizacyjnej, systemowej i technicznej mając na względzie koszt wdrożenia zabezpieczeń i dostępne technologie. Istnieje prawdopodobieństwo, że po wdrożeniu zabezpieczeń w dalszym ciągu będzie istniało ryzyko szczątkowe, które będzie wymagało dalszych czynności i monitorowania w sposób ciągły;
- Akceptacja ryzyka – nie ma potrzeby wdrożenia dodatkowych zabezpieczeń ze względu na jego akceptacje przez Administratora;
- Unikanie ryzyka – gdy zidentyfikowane ryzyka zostaną uznane za zbyt wysokie, Administrator może podjąć decyzję o planowaniu wycofania się z zamiaru przetwarzaniem danych lub też zaprzestaniu ich przetwarzania;
- Przeniesienie ryzyka – najczęściej wiąże się z podziałem ryzyka lub też całkowitym jego przeniesieniem na podmiot zewnętrzny np. poprzez powierzenie przetwarzania danych wyspecjalizowanym podmiotom lub też poprzez zawarcie umowy ubezpieczenia, która będzie wspierać konsekwencje wynikające z naruszenia prywatności.

Jeśli oceniany proces zgodnie z przeprowadzoną analizą wykazuje wysokie prawdopodobieństwo naruszenia praw i wolności osób fizycznych, tj. nieakceptowalny poziom ryzyka, którym Administrator nie jest w stanie odpowiednio zarządzić, PWDL jako Administrator Danych Osobowych zobowiązany jest dokonać tzw. uprzednich konsultacji z PUODO co do dalszego postępowania.

Zabezpieczenia

Wynikiem procesu szacowania ryzyka jest wskazanie procesów, które będą wymagały wdrożenie zabezpieczeń. Dobór zabezpieczeń leży po stronie Administratora, jednak to właśnie Administrator jest obowiązany do wykazania, że są one adekwatne do przetwarzanych danych.
Tutaj również przychodzi nam z pomocą norma ISO i tym razem jest to norma - ISO/IEC 29151:2017 - wytyczne w zakresie wprowadzenia zabezpieczeń przy przetwarzaniu danych. Norma ta w swojej treści odnosi się wprost do zabezpieczeń wynikających z normy PN-ISO/IEC 27001:2017 w aspekcie ochrony danych osobowych. Ponadto podczas doboru zabezpieczeń należy mieć na uwadze obowiązujące przepisy prawa oraz regulacje branżowe.
Na podstawie załącznika A do normy PN-ISO/IEC 27001:2013 oraz normy PN-ISO/IEC 27002:2014 opracowano tabele mapującą zabezpieczenia na zagrożenia i podatności występujące przy przetwarzaniu danych osobowych. Tabela ta została zawarta w załączniku nr 5 do Kodeksu.

Załącznik nr 5

8.5. Wykaz zabezpieczeń systemów IT

ZAGROŻENIA I PODATNOŚCI/ Działanie minimalizujące	Polityka bezpieczeństwa	Role i odpowiedzialności	Polityka kontroli dostępu	Polityka czystego biurka i czystego ekranu	Polityki i procedury przekazywania informacji	Procedury nadawania i odbierania uprawnień do	Procedury logowania	Rejestrowanie zdarzeń	Polityka korzystania z zabezpieczeń kryptograficznych	Polityka bezpieczeństwa informacji w relacjach z	Bezpieczeństwo w umowach z dostawcami	Zarządzanie uprzywilejowanymi prawami dostępu	Odebranie lub dostosowanie praw dostępu	Ochrona informacji zawartych w dziennikach	Zabezpieczanie usługi aplikacyjnych i	Ochrona transakcji usług aplikacyjnych i	Rozdzielanie środowisk rozwojowych, testowych i	Zabezpieczenia przed oprogramowaniem malware	Zarządzanie kluczami kryptograficznymi	Zarządzanie podatnościami technicznymi	Zabezpieczenia sieci	Bezpieczeństwo usług sieciowych	Rozdzielanie sieci	Kopie zapasowe informacji	Zasady budowy bezpiecznego systemu	Wdrażanie ciągłości bezpieczeństwa informacji	Lokalizacja i ochrona sprzętu	Bliska granica obszaru bezpiecznego	Zabezpieczenia wejścia fizycznego	Zabezpieczanie biur, pomieszczeń i urządzeń	Pozostawienie sprzętu użytkownika bez opieki	Bezpieczeństwo sprzętu i aktywów poza siedzibą	Instalacja oprogramowania w systemach operacyjnych	Dostęp do sieci i usług sieciowych	Polityka dla urządzeń mobilnych	Polityka bezpieczeństwa prac rozwojowych	Procedury zarządzania zmianą w systemie	Bezpieczne środowisko rozwojowe	Prace rozwojowe powierzone firmie zewnętrznej	Testowanie bezpieczeństwa systemu	Systemy wspomagające	Konserwacja sprzętu	Inwentaryzacja i własność aktywów	Wiadomości elektroniczne	Telepraca	Szkolenia	Audyt
Uwierzytelnienie użytkowników w systemach teleinformatycznych	x	x	x			x	x	x																																		x	x
Nieuprawniony dostęp przez użytkowników	x	x	x			x				x	x	x	x	x																													x
Nieuprawniony dostęp przez osoby z zewnątrz organizacji	x	x	x			x			x						x		x	x		x	x	x	x	x	x																		x
Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat zdrowia pacjentów	x	x	x	x		x																					x	x	x	x	x												x	x
Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania [...]	x	x	x						x						x		x	x		x	x	x	x	x	x	x																	x	x
Nadużywanie zasobów	x	x	x												x																													x	x
Infiltracja komunikacji elektronicznej	x	x	x						x						x		x	x		x	x	x	x	x	x	x																	x	x
Przechwycenie komunikacji	x	x	x						x						x		x	x		x	x	x	x	x	x	x																	x	x
Brak niezaprzeczalności	x	x	x						x						x				x						x							x											x	x
Błąd połączenia	x	x	x						x						x		x				x	x	x		x	x																	x	x
Osadzanie kodu złośliwego	x	x	x						x						x		x	x		x	x	x	x	x	x	x																	x	x
Przekierowanie połączenia	x	x	x												x		x			x	x	x	x		x																			x	x
Awaria techniczna systemu lub infrastruktury sieciowej	x	x															x			x				x	x	x																		x
Awaria środowiska wsparcia	x	x																		x				x	x	x	x																		x
Awaria systemu lub oprogramowania sieciowego	x	x	x														x			x	x	x			x	x																	x	x
Awaria oprogramowania aplikacji	x	x	x												x		x			x					x	x																			x	x
Błędne operacje	x	x	x																																									x	x
Odzyskiwanie po awarii [...]	x	x																		x					x	x																			x	x
Błąd konserwacji	x	x	x																						x	x																			x	x
Błąd użytkownika	x	x	x		x										x	x									x																				x	x
Kradzież przez użytkowników w tym kradzież sprzętu lub danych	x	x	x				x			x					x														x	x	x			x									x	x
Samowolne uszkodzenia przez użytkowników	x	x	x				x																						x	x	x			x									x	x
Terroryzm	x	x	x														x					x	x	x		x	x		x	x	x			x									x	x

Załącznik nr 6

8.6. Wykaz norm mających zastosowanie w obszarze bezpieczeństwa informacji i ochrony danych osobowych

1. PN-EN ISO/IEC 27000:2017-06 Systemy zarządzania bezpieczeństwem informacji - Przegląd i terminologia.
2. PN-EN ISO/IEC 27001:2017-06 Systemy zarządzania bezpieczeństwem informacji – Wymagania.
3. PN-EN ISO/IEC 27002:2017-06 Praktyczne zasady zabezpieczania informacji.
4. PN ISO/IEC 27005:2014-12 Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.
5. PN-ISO/IEC 27018:2017-07 Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII.
6. PN-EN ISO/IEC 27799:2016-10 Informatyka w ochronie zdrowia - Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002.
7. PN–ISO 31000:2012 Zarzadzanie ryzykiem zasady i wytyczne.
8. PN-EN ISO 22301:2014-11 Systemy zarządzania ciągłością działania – Wymagania.
9. PN-ISO/IEC 29100:2017-07 Techniki bezpieczeństwa – Ramy prywatności.
10. PN-ISO/IEC 29101:2017-07 Techniki bezpieczeństwa – Ramy architektury i prywatności.
11. PN-ISO/IEC 29134:2017- Techniki bezpieczeństwa – Wytyczne dotyczące oceny wpływu na prywatność.
12. PN-ISO/IEC 29151:2017- Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania PII.

W przypadku wydania normy zastępującej którąkolwiek z norm wskazanych powyżej uwzględnia się nową normę.

Załącznik nr 7

8.7. Rekomendacje w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania danych w podmiotach wykonujących działalność leczniczą, w których przetwarzanie danych nie jest uznane za przetwarzanie na dużą skalę

1. Wprowadzenie

Niniejsze rekomendacje opisują minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania danych osobowych w tym danych szczególnej kategorii przez Podmiot wykonujący działalność leczniczą, który:

a) nie przetwarza danych na dużą skalę o którym to przetwarzaniu mowa w art. 35 ust. 3 lit. b) RODO oraz jednocześnie;

b) jest PWDL prowadzonym w formie indywidualnej lub grupowej praktyki zawodowej.

Zasadne jest zaproponowanie odrębnych, uproszczonych wymogów dla wskazanej wyżej grupy PWDL, ze względu na to, iż:

a) są to niewielkie podmioty realizujące typowe i powtarzalne procesy (czynności) przetwarzania danych osobowych;
b) są to podmioty zazwyczaj nieposiadające zasobów i profesjonalnej wiedzy dotyczącej przetwarzania i zabezpieczania danych osobowych;
c) zróżnicowanie wymogów ułatwi stosowanie przez wskazane wyżej PWDL zapisów Kodeksu i uzyskanie statusu podmiotu przestrzegającego Kodeksu.

Podmiot wykonujący działalność leczniczą gdzie nie dochodzi do przetwarzania danych na dużą skalę najczęściej charakteryzuje się tym, że przetwarzanie danych bardzo często odbywa się w gabinetach prywatnych, często współdzielonych, jak również w mieszkaniach prywatnych.

Podmiot wykonujący taką działalność osobiście odpowiedzialny jest za obszar, w którym przetwarza dane oraz za infrastrukturę informatyczną, tj. sprzęt, oprogramowanie, odpowiednie pomieszczenia do przechowywania danych, oraz za zapewnienie obsługi systemu teleinformatycznego i infrastruktury sprzętowej.

W związku z powyższym Podmiot wykonujący działalność leczniczą jest odpowiedzialny za wszystkie działania opisane w poniższych punktach niniejszego załącznika.

2. Organizacja bezpieczeństwa informacji

2.1. Polityka Bezpieczeństwa Danych

W podmiocie wykonującym działalność leczniczą, powinny być stosowane zasady bezpieczeństwa, które obejmują działania związane z identyfikacją, szacowaniem, kontrolą, przeciwdziałaniem i monitorowaniem ryzyka związanego z przetwarzaniem informacji.

Podstawowym dokumentem opisującym przetwarzanie informacji jest polityka bezpieczeństwa danych. Opisane w polityce zasady bezpieczeństwa, powinny być oparte na przyjętych regulacjach wewnętrznych.

Polityka bezpieczeństwa oraz pozostałe dokumenty związane z procesem zarządzania ryzykiem powinny być przedmiotem systematycznych przeglądów, mających na celu wprowadzenie ewentualnych usprawnień.

PWDL zobowiązany jest do posiadania Polityki Bezpieczeństwa.

Polityka bezpieczeństwa zawiera w szczególności: zakres stosowania, podział odpowiedzialności, dobór środków organizacyjnych i technicznych zapewniających bezpieczeństwo danych, sposób reakcji na incydenty i zgłaszania naruszeń, sposoby podnoszenia kompetencji w obszarze ochrony danych osobowych.

2.2. Identyfikacja ryzyka i analiza zagrożeń

a) Celem identyfikacji ryzyka w zakresie bezpieczeństwa przetwarzanych danych jest określenie związanych z nim zagrożeń mogących spowodować naruszenie atrybutów bezpieczeństwa przetwarzania (poufność, integralność, dostępność) oraz określenie gdzie, z jakim prawdopodobieństwem, w jaki sposób i dlaczego te zagrożenia mogą się zmaterializować.

b) PWDL zobowiązane są do dokonania co najmniej uproszczonej oceny ryzyka polegającej na uzupełnieniu wskazanej tabeli skupiającej się na zagrożeniach i przeciwdziałaniu zagrożeniom.

Minimalny katalog zagrożeń naruszenie praw lub wolności osób fizycznych, który musi zostać przeanalizowany przez PWDL.	**Opis zabezpieczeń wprowadzonych w celu minimalizacji ryzyka zmaterializowania się zagrożeń (z uwzględnieniem ochrony zasobów).**	**Uzasadnienie, dlaczego zastosowane zabezpieczenia są wystarczające do minimalizacji ryzyka - nie jest zasadne podejmowanie dodatkowych działań.**
Przypadkowe lub niezgodne z prawem zniszczenie danych		
Utracenie danych		

Nieuprawnione zmodyfikowanie danych		
Nieuprawnione ujawnienie danych		
Nieuprawniony dostęp do danych osobowych przesyłanych		
Nieuprawniony dostęp do danych przechowywanych		
Nieuprawniony sposób przetwarzania danych		
Brak podstawy prawnej do przetwarzania danych osobowych lub wskazana podstawa prawna nie jest jednoznaczna.		

c) Wskazana w poprzednim punkcie tabela podlega przeglądowi i ocenie co najmniej raz do roku bądź też obowiązkowo niezwłocznie po każdym zgłoszeniu naruszenia ochrony danych osobowych zgodnie z art. 33 RODO.
d) Wyniki przeprowadzonej analizy ryzyka powinny zostać przyjęte przez kierownictwo PWDL.
e) PWDL dokumentuje proces przeglądu i oceny, o którym mowa w pkt. c.

3. Bezpieczeństwo fizyczne i środowiskowe

3.1. Na podstawie analizy ryzyka, którego obowiązek przeprowadzenia wynika art. 32 RODO, przeprowadzonej zgodnie z załącznikiem X do Kodeksu bądź przy wykorzystaniu równoważnej metodyki bądź zgodnie z punktem 2.2.2. każdy PWDL ma obowiązek wdrożenia odpowiednich środków bezpieczeństwa spośród określonych w niniejszym rozdziale, PWDL może zastosować inne zabezpieczenia zastępujące zabezpieczenia określone w niniejszym rozdziale, jeśli wykaże, że zapewniają one co najmniej taki sam poziom bezpieczeństwa

3.2. W zakresie ochrony fizycznej należy wprowadzić podział na strefy w zależności od ich dostępności zarówno dla osób współpracujących, jak i Pacjentów.

3.3. Obszar, w którym przetwarzane są dane osobowe w tym dane medyczne, zabezpieczony musi być przed dostępem osób nieuprawnionych na czas nieobecności w nim osób

upoważnionych do przetwarzania danych. Przebywanie osób nieuprawnionych w obszarze, w którym przetwarza się dane osobowe, możliwe jest jedynie za zgodą lekarza lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

3.4. Minimalnymi środkami ochrony fizycznej w zakresie bezpieczeństwa danych osobowych są:

a) Przetwarzanie odbywa się w pomieszczeniu zabezpieczonym drzwiami wyposażonymi w zabezpieczenie w postaci zamka lub kontrolę dostępu,

b) Dane osobowe przetwarzane w postaci papierowej powinny być przechowywane w szafie wyposażonej w zabezpieczenie w postaci zamka i/lub kontrolę dostępu,

c) Kopie zapasowe/archiwalne zbioru danych przechowywane powinny być są w zamkniętej szafie spełniającej wymagania wskazane w pkt. 2, zlokalizowanej w innym miejscu niż obszar przetwarzania spełniającym wymagania wskazane w pkt. 1, w przypadku danych w formie elektronicznej ten wymóg spełniony jest również w przypadku przechowywania kopii zapasowej dokumentacji na bezpiecznym serwerze zlokalizowanym poza obszarem przetwarzania (np. w bezpiecznej chmurze obliczeniowej dostarczanej przez zewnętrznego dostawcę).

d) Pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone powinno być przed skutkami pożaru co najmniej za pomocą wolnostojącej gaśnicy, której miejsce przechowywania jest odpowiednio oznaczone.

e) Jeśli pomieszczenie, w którym przechowywana jest na stałe[77] dokumentacja medyczna wyposażone jest w okna, to powinny być one zabezpieczone folią antywłamaniową lub kratami.

3.5. Przy pierwszym wejściu do obszaru przetwarzania w danym dniu należy upewnić, się czy nie są widoczne ślady ingerencji osób trzecich, pożaru, zalania lub innego uszkodzenia.

3.6. Dokumenty zawierające dane osobowe po ustaniu przydatności powinny być niszczone w sposób mechaniczny za pomocą niszczarek dokumentów lub deponowane w dedykowanych pojemnikach przeznaczonych do utylizacji dokumentów obsługiwanych przez firmę specjalizującą się w utylizacji dokumentów papierowych/nośników danych.

3.7. PWDL zobowiązany jest do wdrożenia środków pozwalających na uniknięcie zniszczeń od pożaru, zalania, wybuchu oraz form katastrof naturalnych lub innych działań spowodowanych przez człowieka. PWDL opisuje wskazane środki w analizie ryzyka wraz z uzasadnieniem skorzystania z nich78.

3.8. W obszarach przetwarzania danych medycznych prace wykonywane przez osoby nieupoważnione, a także obecność tych osób mogą odbywać się wyłącznie pod nadzorem z powodów bezpieczeństwa, jak i z uwagi na uniemożliwienie złośliwych działań.

---

[77] Np. archiwum w którym przechowywana jest dokumentacja medyczna, nie oznacza to konieczności zapezpieczenia we wskazany sposób wszystkich pomieszczeń w których okazjonalnie w trakcie dnia znajduje się dokumentacja medyczna.

[78] Rekomenduje się (choć nie jest to obowiązkowe) korzystanie ze specjalistycznego doradztwa w kwestii tego, jak uniknąć zniszczeń wynikających z przedstawionych wyżej zdarzeń.

3.9. Nie wolno dopuszczać do korzystania z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, np. kamer w urządzeniach przenośnych, w obszarach przetwarzania danych chyba że osoba ma odpowiednie upoważnienie.

3.10. Celem zabezpieczenia sprzętu jest zapobieżenie utracie, uszkodzeniu oraz kradzieży.

3.11. Należy umieścić i chronić sprzęt w taki sposób, aby zminimalizować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz przypadków nieuprawnionego dostępu.

3.12. W celu ochrony sprzętu należy:

a) umieścić sprzęt w taki sposób, aby zminimalizować ryzyko niepotrzebnego dostępu do sprzętu przez osoby nieuprawnione;

b) tak ulokować ekrany komputerowe, aby podczas ich użycia minimalizować ryzyko podglądu przez nieuprawnione osoby,

c) wprowadzić zabezpieczenia minimalizujące ryzyko związane z potencjalnymi zagrożeniami fizycznymi i środowiskowymi, np. kradzieżą, pożarem, dymem, zalaniem i wandalizmem. Pkt. 2.6. stosuje się odpowiednio.

d) wprowadzić procedury związane ze spożywaniem posiłków, napojów oraz paleniem tytoniu w bliskim sąsiedztwie środków przetwarzania danych osobowych – wskazany warunek jest spełniony poprzez wprowadzenie i przestrzeganie zasady zakazu spożywania napojów i płynnych posiłków oraz palenia przy urządzeniach i nośnikach danych.

e) Zapewnić konserwację sprzętu zgodnie z zaleceniami dostawcy, w zakresie częstotliwości i zakresu, naprawianie lub serwisowanie sprzętu tylko przez autoryzowany personel.

f) wprowadzenie odpowiednich zabezpieczeń na czas czynności konserwacyjnych, z uwzględnieniem działań przeprowadzanych przez personel na miejscu lub poza siedzibą organizacji; jeśli zachodzi taka potrzeba i jest to możliwe i zasadne, przed przekazanie do serwisu urządzeń należy wymontować nośniki informacji (dyski twarde)

g) Należy pamiętać o skontrolowaniu urządzenia przed jego ponownym uruchomieniem, po przeprowadzeniu jego konserwacji, w celu zapewnienia, że sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji.

h) Przed podjęciem pracy należy sprawdzić czy sprzęt jest kompletny, nieuszkodzony, czy nie znajdują się na nim ślady zewnętrznej ingerencji

i) sprzęt nie może być pozostawiany w miejscach publicznych bez nadzoru,

j) PWDL zobowiązany jest przestrzegać instrukcji producenta dotyczących ochrony sprzętu, np. ochrony przed wystawieniem na działanie silnego pola elektromagnetycznego.

k) uwzględnić faktże ryzyka np. uszkodzeń, kradzieży lub podsłuchu, mogą znacząco różnić się w zależności od miejsca. W przypadku wystąpienia ryzyka kradzieży, utraty sprzętu na którym przechowywane są istotne dane np. dane medyczne, informacje na sprzęcie powinny być przechowywane w formie zaszyfrowanej. Nie niweluje to ryzyka

kradzieży ale uniemożliwia dostęp do informacji osobom nieuprawnionym w przypadku utraty kontroli nad urządzeniem.

3.13. Pozostawiając sprzęt bez opieki należy:

a) zamykać aktywne sesje po zakończeniu pracy, chyba że są one zabezpieczane przez odpowiedni mechanizm blokujący, np. wygaszacz ekranu chroniony hasłem;

b) wyrejestrowywać się z aplikacji lub usług sieciowych, kiedy nie są już więcej potrzebne;

c) zabezpieczać nieużywane w danym momencie komputery osobiste lub urządzenia mobilne przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób, np. dostęp do komputera po podaniu hasła.

3.14. należy wprowadzić i stosować Politykę czystego biurka i czystego ekranu dla dokumentów papierowych i przenośnych nośników pamięci oraz politykę czystego ekranu dla środków przetwarzania informacji.

Zaleca się rozważenie wprowadzenia następujących rozwiązań organizacyjnych: należy niezwłoczne usuwać z drukarek wydruków zawierających dane osobowe i dane istotne dla ochrony danych osobowych.

3.15. W systemie informatycznym służącym do przetwarzania danych osobowych zastosowane muszą być mechanizmy kontroli dostępu do tych danych,

3.16. W przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, zapewnione musi być, aby:

a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;

b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.

3.17. zapewnić należy aby identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie.

3.18. W przypadku gdy do uwierzytelniania użytkowników używa się hasła powinno ono zawierć małe i wielkie litery oraz cyfry lub znaki specjalne. Jego długość i częstotliwość zmiany wskazana powinna być w Polityce bezpieczeństwa.

3.19. System informatyczny służący do przetwarzania danych osobowych zabezpieczony musi być, co najmniej przed:

a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;

b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

3.20. Dane osobowe przetwarzane w systemie informatycznym zabezpieczone muszą być przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.

3.21. Kopie zapasowe muszą być:

a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
b) przechowywane jeżeli to możliwe w formie zaszyfrowanej;
c) usuwane niezwłocznie po ustaniu ich użyteczności.

3.22. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
a) likwidacji — muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — muszą zostać pozbawione wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
c) naprawy — muszą zostać, jeśli jest to możliwe lub zasadne z punktu widzenia naprawy pozbawione wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora lub Podmiotu przetwarzającego, z którym PWDL zawarł umowę zgodnie z at. 28 RODO.

3.23. Systemy informatyczne służące do przetwarzania danych osobowych muszą być chronione przed zagrożeniami pochodzącymi z sieci publicznej poprzez co najmniej stosowanie oprogramowania antywirusowego.

3.24. Dla zapewnienia bezpieczeństwa systemu oraz danych osobowych należy obligatoryjnie stosować ochronę przed kodem złośliwym. Zaleca się wdrożenie oprogramowania antywirusowego, które umożliwiałoby automatyczną aktualizację oraz posiadało możliwość centralnego zarządzania i raportowania lub też aktualizacje te odbywały się na podstawie odrębnych procedur. Zaleca się aby oprogramowanie to umożliwiało w szczególności:
a) Zmianę ustawień konfiguracyjnych;
b) Możliwość zdalnej instalacji przez Administratora lub instalacje automatyczną w momencie podłączania się komputera do sieci;
c) Automatyczną aktualizację;
d) Wymuszenie skanowania.

3.25. Oprogramowanie antywirusowe musi być regularnie aktualizowane (ręcznie lub automatyczne), zgodnie z zaleceniami producenta:
a) W zakresie definicji wirusów oraz sygnatur antywirusowych okresowo, przynajmniej raz w tygodniu;
b) W zakresie oprogramowania – niezwłocznie po opublikowaniu przez producenta aktualizacji bezpieczeństwa.

3.26. Niezbędne jest regularne skanowanie komputerów przy pomocy oprogramowania antywirusowego.

3.27. Obowiązkowy przegląd, wybór metod i środków ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana oraz przygotowanie i realizacja planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na nowe informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Wprowadzenie przetwarzania Dokumentacji medycznej w postaci elektronicznej wiąże się z wprowadzeniem mechanizmów utrzymania tej dokumentacji. Utrzymanie to nie tylko ochrona danych przed utratą, nieuprawnionym odczytem i zmianą, ale również, podobnie jak dotychczas w przypadku prowadzenia dokumentacji w postaci papierowej, dbałość o przechowywanie i możliwość jej odczytu. W początkowym okresie problem odczytu nie będzie aż tak istotny, jednak tempo rozwoju technologii spowoduje potrzebę konwersji Dokumentacji medycznej z obecnych, uznanych dzisiaj jako standardy formatów danych do nowych. W przypadku dokonania np. zmian w infrastrukturze systemowo-sprzętowej istotne jest, aby dane z archiwum przenieść na nośniki fizyczne, z których będzie można pozyskać dane zapisane wcześniej. Istotna jest tu zarówno zgodność sprzętowa rozwiązań, jak również zabezpieczenie przed skutkami utraty trwałości nośnika wynikającymi z upływającego czasu czy też zużycia. Dlatego obowiązkowe jest regularne dokonywanie przeglądów wymagań i wytycznych w zakresie przetwarzania Dokumentacji medycznej w postaci elektronicznej i wprowadzanie wynikających z nich zmian.

3.28. **Zapewnienie monitorowania i aktualizacji zastosowanych środków bezpieczeństwa, wprowadzenie spójnych i egzekwowalnych zasad.**

PWDL zobowiązany jest do wprowadzenia cyklicznego monitorowania przestrzegania zasad ochrony danych osobowych wskazanych w niniejszym załączniku i w Kodeksie, a także do wprowadzenia regulaminowo określonych sankcji za ich naruszenie.

3.29. **Utrzymanie i konserwacja infrastruktury teleinformatycznej.**

Realizując zadanie utrzymania systemu teleinformatycznego wspomagającego obsługę przetwarzania Dokumentacji medycznej będącej w postaci elektronicznej lub w przypadku mniejszych jednostek, które korzystają z usług zewnętrznych, należy w odpowiedni sposób zadbać o jakość posiadanej infrastruktury teleinformatycznej i zabezpieczyć się na wypadek uszkodzenia. Obowiązek ten można spełnić w szczególności poprzezposiadanie umów serwisowych z podmiotami zewnętrznymi, które gwarantują konserwację, dostępność i wymianę sprzętu oraz oprogramowania w krótkim, nie wpływającym na poziom obsługi Pacjentów czasie. Należy również wykazywać się daleko idąca dbałością o aktualizację i wymianę sprzętu po okresie jego używalności. Ma to bezpośrednie przełożenie na bezpieczeństwo i niezawodność realizowanych usług.

Załącznik nr 8

8.8. Wzór oświadczenia o spełnieniu wymogów wynikających z Kodeksu

Dane PWDL/ Podmiotu przetwarzającego (dalej: „Podmiot")

Firma, nazwa albo imię i nazwisko podmiotu leczniczego/ Podmiotu przetwarzającego:

Adres siedziby podmiotu leczniczego/ Podmiotu przetwarzającego, a w przypadku osoby fizycznej – adres do korespondencji:

Numer księgi rejestrowej (rejestr PWDL), jeśli dotyczy

Numer Krajowego Rejestru Sądowego, jeśli dotyczy

Numer telefonu kontaktowego:

Adres e-mail:

Data złożenia oświadczenia:

Działając na podstawie pkt 7.3.1. Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dotyczącego Podmiotów wykonujących działalność leczniczą oraz Podmiotów przetwarzających i zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych w dniu ___ niniejszym w imieniu Podmiotu oświadczam, iż w odniesieniu do:

☐ Całości działalności prowadzonej w charakterze Podmiotu przetwarzającego objętej zakresem Kodeksu

☐ Całości prowadzonej działalności leczniczej objętej zakresem Kodeksu

☐ Działalności leczniczej prowadzonej w ramach wskazanego/wskazanych zakładów leczniczych objętej zakresem Kodeksu[79]:

.....

.....

Podmiot spełnia wszystkie wymagania nałożone na niego zapisami Kodeksu i tym samym chce uzyskać tytuł Podmiotu przestrzegającego Kodeksu. Tym samym zobowiązuje się do spełniania wszelkich nałożonych przez Kodeks obowiązków, w szczególności do zapewnienia odpowiedniej ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

_____

Podpis osoby lub osób upoważnionych do reprezentacji Podmiotu.

Spis załączników do Oświadczenia:

1) Kwestionariusz odnoszący się do poszczególnych obowiązków wynikających z Kodeksu (załącznik nr 10 do Kodeksu);
2) Pozytywna opinia wydana przez Inspektora Ochrony Danych (jeśli został powołany) lub inny podmiot dysponujący odpowiednim poziomem wiedzy fachowej w dziedzinie będącej przedmiotem Kodeksu, stwierdzającą spełnianie przez PWDL lub Podmiot przetwarzający wymogów Kodeksu.

[79]Należy podać nazwę i adres zakładu leczniczego zgodnie z rejestrem PWDL.

Załącznik nr 9

8.9. Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu

Dane PWDL/ Podmiotu przetwarzającego (dalej: „Wnioskodawca")

Firma, nazwa albo imię i nazwisko podmiotu leczniczego/ Podmiotu przetwarzającego:

Adres siedziby podmiotu leczniczego/ Podmiotu przetwarzającego, a w przypadku osoby fizycznej – adres do korespondencji:

Numer księgi rejestrowej (rejestr PWDL), jeśli dotyczy

Numer Krajowego Rejestru Sądowego, jeśli dotyczy

Numer telefonu kontaktowego:

Adres e-mail:

Nazwa Podmiotu monitorującego, do którego składany jest wniosek:

Data złożenia wniosku:

Działając na podstawie pkt 7.4.1. Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dotyczącego Podmiotów wykonujących działalność leczniczą i Podmiotów przetwarzających i zatwierdzonego przez Prezesa Urzędu Ochrony Danych Osobowych w dniu ___ niniejszym w imieniu Wnioskodawcy w odniesieniu do:

☐ Całości działalności prowadzonej w charakterze Podmiotu przetwarzającego objętej zakresem Kodeksu

☐ Całości prowadzonej działalności leczniczej objętej zakresem Kodeksu

☐ Działalności leczniczej prowadzonej w ramach wskazanego/wskazanych zakładów leczniczych objętej zakresem Kodeksu[80]

.....

.....

wnioskuję o uzyskanie przez Wnioskodawcę statusu Podmiotu przestrzegającego Kodeksu i jedocześnie oświadczam, iż Wnioskodawca deklaruje gotowość do poddania się audytowi wstępnemu zgodnie z pkt. 7.4.5. Kodeksu, a także w przypadku uzyskania tego statusu zobowiązuje się do spełniania wszelkich nałożonych przez Kodeks obowiązków, w szczególności do zapewnienia odpowiedniej ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

_____

Podpis osoby lub osób upoważnionych do reprezentacji Wnioskodawcy.

Spis załączników do Oświadczenia:

1) Kwestionariusz odnoszący się do poszczególnych obowiązków wynikających z Kodeksu (załącznik nr 10 do Kodeksu);
2) **Fakultatywnie:** Pozytywna opinia wydana przez Inspektora Ochrony Danych (jeśli został powołany) lub inny podmiot dysponujący odpowiednim poziomem wiedzy fachowej

[80] Należy podać nazwę i adres zakładu leczniczego zgodnie z rejestrem PWDL.

w dziedzinie będącej przedmiotem Kodeksu, stwierdzającą spełnianie przez PWDL lub Podmiot przetwarzający wymogów Kodeksu.

Załacznik nr 10

8.10. Wzór kwestionariusza, który dołącza się do oświadczenia, o którym mowa w załączniku nr 8 lub wniosku, o którym mowa w załączniku nr 9

Wymóg wynikający z Kodeksu	Kogo dotyczy (PWDL/ Podmiot przetwarzający/ oba)	Wyjaśnienia do wymogu	Wskazanie w jaki sposób wymóg został spełniony (wypełnia Podmiot składający oświadczenie lub wniosek)[81]
Prawidłowe określenie celów i podstaw prawnych przetwarzania	PWDL	Należy ocenić m.in. treści obowiązków informacyjnych, rejestrów czynności przetwarzania, sprawdzić zasadność pobierania zgody	
Prawidłowy zakres przetwarzania danych, dla którego podstawą nie jest zgoda	PWDL	Należy w szczególności zweryfikować, czy zakres przetwarzanych danych jest adekwatny, stosowny i ograniczony dla celów przetwarzania	
Prawidłowy zakres przetwarzania danych, dla którego podstawą nie jest zgoda	PWDL	Należy w szczególności zwrócić uwagę na zasadność wykorzystania zgody jako podstawy prawnej przetwarzania danych w danym procesie, należy ocenić prawidłowość zbieranych zgód w stosunku do procesu przetwarzania, a także procedurę i okoliczności jej gromadzenia (zapewnienie swobody, niewykorzystywanie stosunku zależności) oraz wycofywania (zwłaszcza łatwość wycofania), sposób realizacji zasady rozliczalności w odniesieniu do zgody	

[81]Należy w sposób syntetyczny wskazać sposób wypełnienia obowiązku, jeśli jest to celowe i zasadne należy również odnieść się do dokumentacji wdrożonej przez podmiot, takiej jak posiadane procedury, czy wzory.

Prawidłowa identyfikacja podmiotów jako Podmioty przetwarzające/ administratorzy/ osoby przetwarzające dane z upoważnienia.	Oba*	Należy w szczególności zwrócić uwagę, czy podmiot odpowiednio identyfikuje w zawartych przez siebie umowach role i obwiązki związane z przetwarzaniem danych, w tym czy zawiera umowy powierzenia przetwarzania danych z właściwymi podmiotami. Uwaga: możliwe jest uznanie wskazanego wymogu za spełniony przez PWDL, jeżeli występują łącznie następujące okoliczności: a) ilość zawartych umów, w których zastosowano niewłaściwą klasyfikację jest niewielka (mniejsza niż 20% wszystkich umów związanych z przetwarzaniem danych, których stroną jest podmiot); b) nie jest możliwa zmiana lub rozwiązanie wskazanych umów bez poniesienia istotnego uszczerbku przez PWDL i jednocześnie PWDL oświadcza, że wskazane umowy ulegną rozwiązaniu lub zmianie nie później niż w ciągu roku od dnia złożenia oświadczenia; c) odstępstwo od wskazanego wymogu nie stwarza istotnego ryzyka naruszenia praw i wolności osób w związku z przetwarzaniem ich danych osobowych. *w odniesieniu do Podmiotów przetwarzających należy sprawdzić, czy prawidłowo ustalają swoją rolę w procesie (jako Podmioty przetwarzające), w przypadku nieprawidłowej identyfikacji	

		nie jest możliwe uzyskanie statusu Podmiotu przestrzegającego Kodeksu.	
Prawidłowe zarządzanie zasadami dostępu personelu do danych osobowych Pacjentów	PWDL	Należy ocenić, w szczególności celowość i niezbędność dostępu danych osobowych Pacjentów ze względu na zadania personelu. Należy zwrócić uwagę, czy te same zadania mogłyby być realizowane bez dostępu do danych, w szczególności do danych sensytywnych. Należy zweryfikować prawidłowość nadawania upoważnień.	
Prawidłowe udostępnianie Dokumentacji medycznej	Oba*	Należy w szczególności ocenić sposób udostępniania Dokumentacji medycznej, treść upoważnienia do dostępu do Dokumentacji medycznej itp. *wskazany wymóg można analizować w odniesieniu do Podmiotów przetwarzających, które dostarczają rozwiązania techniczne i/lub organizacyjne i uczestniczą w procesie udostępniania Dokumentacji medycznej[82].	
Prawidłowa anonimizacja lub pseudonimizacja danych przed udostępnieniem podmiotom trzecim	PWDL	Należy w szczególności zweryfikować, czy w przypadku udostępnienia danych podmiotom trzecim, które nie są upoważnione do dostępu do danych osobowych dane zostały poddane skutecznej anonimizacji lub pseudonimizacji, której odwrócenie przez osobę trzecią byłoby niemożliwie bez uzyskania dodatkowych informacji prawnie chronionych w sposób niezgodny z prawem	
Udostępnianie danych	PWDL	Należy w szczególności zweryfikować,	

[82]W przypadku Podmiotów przetwarzających, które nie przetwarzają danych w ramach procesu ich udostępniania podmiotom trzecim, w kolumnie obok należy wpisać: „nie dotyczy".

osobowych Pacjentów osobom trzecim w stanie wyższej konieczności, które to osoby nie są upoważnione do dostępu do danych na podstawie przepisów polskiego prawa medycznego (na podstawie art. 9 ust. 2 lit c. RODO)		czy istnieje procedura/ zasady informowania osób trzecich w stanie wyższej konieczności, czy zasady te są zgodne z zapisami Kodeksu.	
Postępowanie w wybranych sytuacjach związanych ze zwiększonym ryzykiem naruszenia praw Pacjentów w związku z przetwarzaniem danych osobowych	PWDL	Należy zweryfikować, czy podmiot wdrożył zalecenia wskazane w załączniku nr 3 do Kodeksu	
Weryfikacja czy podmiot jest zobowiązany do powołania IOD i czy powołał IOD	PWDL	Należy w szczególności zweryfikować, czy PWDL przetwarza dane na dużą skalę zgodnie z Kodeksem	
Weryfikacja, czy podmiot zapewnia bezpieczeństwo ochrony danych osobowych	Oba	Należy w szczególności zweryfikować, czy podmiot prawidłowo oszacował poziom ryzyka i czy wdrożył odpowiednie środki zaradcze. Możliwe jest wykorzystanie własnej metodyki analizy ryzyka i własnych zabezpieczeń, przy czym PWDL lub Podmiot przetwarzający muszą wykazać, że przyjęta metodyka zapewnia co najmniej taki sam poziom bezpieczeństwa jak wskazany w Kodeksie.	

Weryfikacja, czy podmiot prowadzi w sposób odpowiedni ocenę skutków dla ochrony danych	Oba*	Należy w szczególności zweryfikować, czy podmiot prawidłowo zweryfikował procesy wymagające przeprowadzenia oceny skutków, a także, czy podmiot prawidłowo oszacował poziom ryzyka i czy wdrożył odpowiednie środki zaradcze. Możliwe jest wykorzystanie własnej metodyki analizy ryzyka i własnych zabezpieczeń, przy czym PWDL lub Podmiot przetwarzający muszą wykazać, że przyjęta metodyka zapewnia co najmniej taki sam poziom bezpieczeństwa jak wskazany w Kodeksie. *w odniesieniu do Podmiotu przetwarzającego weryfikacji podlega spełnienie wymogu wskazanego w pkt. 5.3.6.	
Weryfikacja zasad powierzenia przetwarzania danych	Oba*	W odniesieniu do PWDL należy w szczególności zweryfikować, czy PWDL dokonuje oceny Podmiotów przetwarzających i czy korzysta z usług Podmiotów przetwarzających dających wystarczające gwarancje bezpieczeństwa, należy również zweryfikować czy umowa powierzenia przetwarzania spełnia wymogi określone w RODO, a także czy zapewnia niezakłócone korzystanie z usług oraz możliwość przeprowadzenia audytu zgodnie z Kodeksem. *w odniesieniu do Podmiotu przetwarzającego, należy zweryfikować zawierane przez ten podmiot umowy, ale tylko jeżeli ten podmiot korzysta z przygotowanych przez siebie wystandaryzowanych wzorów umów powierzenia przetwarzania, (odniesienie	

		do tych wzorów musi zostać wskazane w ostatniej kolumnie[83]), należy również ocenić relacje tego podmiotu z podprocesorami). Należy w szczególności ocenić spełnienie punktu 5.4.6., 5.4.8. i 5.4.9. Kodeksu. Należy zweryfikować czy Podmiot przetwarzający zapewnia niezakłócone korzystanie z usług przetwarzania danych. Zmiany we wzorach, które nie są istotne z punktu widzenia ochrony danych osobowych nie wymagają zgłoszenia Komitetowi sterującemu.	
Zapewnienie odpowiedniego poziomu wiedzy dotyczącej bezpieczeństwa danych osobowych	Oba	Należy w szczególności zweryfikować poziom wiedzy personelu przetwarzającego danc osobowc, nalcży również zweryfikować czy PWDL lub Podmiot przetwarzający prowadzą udokumentowane i cykliczne działania w obszarze zwiększenia wiedzy w zakresie bezpieczeństwa danych osobowych.	
Zapewnienie właściwej realizacji praw Pacjentów jako podmiotów danych	PWDL	Należy w szczególności zweryfikować zarówno ogólne kwestie dotyczące realizacji praw, takie jak sposób ustalenia tożsamości Pacjenta, czy forma przekazywania informacji Pacjentowi, jak również należy odnieść się szczegółowo do wszystkich praw i obowiązków wskazanych w Kodeksie (art. 13, 14, 15, 16, 17 , 18, 20, 21 RODO)	
Zgodność z prawem procesów wykorzystujących profilowanie lub inne	PWDL	Należy w szczególności ocenić, czy PWDL podejmuje decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu danych, które to decyzje	

[83]Np.w kolumnie obok należy wskazać link pod którym można pobrać wzór umowy ze wskazaniem jakiej wersji dotyczy oświadczenie.

zautomatyzowane przetwarzanie danych		istotnie wpływają na Pacjentów lub osoby trzecie i zweryfikować zgodność z prawem takiego przetwarzania.	

Załącznik nr 2 do wniosku

Warszawa, 13 listopada 2018 r.

RAPORT Z KONSULTACJI PUBLICZNYCH DOTYCZĄCY PROJEKTU „KODEKSU BRANŻOWEGO DLA SEKTORA OCHRONY ZDROWIA" PRZYGOTOWANEGO W RAMACH INICJATYWY WWW.RODOWZDROWIU.PL" (DALEJ: „KODEKS")

1. CEL DOKUMENTU

W art. 40 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 (dalej: „RODO" lub „Rozporządzenie") państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych oraz Komisja zachęcają do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu Rozporządzenia - z uwzględnieniem specyfiki różnych sektorów dokonujących przetwarzania oraz szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

Zgodnie z motywem 99 RODO „Sporządzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji". Dodatkowo zgodnie z art. 27 ust 2, ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych (dalej: UODO) **„Kodeks postępowania przed przekazaniem do zatwierdzenia Prezesowi Urzędu podlega konsultacjom z zainteresowanymi podmiotami"**, natomiast ust. 3 obliguje wnioskodawcę przedkładającego kodeks do zatwierdzenia, do **przedłożenia Prezesowi Urzędu Ochrony Danych Osobowych informacji o przeprowadzonych konsultacjach. Niniejszy raport ma na celu uczynienie zadość wskazanemu wymogowi i opisuje przebieg szeroko prowadzonych konsultacji publicznych kolejnych wersji Kodeksu.**

Projekt Kodeksu powstał na podstawie przywołanego art. 40 RODO i jest efektem współpracy dziesiątek podmiotów reprezentujących administratorów i podmioty przetwarzające w rozumieniu przepisów RODO. Zgodnie z początkowym założeniem w opracowywaniu i konsultacjach Kodeksu brały udział centralne organy administracji publicznej, jednostki samorządu terytorialnego, przedsiębiorcy, organizacje pacjenckie, samorządy zawodowe i wiele innych podmiotów.

Prace nad treścią Kodeksu trwały od lipca 2017 r. do listopada br. i od samego początku prowadzone były w szerokim gronie interesariuszy. W trakcie prawie półtorarocznej pracy przeprowadzono dziesiątki spotkań, telekonferencji, warsztatów, a także zorganizowano nieodpłatną ogólnopolską konferencję, w której uczestniczyło ponad 550 osób, a także prowadzono newsletter na stronie www.rodowzdrowiu.pl. Poza organizacją spotkań przeanalizowano również setki stanowisk, które pochodziły zarówno od osób fizycznych (pacjentów), personelu medycznego, placówek medycznych,

organizacji branżowych jak również ze strony samorządów zawodowych, czy też podmiotów publicznych. Swoje obszerne stanowiska złożyli przedstawiciele Naczelnej Izby Lekarskiej, Krajowej Izby Fizjoterapeutów oraz Centrum Systemów Informacyjnych Ochrony Zdrowia. Merytorycznie Kodeks był również konsultowany z przedstawicielami Ministerstwa Zdrowia i Rzecznikiem Praw Pacjenta.

W imieniu Polskiej Federacji Szpitali w związku ze złożeniem wniosku o akceptację Kodeksu do Prezesa Urzędu Ochrony Danych Osobowych pragniemy przedstawić szczegółowy raport z przeprowadzonych konsultacji publicznych dotyczący *„Kodeksu branżowego dla sektora ochrony zdrowia"*.

2. OGÓLNE ZAŁOŻENIA W ZAKRESIE PRACY NAD KODEKSEM

Komitet sterujący w trakcie prac nad Kodeksem kierował się następującymi głównymi zasadami:

a) **pełną transparentnością od samego początku prac nad projektem Kodeksu;**

b) **inkluzyjnością procesu tworzenia i konsultowania Kodeksu;**

Wskazane wyżej cele udało się zrealizować poprzez zapewnienie łatwego i nieodpłatnego dostępu do kolejnych wersji Kodeksu, a także umożliwienie udziału w pracach nad projektem Kodeksu i ustosunkowania się do niego szerokiemu gronu podmiotów. Twórcy Kodeksu mieli bowiem świadomość, że jedynie połączenie różnych punktów widzenia pozwoli na wypracowanie wspólnych rozwiązań akceptowanych dla większości branży medycznej, niezależnie od formy organizacyjnej, wielkości, czy przedmiotu działalności. W praktyce, poprzez aktualizację kolejnych wersji Kodeksu na stronie internetowej, rozsyłanie bieżących informacji w formie newslettera, prowadzenie konsultacji publicznych, Komitet sterujący zapewnił sobie szerokie wsparcie merytoryczne przy pracy nad Kodeksem. **Zwracamy uwagę, że w pracę nad Kodeksem, za pośrednictwem organizacji zrzeszających, włączona została zdecydowana większość osób wykonujących zawody medyczne, administratorów danych i podmiotów przetwarzających dane działających w sektorze medycznym. Tym samym Kodeks powinien być postrzegany jako dokument wypracowany przez reprezentatywną grupę podmiotów i powinien być postrzegany jako wyraz konsensusu kluczowych przedstawicieli branży medycznej w Polsce.**

3. PODMIOTY ZAANGAŻOWANE W PRACE NAD KODEKSEM

W prace nad Kodeksem włączyły się dziesiątki podmiotów i organizacji branżowych reprezentujących zarówno sektor publiczny jak i prywatny. Stanowiska i opinie w ramach konsultacji publicznych były na bieżąco analizowane. Poniżej pragniemy przedstawić katalog podmiotów, które przyczyniły się do powstania Kodeksu.

3.1 Komitet sterujący

Komitet sterujący (dalej: Komitet) współtworzą jedne z największych i najbardziej reprezentatywnych organizacji branżowych sektora ochrony zdrowia (obejmujące swym zasięgiem większość. rynku medycznego w Polsce), które podjęły solidarną decyzję o utworzeniu i opracowaniu Kodeksu. W skład Komitet sterującego wchodzi:

(a) **Polska Federacja Szpitali (dalej: PFSz)** - ogólnopolska organizacja pracodawców zrzeszająca i reprezentująca polskie szpitale na forum krajowym, a także międzynarodowym, do której należy około 250 szpitali z obszaru całego kraju. PFSz jest organizacją działającą na rzecz bezpieczeństwa pacjentów oraz pracowników szpitali, a także na rzecz jakości, dobrych praktyk zarządzania oraz dobrego ustawodawstwa;

(b) **Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie** (dalej: Porozumienie Zielonogórskie) - organizacja działająca w 15 województwach, skupiająca 13 tysięcy lekarzy sprawujących opiekę nad 12 milionami pacjentów, stanowiąca największą organizację pracodawców ochrony zdrowia w Polsce. Głównym celem Porozumienia Zielonogórskiego jest wspieranie działań mających na celu podnoszenie poziomu opieki zdrowotnej;

(c) **Telemedyczna Grupa Robocza (dalej: TGR)** - organizacja branżowa zrzeszająca interdyscyplinarny zespół świadczeniodawców, producentów wyrobów medycznych, dostawców usług IT oraz ekspertów prawno-medycznych działający wspólnie na rzecz rozwoju telemedycyny w Polsce. Celem TGR jest rozwój telemedycyny, a w szczególności zwiększenie bezpieczeństwa prawnego związanego z działalnością telemedyczną. W skład TGR wchodzi ok. 20 wiodących podmiotów świadczących usługi telemedyczne lub oferujących technologie telemedyczne.

(d) **Związek Pracodawców Technologii Cyfrowych Lewiatan (dalej: ZPTC Lewiatan)** - organizacja zrzeszająca grupę najaktywniejszych firm IT w Polsce. Lewiatan doskonale zna potrzeby, zagrożenia i wyzwania, jakie stoją przed podmiotami przetwarzającymi;

(e) **Organizacja Pracodawców Medycyny Prywatnej (dalej: Medycyna Prywatna)** - organizacja zrzeszająca prywatnych świadczeniodawców usług medycznych, wśród których znajdują się liderzy rynku pracowniczych programów zdrowotnych, spółki giełdowe oraz lokalni pracodawcy ochrony zdrowia. Cele i zadania Związku realizowane są m.in. przez prezentowanie opinii w sprawach związanych z ochroną zdrowia, organizowanie zespołów doradczych oraz współpracę z innymi organizacjami pozarządowymi o celach zbieżnych z celami Związku;

(f) **Polska Izba Informatyki i Telekomunikacji (dalej: PIIT)** - organizacja reprezentująca interesy gospodarcze firm przemysłu teleinformatycznego, realizująca światowej klasy cyfrowe produkty i usługi. PIIT pracuje na rzecz dobrych regulacji i procedur, które umożliwiają cyfrowy rozwój i modernizację Państwa, jej celem jest zapewnienie racjonalnych regulacji i wspieranie inicjatywy wdrażania cyfrowych innowacji oraz budowanie partnerskiej współpracy przemysłu teleinformatycznego i administracji publicznej;

W pracach nad Kodeksem swój udział ma również Kancelaria Domański Zakrzewski Palinka – jedna z największych polskich kancelarii, wielokrotnie wyróżniania w rankingach o zasięgu krajowym oraz międzynarodowym, posiadająca jedną z najlepiej ocenianych praktyk Life Sciences w Polsce. Chociaż Kancelaria formalnie nie należy do Komitetu sterującego to odpowiada za koordynację merytorycznych prac nad Kodeksem.

3.2 Podmioty publiczne i organizacje wspierające bezpośrednio pracujące nad Kodeksem

Kodeks był również przedstawiany i opiniowany na bieżąco przez szerokie grono podmiotów publicznych związanych z sektorem ochrony zdrowia. Dzięki otrzymanym stanowiskom strony publicznej, mogliśmy uwzględnić cenne uwagi przedstawione przez podmioty zaangażowane i tym samym wzbogacić treść Kodeksu. Podmiotami, które bezpośrednio włączyły się w prace nad Kodeksem były:

(a) **Centrum Systemów Informacyjnych Ochrony Zdrowia (dalej: „CSIOZ")** – państwowa jednostka budżetowa, która jest obecnie regulatorem rynku w zakresie rozwiązań teleinformatycznych. Głównym przedmiotem działalności CSIOZ jest realizacja zadań z zakresu budowy społeczeństwa informacyjnego, obejmujących organizację i ochronę zdrowia oraz wspomaganie decyzji zarządczych ministra właściwego do spraw zdrowia na podstawie prowadzonych analiz. **CSIOZ współtworzyło istotną część zapisów Kodeksu, w szczególności rozdział 5 Kodeksu dotyczący kwestii bezpieczeństwa przetwarzania danych osobowych. CSIOZ było również jednym z inicjatorów prac nad Kodeksem.**

(b) **Ministerstwo Zdrowia (dalej: „MZ")** – przedstawiciele MZ obecni byli w trakcie inauguracji prac nad Kodeksem, byli również obecni na kolejnych spotkaniach roboczych.

(c) **Naczelna Izba Lekarska (dalej: „NIL")** - samorząd lekarzy i lekarzy dentystów na szczeblu państwowym, reprezentujący racje stojące po stronie osób wykonujących zawód lekarza i lekarza dentysty. NIL prezentuje stanowisko samorządu i angażuje się w proces stanowienia aktów, mających szczególne znaczenie dla sektora medycznego. **Naczelna Izba Lekarska, zwłaszcza po wyborach do samorządu, wyjątkowo aktywnie włączyła się w prace nad Kodeksem, uczestnicząc w spotkaniach telekonferencjach a także przedstawiając kilka stanowisk w formie uchwał Prezydium NRL do kolejnych wersji Kodeksu.**

(d) Naczelna Izba Pielęgniarek i Położnych (dalej: „NIPiP") – samorząd zawodowy reprezentujący osoby wykonujące zawód pielęgniarki lub położnej. NIPiP była obecna w procesie tworzenia Kodeksu od samego początku.

(e) **Krajowa Izba Fizjoterapeutów (dalej: „KIF")** – samorząd zawodowy zrzeszający wszystkich polskich fizjoterapeutów z prawem wykonywania zawodu. KIF reprezentuje racje stojące po stronie fizjoterapeutów, obok NIL i NIPiP jest trzecim co do wielkości samorządem w Polsce;

(f) **Samorząd Województwa Wielkopolskiego** – podmiot tworzący dla ok. 20 podmiotów wykonujących działalność leczniczą, w tym Wojewódzkiego Szpitala dla Nerwowo i Psychicznie Chorych „Dziekanka" im. Aleksandra Piotrowskiego w Gnieźnie, Szpitala Wojewódzkiego w Poznaniu oraz Wielkopolskiego Centrum Onkologii im. Marii Skłodowskiej - Curie w Poznaniu. Podmiot, który doskonale zna specyfikę działalności zarówno małych jak i dużych podmiotów leczniczych;

(g) **Centrum Monitorowania Jakości w Ochronie Zdrowia (dalej: „CMJ")** – jednostka Ministerstwa Zdrowia, która wspiera działania zmierzające do poprawy jakości usług medycznych. W swojej działalności zajmuje się monitorowaniem wskaźników jakości w służbie zdrowia. CMJ posiada 20-letnie doświadczenie w ocenie placówek medycznych, ma bardzo szerokie spojrzenie na zagadnienia związane z ochroną zdrowia.

3.3 Inne podmioty publiczne i organizacje, z którymi konsultowano projekt i które uczestniczyły bezpośrednio lub pośrednio w kształtowaniu zapisów Kodeksu

Bardzo ważnym aspektem z perspektywy opracowywania Kodeksu były również uwagi zgłaszane w ramach przeprowadzanych systematycznie spotkań i prowadzonej korespondencji. Do grona podmiotów, z którymi współpracowaliśmy zaliczają się m.in. (wybrane podmioty):

(a) **Rzecznik Praw Pacjenta (dalej: „RPP")** – podejmuje działania na rzecz ochrony praw pacjentów, zapewnia trwały wzrost stopnia przestrzegania praw pacjentów w Polsce i podnosi poziom wiedzy o prawach pacjenta. **RPP konsultował treść jednej z wersji projektowanego Kodeksu.**

(b) **Prezes Urzędu Ochrony Danych Osobowych (dalej: „PUODO")** – Przedstawiciele inicjatywy pracującej nad Kodeksem **odbyli kilka spotkań z przedstawicielami PUODO, w przedmiocie Kodeksu, w tym jedno spotkanie dedykowane wyłącznie inicjatywie powstania Kodeksu.**

(c) **Fundacja MY Pacjenci** – zapewnia wsparcie eksperckie organizacjom pacjenckim, żeby komunikowały skuteczniej swoje problemy i potrzeby. Misją Fundacji jest budowanie płaszczyzn współpracy między administracją publiczną, pacjentami i ich organizacjami, lekarzami, światem akademickim i biznesem w ochronie zdrowia. Fundacja bierze udział w konsultacjach publicznych w zakresie projektów aktów związanych z sektorem ochrony zdrowia. Kierownictwo Fundacji na bieżąco otrzymywało informacje dotyczące postępu prac nad Kodeksem i było obecne w trakcie części spotkań roboczych dotyczących Kodeksu, a także we współpracy z Fundacją Panoptykon złożyło oficjalne stanowisko do jednej z wersji Kodeksu.

(d) **Fundacja Panoptykon** - fundacja, której celem jest działanie na rzecz wolności i ochrony praw człowieka w społeczeństwie nadzorowanym. Fundacja we współpracy z Fundacją My Pacjenci uczestniczyło w pracach nad przygotowaniem stanowiska do jednej z wersji Kodeksu.

(e) **Rada Dialogu Społecznego** – została powołana przez Prezydenta RP w dniu 22 października 2015 r., na mocy Ustawy z dnia 24 lipca 2015 r. o Radzie Dialogu

Społecznego i innych instytucjach dialogu społecznego (Dz. U. z 2015 r., poz. 1240). Instytucja ta stanowi forum dialogu trójstronnego w Polsce i współpracy strony pracowników, strony pracodawców oraz strony rządowej, funkcjonującej na poziomie centralnym. **Projekt jednej z wersji Kodeksu był przedmiotem dyskusji w jednym z podzespołów w ramach RDS.**

(f) **Fundacja Onkologia 2025** – stanowi platformę do debaty i współdziałania dla osób oraz instytucji zainteresowanych poprawieniem dostępności i efektywności opieki onkologicznej w Polsce, ze szczególnym uwzględnieniem badań naukowych i wtórnego wykorzystania danych (secondary use of data) w badaniach naukowych – fundacja była na bieżąco informowana o postępach prac nad Kodeksem, a także wspierała inicjatywę Kodeksu w zakresie badań naukowych.

(g) **Konferencja Rektorów Akademickich Uczelni Medycznych** – zrzeszenie Dziekanów Wydziałów Lekarskich Uczelni Publicznych. Obecnie celem Konferencji Rektorów Akademickich Uczelni Medycznych jest wprowadzenie wspólnego stanowiska Rektorów i wyrażanie opinii w sprawach szpitali klinicznych.

Dodatkowo zapisy kolejnych wersji Kodeksu były konsultowane ze wszystkimi zainteresowanymi osobami i organizacjami, co zostało zrealizowane poprzez:

a) Szeroką wysyłkę ankiet dotyczących projektowanego kształtu Kodeksu, jeszcze w 2017 roku.

b) Zorganizowanie bezpłatnej ogólnopolskiej konferencji w Warszawie, w której uczestniczyło **ponad 550 osób**.

c) Prowadzenie **dedykowanej strony internetowej i newslettera**, które umożliwiły sprawne przekazywanie informacji szerokiej grupie interesariuszy. **Do newslettera zapisało się dotychczas ok. 2000 osób i instytucji**.

W ramach prowadzonych konsultacji publicznych otrzymaliśmy **kilkaset stanowisk i opinii od uczestników Konferencji RODO w zdrowiu oraz osób, które zapisały się do newslettera** poprzez stronę internetową www.rodowzdrowiu.pl.

4. PRZEBIEG KONSULTACJI PUBLICZNYCH

4.1 Inauguracja prac nad Kodeksem

Spotkanie inaugurujące współpracę administracji publicznej z organizacjami branżowymi nad stworzeniem Kodeksu postępowania dla podmiotów sektora ochrony zdrowia dotyczącego ochrony danych osobowych odbyło się **26 lipca 2017 r.** w Warszawie. W spotkaniu uczestniczyli przedstawiciele PIIT, PFSz, TGR, Medycyny Praktycznej, ZPTC Lewiatan, CSIOZ, CMJ, NIPiP, KIF, MZ, Województwa Dolnośląskiego oraz DZP. Uczestnicy spotkania z uwagi na zbliżający się termin wejścia w życie RODO, art. 40 RODO i konieczność zapewnienia z jednej strony szczególnej ochrony przetwarzania danych medycznych Pacjentów, a z drugiej strony dostępu do tych danych w zakresie niezbędnym do efektywnej realizacji procesu terapeutycznego oraz rozwoju badań dostrzegli zasadność stworzenia i pracy nad opracowaniem Kodeksu

branżowego. Swoje stanowisko wyrazili w liście intencyjnym. Sygnatariusze poza poparciem idei utworzenia Kodeksu i deklaracją gotowości do pracy nad jego treścią podkreślili, iż opracowanie Kodeksu powinno opierać się na dialogu i współpracy organizacji branżowych sektora ochrony zdrowia, organizacji reprezentujących pacjentów i strony publicznej, a finalna treść Kodeksu winna być uzgodniona przez strony tworzące Kodeks oraz wspierające jego powstanie.

4.2 Wysłanie kwestionariuszy do członków inicjatywy + zawiązanie IV grup roboczych

Po spotkaniu inauguracyjnym do członków inicjatywy zostały wysłane kwestionariusze/ ankiety dotyczące zakresu podmiotowego i przedmiotowego Kodeksu. Ankieta stanowi załącznik 1 do niniejszego Raportu. W odpowiedzi otrzymano kilkadziesiąt wypełnionych ankiet i uwag do ankiet (do listopada 2017). Na podstawie ankiet powołano IV grupy robocze, które pracowały niezależnie nad przygotowaniem części Kodeksu. Kancelaria DZP była koordynatorem całości prac:

a) **Grupa robocza I:** zakres kodeksu, ogólne ustalenia (administratorzy danych, podstawa prawna, cel i zakres przetwarzania itp.)

b) **Grupa robocza II:** bezpieczeństwo danych – CSIOZ jako lider grupy

c) **Grupa robocza III:** prawa pacjenta

d) **Grupa robocza IV:** badania naukowe, wtórne wykorzystanie danych.

4.3 Przygotowanie 1 wersji Kodeksu

Pierwsza wersja Kodeksu została zaprezentowana na krótko przed ogólnopolską konferencją www.rodowzdrowiu.pl, wersja ta zawierała już dość szczegółowe zapisy wypracowane przez grupy robocze I-III, bez zagadnień dotyczących Komitetu sterującego i monitorowania przestrzegania Kodeksu.

4.4 Założenie strony internetowej i przygotowanie bezpłatnej Konferencji

W celu budowania dialogu i pochylenia się nad problematyką związaną z wprowadzeniem RODO Komitet sterujący podjął decyzję o organizacji bezpłatnej konferencji. W związku z konferencją podjęto decyzję o utworzeniu strony internetowej www.rodowzdrowiu.pl, na której umieszczano szczegółowe informacje dotyczące konferencji, a później również kolejne wersje Kodeksu.

Konferencja „RODO w sektorze medycznym – gdzie jesteśmy, dokąd zmierzamy?" odbyła się 14 marca br. na Uczelni Łazarskiego w Warszawie. W trakcie spotkania organizatorzy przedstawili do konsultacji publicznych pierwszą wersję kodeksu branżowego dot. przetwarzania danych medycznych, która została przygotowana przez szeroką koalicję interesariuszy.

Uczestnicy dyskutowali o dotychczasowych doświadczeniach z wdrożenia RODO w różnych placówkach medycznych, a wspólnie z przedstawicielami strony publicznej omówili największe i najczęstsze wyzwania oraz problemy związane z wdrożeniem RODO. Wspólnie zastanowili się również nad tym, na co jeszcze zwrócić uwagę i co można zrobić na 2 miesiące przed rozpoczęciem obowiązywania RODO.

Prelegentami i panelistami byli przedstawiciele strony publicznej (m.in. CSIOZ, GIODO – Pani Dyrektor Krasińska, pacjentów) oraz czołowi eksperci branżowi w dziedzinie prawa, IT oraz analizy ryzyka.

Uwagi dotyczące Kodeksu przekazane przez uczestników były dla nas bardzo wartościowe, wiele z nich zostało uwzględnionych w kolejnej wersji Kodeksu.

4.5 Newsletter i kolejne wersje Kodeksu

Po Konferencji o dalszych pracach informowaliśmy interesariuszy za pomocą strony internetowej i newslettera, do którego można było przystąpić wypełniając formularz na stronie.

kolejna wersja projektu kodeksu branżowego pojawiały się sukcesywnie na stronie www.rodowzdrowiu i/lub na listach mailingowych podmiotów bezpośrednio zaangażowanych w prace. W dniu 17 września br. na stronie www.rodowzdrowiu.pl pojawiła się już prawie kompletna wersja Kodeksu, zawierająca również kwestie dotyczące monitorowania przestrzegania Kodeksu. Dodatkowo projekt został uzupełniony o wzór zgody na przetwarzanie danych osobowych oraz odnosi się do takich kwestii jak kwalifikacja materiału biologicznego jako danych osobowych. Termin na zgłoszenie uwag do drugiej wersji projektu upływał 27.09.2018 r. Kika kolejnych wersji Kodeksu było opracowywanych na podstawie napływających drogą mejlową uwag i na podstawie uwag zgłoszonych przez samorządy zawodowe i organizacje zrzeszające administratorów danych.

4.6 Kontakt z mediami

Równolegle do innych działań komunikacyjnych podmioty działające w ramach inicjatywy Kodeksu, prowadziły szeroko zakrojone działania w mediach promujące ideę Kodeksu i zachęcające do udziału w pracach nad Kodeksem. Działania te dotyczyły zarówno mediów branżowych, jak również innych mediów o zasięgu ogólnopolskich. Przykłady działań wskazane są poniżej:

http://www.rynekzdrowia.pl/Prawo/RODO-opublikowano-wstepny-szkic-kodeksu-dla-placowek-medycznych,182193,2.html

https://www.prawo.pl/zdrowie/rodo-kogo-obejmie-kodeks-branzowy-dla-sektora-ochrony-zdrowia,261668.html

https://serwisy.gazetaprawna.pl/zdrowie/artykuly/1122299,jak-stosowac-rodo-w-sluzbie-zdrowia.html

http://www.politykazdrowotna.com/36542,rodo-w-sektorze-medycznym-kolejna-wersja-kodeksu-branzowego

4.7 Indywidualne konsultacje

Równolegle do szeroko prowadzonych konsultacji publicznych, prowadzono również dedykowane warsztaty dla kluczowych interesariuszy. Takie indywidualne spotkania/warsztaty odbyły się m.in. z:

a) PUODO – z Panem Dyrektorem Drobkiem,

b) Przedstawicielami Rzecznika Praw Pacjenta;

c) CSIOZ – konsultacje i spotkania odbywały się cyklicznie w węższym lub szerszym gronie CSIOZ było jednym z liderów merytorycznych projektu Kodeksu

d) Samorządami zawodowymi – KIF, NIPiP, NIL

e) Organizacjami branżowymi będącymi członkami Komitetu sterującego

f) RDS

4.8 Zakończenie prac

Po zamknięciu ostatniego etapu konsultacji publicznych i zakończeniu niezależnych konsultacji indywidualnych, rozpoczęto pracę nad finalną wersją Kodeksu. Po blisko miesiącu prac przedstawiono końcową wersję Kodeksu, która niniejszym zostaje zaprezentowana zgodnie z procedurą Prezesowi Urzędu Ochrony Danych Osobowych do zaakceptowania.

4.9 Stanowiska podmiotów uczestniczących w konsultacjach

W załączniku nr 2 do Raportu a także w załączniku nr 3 oraz 4 do wniosku do zatwierdzenie Kodeksu zamieszczono wybrane stanowiska, które napłynęły do Komitetu sterującego w ramach konsultacji publicznych, a także wyrazy poparcia.

Załącznik nr 2 do wniosku

Załącznik 1 do Raportu:

ANKIETA DOTYCZĄCA ZAKRESU PRZEDMIOTOWEGO KODEKSU BRANŻOWEGO SEKTORA OCHRONY ZDROWIA, WRZESIEŃ 2017 r.

Szanowni Państwo,

W nawiązaniu do rozmów podczas spotkania inaugurującego prace nad kodeksem branżowym, przesyłamy Państwu proponowany zakres przedmiotowy kodeksu z prośbą o uzupełnienie swoich uwag lub propozycji konkretnych zapisów postanowień kodeksu. Zależy nam na tym, że kodeks w jak największym stopniu uwzględniał specyfikę działania branży medycznej. Zebrane uwagi i komentarze uwzględnimy przy planowaniu szkieletu kodeksu.

Prosimy o odesłanie dokumentu do 24 września.

Z poważaniem

Piotr Najbuk

1. **Zasady przetwarzania danych osobowych**

Proponowany zakres	Komentarze/propozycje postanowień
wskazanie kategorii pracowników służby zdrowia i personelu administracyjnego, który będzie mógł przetwarzać dane o stanie zdrowia pacjentów na podstawie przesłanki określonej w art. 9 ust. 2 lit h RODO w zw. z art. 9 ust. 3 RODO	
określenie standardów służących spełnieniu zasady rozliczalności przez administratorów danych i przez podmioty przetwarzające, tj.: – opracowanie wytycznych co do zawartości polityk ochrony danych, o których mowa w art. 24 ust. 2 RODO; – zasady dokumentowania wykonania obowiązków wynikających z art. 25 RODO; - wypracowanie jednolitych zasad w zakresie podejścia do oceny skutków dla przetwarzania danych osobowych (art. 35 RODO), w tym w szczególności wypracowanie modelowego formularza oceny i jednolitego podejścia do operacji trwających przed wejściem w życie przepisów RODO.	

2. **Zasady pseudonimizacji**

Proponowany zakres	Komentarze/propozycje postanowień
określenie procesów przetwarzania danych osobowych na potrzeby udzielania świadczeń medycznych, w których możliwe jest zastosowanie metod pseudonimizacji danych;	
określenie preferowanych metod pseudonimizacji danych.	

Załącznik nr 2 do wniosku

3. Informowanie opinii publicznej i osób, których dane dotyczą

Proponowany zakres	Komentarze/propozycje postanowień
sposób konstrukcji i wykonania obowiązku informacyjnego wobec pacjentów, o którym mowa w art. 13 RODO w odniesieniu do podmiotów udzielających świadczeń zdrowotnych stacjonarnie jak i na odległość, np. poprzez określenie jednolitego wzoru klauzuli obowiązku informacyjnego stosowanego przez te podmioty.	

4. Zasady wykonywania przez osoby, których dane dotyczą przysługujących im praw

Proponowany zakres	Komentarze/propozycje postanowień
określenie wzorca informacji przekazywanej osobie, której dane dotyczą w związku z wykonywaniem prawa dostępu określonego w art. 15 RODO;	
doprecyzowanie zasad wykonywania obowiązku, o którym mowa w art. 15 RODO w kontekście zasad udostępniania dokumentacji medycznej na rzecz osób upoważnionych przez pacjenta	
określenie zasad postępowania w przypadku otrzymania przez administratora danych osobowych żądania sprostowania lub usunięcia danych osobowych w kontekście obowiązku powiadamiania odbiorców danych określonego w art. 19 RODO;	
określenie minimalnych wymagań technicznych związanych z realizacją prawa do przenoszenia danych w kontekście działalności podmiotów z sektora eHealth, telemedycznego i mHealth w zakresie w jakim podmioty te mogą przetwarzać dane pacjentów na podstawie ich zgody;	
określenie zasad pozyskiwania zgody pacjentów na profilowanie w kontekście działalności innowacyjnej w sektorze ochrony zdrowia (np. w kontekście wyrobów, które w zautomatyzowany sposób analizują wyniki badań pacjenta i kwalifikują do dalszej diagnostyki)	
określenie zasad współpracy pomiędzy administratorami danych a podmiotami przetwarzającymi w celu pomocy administratorom danych w wywiązaniu się z obowiązków dotyczących odpowiadania na żądań osób, których dane dotyczą w zakresie wykonywania ich praw określonych w rozdziale III RODO;	
wprowadzenie reguł postępowania w zakresie	

składania przez osobę, której dane dotyczącą, wniosku lub żądania związanego z wykonywaniem przysługujących jej praw (art. 15-21 RODO) bezpośrednio do podmiotów przetwarzających z pominięciem administratora danych	

5. Informowanie i ochrona dzieci, oraz sposób pozyskiwania zgody osoby sprawującej władzę lub opiekę nad dzieckiem

Proponowany zakres	Komentarze/propozycje postanowień
określenie zasad ochrony i informowania i osób małoletnich o zasadach przetwarzania danych w sytuacji, w której byłyby one osobami korzystającymi z usług o charakterze eHealth, telemedycznym lub Health. Ponadto określenie sposobu pozyskania zgody opiekuna tej osoby na przetwarzanie danych osobowych, w kontekście wymogów świadomej zgody pacjenta pow. 16 roku życia wynikających z przepisów ustawy o prawach pacjenta i ustawy o zawodach lekarza i lekarza dentysty.	

6. Środki i procedury zapewniające bezpieczeństwo przetwarzania

Proponowany zakres	Komentarze/propozycje postanowień
opracowanie ogólnych wytycznych służących ocenie bezpieczeństwa rozwiązań technologicznych stosowanych do przetwarzania danych osobowych;	
opracowanie ogólnych wytycznych służących ocenie wiarygodności podmiotów, którym mają zostać powierzone do przetwarzania dane osobowe zawarte w dokumentacji medycznej;	
opracowanie modelowych klauzul do umowy powierzenia przetwarzania danych osobowych zawartych w dokumentacji medycznej, uwzględniających wymogi RODO i ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (określenie minimalnych wymogów co do treści umowy);	
opracowanie modelowych klauzul do umowy dalszego powierzenia przetwarzania danych osobowych zawartych w dokumentacji medycznej, uwzględniających wymogi RODO i ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (określenie minimalnych wymogów co do treści)	
opracowanie ogólnych wytycznych co do kształtu dokumentacji ochrony danych osobowych, którą powinny wdrożyć podmioty z sektora ochrony zdrowia	

7. **Zgłaszanie organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamianie o takich naruszeniach osób, których dane dotyczą**

Proponowany zakres	Komentarze/propozycje postanowień
opracowanie wzorcowego modelu postępowania w sytuacji naruszenia ochrony danych osobowych dla podmiotów udzielających świadczeń stacjonarnych, podmiotów przetwarzających oraz podmiotów działających w branży eHealth, telemedycznej i mHealth; opracowane wytyczne powinny uwzględniać różną specyfikę tychże podmiotów;	
opracowanie przykładowego katalogu naruszeń ochrony danych osobowych, których zaistnienie będzie uznawane za skutkujące ryzykiem naruszenia praw osób, których dane dotyczą	
opracowanie wzorcowego szablonu informacji przekazywanej osobom, których dane dotyczą w sytuacji naruszenia ochrony danych osobowych	

8. **Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych**

Proponowany zakres	Komentarze/propozycje postanowień
określenie zasad transferu danych osobowych zawartych w dokumentacji medycznej do państw trzecich w sytuacji konieczności zapewnienia ciągłości udzielanych świadczeń medycznych	

9. **Postępowania pozasądowe oraz inne tryby rozstrzygania sporów w celu rozstrzygania sporów w zakresie przetwarzania między administratorami a osobami, których dane dotyczą**

Proponowany zakres	Komentarze/propozycje postanowień
wprowadzenie podstawowych zasad rozpatrywania skarg dot. przetwarzania danych, które mogą zostać złożone bezpośrednio do podmiotów działających w sektorze ochrony zdrowia	
wprowadzenie zasad rozpatrywania skarg dotyczących przetwarzania danych osobowych złożonych do podmiotów przetwarzających dane osobowe, których administratorami są podmioty wykonujące działalność leczniczą;	

Warszawa, dnia 30 marca 2018 r.

RZECZPOSPOLITA POLSKA
Rzecznik Praw Pacjenta
Bartłomiej Chmielowiec

RzPP-ODO.0130.4.2018

Pan
Piotr Najbuk
Kancelaria Domański
Zakrzewski Palinka sp. k.
Partner merytoryczny grupy
inicjatywnej
piotr.najbuk@dzp.pl

Z zainteresowaniem obserwuję prace nad kodeksem branżowym sektora ochrony zdrowia, który powstaje od kilku miesięcy z inicjatywy szerokiej koalicji interesariuszy – przedstawicieli organizacji branżowych, we współpracy ze stroną publiczną, wsparciem organizacji pacjentów oraz organizacji samorządów zawodowych.

Podjęcie przez organizacje branżowe, które zrzeszają podmioty wykonujące działalność leczniczą, działań zmierzających do lepszego przygotowania swoich członków na nadchodzące zmiany przepisów w zakresie ochrony danych osobowych to w mojej ocenie inicjatywa istotna i potrzebna.

Kodeks branżowy z założenia ma na celu doprecyzowanie zasad przetwarzania i ochrony danych osobowych określonych 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[1] (ogólne rozporządzenie o ochronie danych osobowych – dalej: „RODO") z uwzględnieniem specyfiki sektora ochrony zdrowia.

Ma pomóc we właściwym stosowaniu niniejszego rozporządzenia poprzez dookreślenie zakresu stosowania ogólnych przepisów RODO i dostosowanie przyjętych

[1] Dz. Urz. UE L 119, s.1

rozwiązań do specyfiki branży. Może być sposobem na obniżenie ryzyka związanego ze stosowaniem RODO, w tym w zakresie ograniczania ryzyka naruszenia praw i wolności osób fizycznych.

Przygotowywany kodeks powinien być przede wszystkim zgodny z RODO, co będzie przedmiotem oceny organu nadzorczego – Generalnego Inspektora Ochrony Danych Osobowych, a po wejściu w życie nowej ustawy o ochronie danych osobowych Prezesa Urzędu Ochrony Danych Osobowych – który wydaje opinię o zgodności projektów kodeksów branżowych z RODO i zatwierdza takie projekty, jeżeli uzna, że stanowią one odpowiednie zabezpieczenia.

Powinien również zawierać jasne rozwiązania określonych problemów w obszarach charakterystycznych dla sektora ochrony zdrowia. Obszary te obejmują między innymi rzetelne i przejrzyste przetwarzanie danych osobowych, informowanie osób, których dane dotyczą oraz wykonywanie przez te osoby przysługujących im praw wynikających z RODO. Najważniejszymi podmiotami danych, do których odnosi się projektowany kodeks, są pacjenci, dlatego też pragnę zwrócić Państwa uwagę na kilka istotnych z punktu widzenia pacjentów kwestii, mając świadomość, że prace nad kodeksem wciąż trwają, a uwagi odnoszą się do wersji roboczej dokumentu.

Zgodnie z unormowaniem art. 3 ust. 1 pkt 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[2] pacjentem jest osoba zwracającą się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub osobę wykonującą zawód medyczny. Podkreślić należy, iż status pacjenta jest ściśle związany z procesem leczniczym, a więc procesem mającym na celu zachowanie, ratowanie, przywracanie lub poprawę stanu jego zdrowia.

Nie każda relacja osoby fizycznej z lekarzem jest relacją w której osoba ta posiada status pacjenta. Przykładem będą lekarze orzecznicy ZUS, którzy nie biorą udziału w procesie leczniczym osoby przez nich badanej. Inny jest cel tego badania aniżeli leczniczy. Podobnie sytuacja wygląda w przypadku powoływanych przez sąd powszechny, korporacyjny lub np.: prokuratora biegłych lekarzy.

Na uwagę zasługują również dwa orzeczenia Trybunału Konstytucyjnego[3], w których podniesiono, iż nie każde badanie (świadczenie) przeprowadzane przez lekarza może zostać

[2] Dz.U. z 2017 r. poz. 1318 ze zm.
[3] wyrok TK z dnia 13 czerwca 2013 r. sygn. akt K 17/11 oraz wyrok TK z dnia 5 marca 2013 r. sygn. akt U 2/11

zakwalifikowane jako świadczenie zdrowotne w rozumieniu art. 2 ust. 1 pkt 10 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.[4]

W pracach na kodeksem trzeba również zwrócić uwagę i uwzględnić przetwarzanie danych osobowych podmiotów innych niż pacjent, tj. przedstawicieli ustawowych czy opiekunów faktycznych.

W zakresie zaproponowanych w projekcie kodeksu definicji i skrótów zasadne jest rozszerzenie definicji dokumentacji medycznej poprzez wskazanie, że obok ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz przepisów wykonawczych do ww. ustawy dokumentacja medyczna może być definiowana w „innych przepisach odrębnych". Przykładem może być karta uodpornienia, zawierająca dane medyczne, która pomimo swojego specjalnego statusu, powinna być traktowana jak dokumentacja medyczna w świetle Kodeksu. Brakuje również definicji profilaktyki zdrowotnej, do której jako jednego z celów przetwarzania danych kodeks wielokrotnie się odwołuje.

Wydaje się również, iż w Kodeksie pominięto istnienie przepisów ustawy o ochronie zdrowia psychicznego[5] m.in. w przedmiocie przyjęcia pacjenta bez zgody – a w konsekwencji sytuacji ochrony danych osobowych takiego pacjenta.

W projekcie Kodeksu wymieniono cele, w jakich podmioty wykonujące działalność leczniczą mogą przetwarzać dane osobowe pacjentów. Szczegółowe określenie celów, a co z tym związane określenie adekwatnego do celu zakresu przetwarzania, wypełnia postulat przejrzystości i rzetelności przetwarzania. Warto zatem rozważyć doprecyzowanie celów i zakresu przetwarzania, np. w zakresie pozyskiwania informacji zarządczych, czynności pomocniczych, wymiany informacji o stanie zdrowia pomiędzy różnymi podmiotami wykonującymi działalność leczniczą czy badania satysfakcji pacjentów.

Wątpliwości budzą zaproponowane w Kodeksie zapisy dotyczące administratora danych. Zasadne jest ich doprecyzowanie, tak aby jasno z nich wynikało, na jakiej podstawie dane są przetwarzane – umowy powierzenia czy upoważnienia – oraz kto jest ich administratorem.

Z treści Kodeksu jasno powinno wynikać, np. na jakiej zasadzie i w jakim zakresie w razie udostępnienia dokumentacji medycznej pomiędzy Podmiotami Wykonującymi Działalność Leczniczą (dalej: PWDL) podmiot, któremu ta dokumentacja jest udostępniona, jest obowiązany do zapewnienia ochrony danych zawartych w tej dokumentacji (jeżeli działa

[4] Dz.U. z 2018 r. poz. 160 ze zm.
[5] Dz.U. z 2017 r. poz. 882 ze zm.

na rzecz innego PWDL). Badania wykonywane są często w innym PWDL niż ten, który następnie wykorzystuje wyniki tych badań, np. do zabiegu operacyjnego. Następuje to na podstawie zlecenia, a więc PWDL, który wykonuje badania działa na rzecz PWDL, w którym ma zostać przeprowadzony zabieg. Wówczas PWDL, który wykorzystuje wyniki tych badań – dołączając je do historii choroby - staje się administratorem danych, pomimo że nie on był ich wytwórcą. Kopia wyników badań może być również przechowywana w PWDL, który przeprowadził te badania (np. w systemie teleinformatycznym).

Pomimo iż w Kodeksie wskazano, że prawa wynikające z RODO a prawa pacjenta stanowią uprawnienia odrębne, nie można negować faktu, iż w ramach uprawnienia osoby upoważnionej przez pacjenta do otrzymywania informacji o stanie zdrowia, następuje przekazywanie danych osobowych. Z tych względów Kodeks nie powinien pomijać wskazówek odnośnie weryfikacji osoby upoważnionej przez pacjenta. Analogicznie, należałoby wskazać na konieczność prac w zakresie weryfikacji tożsamości osoby dzwoniącej do podmiotu leczniczego celem realizacji prawa pacjenta do kontaktu z osobami bliskimi.

Nie wskazano również, w jaki bezpieczny sposób pozyskiwany jest adres e-mail pacjenta. Biorąc pod uwagę, iż obecnie w środowisku medycznym istnieją wątpliwości co do sposobu realizacji uprawnienia pacjenta do otrzymania dokumentacji medycznej drogą elektroniczną, wydaje się zasadnym, aby kodeks branżowy rozwiązywał niniejszy dylemat w sposób precyzyjny.

Proponuję również rozważyć kwestię regulowanego art. 15 ust. 3 RODO prawa do otrzymania kopii danych osobowych podlegających przetwarzaniu. Przepis ten nakłada na administratora danych obowiązek bezpłatnego pierwszorazowego udostępnienia na żądanie osoby, której dane dotyczą, kopii jej danych. PWDL przetwarzają dane osobowe pacjentów w szczególności w prowadzonej dokumentacji medycznej, realizując zatem ww. obowiązek zobowiązane będą do udostępnienia kopii dokumentacji medycznej. W kodeksie zaproponowano zapisy mówiące, że prawo do bezpłatnej kopii danych przysługuje pacjentowi jednoznacznie powołującemu się na to prawo. Natomiast w przypadku żądania dokumentacji medycznej bez wskazania, że pacjent zamierza realizować prawo, o którym mowa w art. 15 RODO, kopia dokumentacji udostępniana jest odpłatnie, na zasadach określonych w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta. Konieczność powołania się na konkretną podstawę prawną i uzależnienie od tego konieczności wniesienia opłaty bądź bezpłatnego otrzymania pierwszej kopii danych osobowych, których nośnikiem jest dokumentacja medyczna, utrudni Pacjentowi realizację jego praw zgodnie z jego najlepszym interesem.

W celu uniknięcia wątpliwości interpretacyjnych oraz w interesie pacjenta byłoby przyjęcie, że pierwsza kopia dokumentacji medycznej, niezależnie od przywołania przez pacjenta podstawy żądania, będzie dostarczana bezpłatnie. Rozwiązanie takie uprości procedury po stronie PWDL oraz pozwoli ograniczyć ewentualne roszczenia pacjentów wynikające z interpretacji złożonych przez nich oświadczeń woli.

Warto również podkreślić, że wyłącznie uprzednio uświadomieni pacjenci będą świadomie korzystać z uprawnień, jakie daje im RODO. Niezwykle istotne jest zatem rzetelne realizowanie obowiązków informacyjnych, czyli zapewnienie, że wymagane informacje będą realnie dostępne dla pacjenta. W tym kontekście należy zauważyć, że dostęp pacjentów do regulaminów organizacyjnych w podmiotach leczniczych jest niekiedy ograniczony. Tylko niektóre dane zawarte w tych regulaminach muszą być zgodnie z ustawą o działalności leczniczej podane do wiadomości pacjentów przez ich wywieszenie w widoczny sposób w miejscu udzielania świadczeń oraz na stronie internetowej tego podmiotu (patrz. art. 24 ust. 2 ww. ustawy). Proponuję więc, aby możliwość zamieszczenia klauzul informacyjnych w ww. regulaminie było powiązane z obowiązkiem określonym w art. 24 ust. 2 ustawy o działalności leczniczej. Ponadto pacjent skorzysta z prawa do swobodnego wyboru podstawy oraz zakresu żądania związanego z dostępem do informacji na jego temat przetwarzanych przez PWDL, tylko jeśli zostanie poinformowany o przysługujących mu prawach.

W zakresie prawa do bycia zapomnianym projekt kodeksu precyzuje, że PWDL odmawia zrealizowania tego prawa w odniesieniu do danych osobowych zawartych w dokumentacji medycznej przez cały wymagany przepisami prawa okres archiwizacji dokumentacji medycznej. Jednak, prawo pacjenta do bycia zapomnianym w tym zakresie można zrealizować po upływie okresów, o których mowa w art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta przez wydanie pacjentom, ich przedstawicielom ustawowym lub osobom przez nich upoważnionym dokumentacji medycznej. Również prawo do sprzeciwu wobec przetwarzania danych osobowych powinno być możliwe do zrealizowania po upływie okresów przechowywania dokumentacji medycznej, o których mowa w art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

Zgodnie z motywem 99 preambuły RODO podmioty sporządzające kodeksy postępowań *powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji.* Pozyskanie uwag i opinii pacjentów

oraz ich wnikliwa analiza jest w mojej ocenie elementem niezbędnym do stworzenia regulacji spełniającej potrzeby wszystkich interesariuszy projektowanego kodeksu.

Ogólne rozporządzenie o ochronie danych osobowych będzie miało szczególnie znaczenie dla obszaru zdrowia publicznego. Zmiany w przepisach oznaczają dla wielu podmiotów wykonujących działalność leczniczą konieczność przyjęciach nowych rozwiązań organizacyjnych i technicznych. Jednym z takich rozwiązań jest stworzenie i stosowanie kodeksu branżowego.

Kodeks branżowy dla sektora ochrony zdrowia jest w fazie projektu i nie znamy jeszcze jego ostatecznego kształtu, mam jednak nadzieję, że spełni oczekiwania podmiotów funkcjonujących w systemie ochrony zdrowia, a przede wszystkim pacjentów – gwarantując ochronę ich prywatności i odpowiedni poziom ochrony danych o stanie zdrowia. Liczę na to, że przyczyni się do realizacji nadrzędnego celu, który powinien przyświecać wszystkim podmiotom koncentrującym swoje działania na pacjencie, dla jego dobra.

Z poważaniem

RZECZNIK PRAW PACJENTA

Bartłomiej Chmielowiec

FUNDACJA PANOPTYKON

FUNDACJA MY PACJENCI

Warszawa, 19 stycznia 2018 r.

Szanowni Państwo,

w imieniu **Fundacji Panoptykon** oraz **Fundacji My pacjenci** przekazujemy Państwu w załączniku nasze robocze uwagi do projektu kodeksu postępowania podmiotów wykonujących działalność leczniczą w wersji 8.0 przygotowanej 31 grudnia 2017 r.

Ewa Borek

Prezes Zarządu Fundacji My Pacjenci

Fundacja Panoptykon | ul. Orzechowska 4 lok. 4 | 02-068 Warszawa
e: fundacja@panoptykon.org | t: +48 660 074 026 | w: panoptykon.org

Robocze uwagi Fundacji Panoptykon i Fundacji My pacjenci do projektu kodeksu postępowania podmiotów wykonujących działalność leczniczą w wersji 8.0 przygotowanej 31 grudnia 2017 r.

wyłączenie/ograniczenie	gdzie w kodeksie	Uwagi
korzystanie z praw przez pacjentów nie posługujących się językiem polskim - jedynie możliwość podjęcia działań przez PWDL	6.1.2	-
dodatkowa opłata w przypadku **nieuzasadnionych lub nadmiernych żądań** rozumianych *w szczególności* jako: • częściej niż raz na 3 miesiące, jeśli zakres danych nie ulegał zmianie; • żądanie informacji w niestandardowym formacie; • informacje sztucznie dzielone na kilkanaście żądań, • żądanie odpowiedzi w innym języku niż polski	6.1.5; 6.1.6	w naszej ocenie administrator powinien każdorazowo uzasadniać zamiar pobrania opłaty [art. 12 ust. 5 RODO]
odmowa udzielenia informacji w następujących przypadkach: • żądanie informacji, których przekazanie spowodowałoby nieuprawnione ujawnienie tajemnicy przedsiębiorstwa, tajemnicy zawodowej lub danych innych pacjentów; • żądanie informacji, których udzielenie wymagałoby **zaangażowania personelu w sposób utrudniający bieżące funkcjonowanie PWDL**, np. poprzez: - konieczność ograniczenia liczby pacjentów, którym udzielane byłyby	6.1.7	Sformułowanie „zaangażowanie personelu w sposób utrudniający bieżące funkcjonowanie" niesie ryzyko nadużyć – postulujemy jego doprecyzowanie Podobne ryzyko nadużyć dostrzegamy w argumencie wydłużenia czasu realizacji innych praw pacjentów (można te procesy tak zaprojektować, żeby nie było kolizji) – propozycja rodzi ryzyko, że będzie to furtka umożliwiająca bezpodstawną odmowę udostępnienia informacji

świadczenia, **- konieczność wydłużenia czasu realizacji innych praw pacjentów**		
weryfikacja tożsamości pacjenta na potrzeby realizacji praw: • zawsze obowiązkowa • za pomocą dokumentu tożsamości z numerem PESEL • PWDL może **utrwalić informacje o dokumencie** (np. numer i seria) • przy weryfikacji na odległość możliwość żądania dodatkowych informacji, w tym danych osobowych, jak również dodatkowych czynności weryfikacyjnych, np. **przelew bankowy**; wszystkie dodatkowe dane mogą być utrwalone.	6.2.3.2 6.2.6.2; 6.2.5	Wątpliwa jest możliwość utrwalania informacji o dokumencie wykorzystanym przy weryfikacji – w naszej ocenie powinno być ona zastąpiona utrwaleniem (jeśli to konieczne) informacji, że tożsamość pacjenta została dodatkowo zweryfikowana. Przelew bankowy może być nadmiernie obciążającym sposobem weryfikacji dla części pytających – weryfikacja za jego pomocą powinna się odbywać wyjątkowo i wyłącznie jako alternatywa do innych metod weryfikacji.
Obowiązek informacyjny (art. 13 RODO): • Obowiązku nie trzeba realizować, gdy pacjent posiada już stosowne informacje.	6.3.4	Pojęcie „stosownych informacji" jest nieprecyzyjne. Niejasne jest, w jaki sposób informacje te miałyby być przekazane, w jaki sposób następuje sprawdzenie, czy takie informacje pacjent już ma? Proponujemy rozważenie zastąpienia sformułowania „stosowne informacje" sformułowaniem „informacje, których żąda pacjent, zostały już mu przekazane"
Obowiązek informacyjny (art. 14 RODO): • nie trzeba go realizować, jeśli PWDL wchodzi w posiadanie danych osobowych Pacjenta w związku z udostępnieniem mu dokumentacji medycznej ze względu na konieczność zapewnienia ciągłości udzielania świadczeń zdrowotnych, jak również w innych przypadkach w celach medycznych (podstawa	6.4	-

wyłączenia art. 14 ust. 5 lit. c i d RODO)		
Prawo dostępu: • nieodpłatna jest tylko pierwsza kopia dokumentacji (zgodnie z art. 15 ust. 3 RODO)	6.5.7	Pobranie opłaty jest dopuszczalne przez RODO, opłata musi być rozsądna.
Informowanie odbiorców danych o sprostowaniu / uzupełnieniu: • wyłączone, jeśli zmiany nie zagrażają życiu lub zdrowiu pacjenta, a poinformowanie jest niemożliwe lub nadmiernie utrudnione (np. nie można się z odbiorcą danych skontaktować drogą mailową, **dane udostępniono odbiorcy wcześniej niż na rok od chwili sprostowania)**	6.6.4.2	RODO umożliwia wyłączenie informowania odbiorców danych w niektórych sytuacjach (art. 19). Mamy wątpliwości, czy zaproponowane w kodeksie sytuacje wpisują się w te dopuszczalne wyłączenia, np. czy brak możliwości kontaktu drogą elektroniczną jest nadmierną uciążliwością? Nasze szczególne wątpliwości budzi niejasna ostatnia przesłanka („dane udostępniono odbiorcy wcześniej niż na rok od chwili sprostowania")
Prawo do bycia zapomnianym: • całkowite wyłączenie w stosunku do danych przetwarzanych w celach medycznych z uwagi na wymagany prawem okres archiwizacji dokumentacji medycznej • **ma być realizowane** w stosunku do danych objętych zgodą na przetwarzanie • informowanie odbiorców danych - **przyjęcie założenia, że posiadają oni wiedzę o usunięciu**, jeśli żądanie zgłoszono po upływie okresu obowiązkowego przechowywania dokumentacji medycznej	6.7	Wyłączenie dla celów archiwizacji wymaganej prawem jest ok. Wątpliwości budzi trzeci punkt - dlaczego z góry zakładać, że mają oni wiedzę o usunięciu, jeśli mimo upływu okresu archiwizacji mogą nadal te dokumenty posiadać i powinni być poinformowani o woli podmiotu praw.
Prawo do ograniczenia przetwarzania danych (ze względu na nieprawidłowość danych):	6.8.1	-

• wyłączone ze względu na ważne interesy publiczne		
Prawo do przenoszenia danych: • wyłączone w zakresie danych przetwarzanych dla celów medycznych	6.9	-
Prawo sprzeciwu: • wyłączone w zakresie danych przetwarzanych dla celów medycznych	6.10	-
Profilowanie: • **dopuszczalne bez zgody pacjenta**, również w oparciu o dane o stanie zdrowia, jest profilowanie które **nie skutkuje podejmowaniem decyzji** opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych wywołujących wobec Pacjentów skutki prawne lub w podobny sposób istotnie na nich wpływających • Pacjent nie może wykonać prawa do wniesienia sprzeciwu ze względu na odmienne podstawy przetwarzania danych przez PWDL niż wskazane w art. 21 RODO Profilowanie, które **skutkuje podejmowaniem decyzji** opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych wywołujących wobec Pacjentów skutki prawne lub w podobny sposób istotnie na nich wpływa: • pacjent ma prawo do uzyskania interwencji ze strony personelu • pacjent może wyrazić swoją opinię na temat decyzji • pacjent ma prawo nie podlegać decyzji opartej wyłącznie na	6.11.2 6.11.3 6.11.5 6.11.6	Profilowanie, szczególnie oparte o dane wrażliwe, musi mieć podstawę prawną. Fragment umożliwiający profilowanie bez zgody pacjenta rozumiemy jako odwołanie do wyraźnej zgody wymaganej na podstawie art. 22 RODO (jeśli tak, to wymaga to naszym zdaniem doprecyzowania). Zwracamy uwagę na brak odniesienia do art. 22 ust. 4 RODO i uzasadnienia, w jakich konkretnych przypadkach można profilować w oparciu o dane zdrowotne. Sformułowanie „pacjent ma prawo nie podlegać decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu" rozumiemy jako możliwość zakwestionowania decyzji (art. 22 ust. 3 RODO) – postulujemy doprecyzowanie tego punktu.

zautomatyzowanym przetwarzaniu, w tym profilowaniu Wyłączenia z definicji profilowania jako podejmowania decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu w rozumieniu art. 22 RODO: • automatyczne ustalanie wyników skal stosowanych w medycynie • **ocena wystąpienia mutacji/ ryzyka choroby na podstawie analizy genomu Pacjenta** • automatyczne klasyfikowanie wyniku jako „w normie" „ponad normę" i „poniżej normy" na podstawie zdefiniowanych przedziałów wyników • wspieranie, za pomocą algorytmów procesu terapeutycznego np. poprzez przedstawienie sugestii badania diagnostycznego, sugestii terapii farmakologicznej i podobnych przez system komputerowy, pod warunkiem, że ostateczną decyzję o sposobie leczenia podejmuje personel medyczny • wspieranie, za pomocą algorytmów komputerowych, procesu selekcji Pacjentów do programów badań profilaktycznych i przesiewowych, pod warunkiem, że ostateczną decyzję o zakwalifikowaniu Pacjentów do udziału w programach podejmuje personel medyczny • wspieranie, za pomocą algorytmów komputerowych, procesu zamawiania przez Pacjentów recept na produkty lecznicze przyjmowane przez dłuższy okres czasu np. poprzez automatyczne informowanie personelu		

medycznego o konieczności skierowania na wizytę kontrolną Pacjentów, którzy składają zapotrzebowanie na receptę ze względu na upływ określonego czasu od ostatniej wizyty • procesy dotyczące badań profilaktycznych i medycyny pracy, gdzie **decyzja o skierowaniu Pacjenta na określone badania** opiera się o czynniki charakterystyczne dla danego stanowiska pracy (zdefiniowane przez pracodawcę), a nie czynniki charakterystyczne dla osoby Pacjenta • działanie **aplikacji i algorytmów będących wyrobami medycznymi lub częściami wyrobów medycznych**, pod warunkiem że wyroby takie zostały dopuszczone do obrotu na terytorium Unii Europejskiej w zgodzie z obowiązującymi przepisami prawa, w zakresie dokonanej certyfikacji		

Jednocześnie zwracamy uwagę na dwa istotne z perspektywy praw pacjenta do ochrony danych osobowych kwestie, które powinny zostać uwzględnione w kodeksie:

- należy zobowiązać instytucję publiczną do zapewnienia pacjentom wsparcia w zarządzaniu swoimi danymi medycznymi. Dotyczy to szczególnie procesu wdrażania elektronicznej dokumentacji medycznej, która zintegruje dotychczas rozproszone dane medyczne pacjentów. Obywatele powinni mieć dostęp do systemowego wsparcia dotyczącego wyjaśniania wątpliwości i udzielania informacji na tematy związane z bezpośrednim zarządzaniem przez pacjentów danymi medycznymi, prawami dostępu oraz innymi prawami które definiuje RODO.

- istotne jest zagwarantowanie pacjentom prawa do wglądu w dane dotyczące osób które przeglądały dane medyczne pacjenta. Dane te powinny być nieusuwalne.

Te dwa elementy – wsparcie pacjentów w zarządzaniu danymi medycznymi oraz zapewnienie pacjentom wiedzy o korzystaniu z ich danych jest warunkiem zbudowania zaufania i w efekcie powodzenia nie tylko wdrożenia RODO ale także transformacji systemowej w ochronie zdrowia polegającej na wdrożeniu elektronicznej dokumentacji medycznej.

Warszawa, dnia 25 października 2018 r.

dr Dobrawa Biadun

Ekspertka ds. polityk publicznych Konfederacji Lewiatan

ul. Zbyszka Cybulskiego 3

00-727 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że projekt *„Kodeksu branżowego dla sektora ochrony zdrowia"* w ramach inicjatywy www.rodowzdrowiu.pl był konsultowany podczas posiedzenia Podzespołu problemowego ds. ochrony zdrowia Rady Dialogu Społecznego w dniu 8 maja2018 roku.

Dobrawa Biadun

PIIT

Warszawa, dnia 5 listopada 2018 r.
PIIT/1407/18

Boris Stokalski-Dzierzykraj
Prezes Zarządu Polskiej Izby Informatyki i Telekomunikacji
Al. Jerozolimskie 136 (IX piętro), 02-305 Warszawa

Szanowna Pani
DR EDYTA BIELAK–JOMAA

Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że Polska Izba Informatyki i Telekomunikacji (dalej: PIIT), organizacja reprezentująca interesy gospodarcze firm przemysłu teleinformatycznego, realizująca światowej klasy cyfrowe produkty i usługi, na podstawie art. 40 ust. 2 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 brała czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks). Członkowie PIIT konsultowali treść Kodeksu, PIIT deklaruje swoje poparcie dla idei utworzenia Kodeksu w proponowanym kształcie.

PIIT wyraża tym samym tym samym zgodę na współdziałanie z innymi organizacjami branżowymi w ramach Komitetu sterującego, o którym mowa w pkt. 7.1. Kodeksu i ustala zgodnie z pkt. 7.1.2.2. Kodeksu, iż Polska Federacja Szpitali będzie wnioskodawcą występującym o zatwierdzenie Kodeksu.

ZA ZGODNOŚĆ Z ORYGINAŁEM
Warszawa
dnia 13. 11. 2018
Tomasz Kaczyński
Radca Prawny WA-8646

Boris Stokalski-Dzierzykraj
Prezes Zarządu
Polska Izba Informatyki i Telekomunikacji

Polska Izba Informatyki i Telekomunikacji
Al. Jerozolimskie 136 - Eurocentrum Alfa, IX piętro
02-305 Warszawa
tel. +48 22 628-22-60, +48 22 628-24-06
fax +48 22 628-55-36
NIP 526-12-89-338, REGON 010220521

Warszawa, dnia 25 października 2018 r.

Anna Rulkiewicz

Prezes Zarządu

Związku Pracodawcy Medycyny Prywatnej

ul. Chodakowska 24 lok. 11

03-826 Warszawa

Szanowna Pani

dr Edyta Bielak–Jomaa

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, Związek Pracodawców Medycyny Prywatnej (dalej: ZPMP), wiodącej organizacji zrzeszającej prywatnych świadczeniodawców usług medycznych, wśród których znajdują się liderzy rynku pracowniczych programów zdrowotnych, spółki giełdowe oraz lokalni pracodawcy ochrony zdrowia, na podstawie art. 40 ust. 2 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 brał czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* (dalej: Kodeks). Członkowie MP konsultowali treść Kodeksu i deklarują swoje poparcie dla zatwierdzenia Kodeksu w proponowanym kształcie.

ZPMP wyraża tym samym zgodę na współdziałanie w ramach Komitetu sterującego, o którym mowa w pkt. 7.1. Kodeksu i ustala zgodnie z pkt. 7.1.2.2. Kodeksu, iż Polska Federacja Szpitali będzie wnioskodawcą występującym o zatwierdzenie Kodeksu.

ZA ZGODNOŚĆ Z ORYGINAŁEM
Warszawa
dnia 13. 11. 2018
Tomasz Kaczyński
Radca Prawny [illegible]-8646

Warszawa, dnia 5 listopada 2018 r.

Michał Czarnuch

Prezes Zarządu

Andrzej Osuch

Członek Zarządu

Fundacja Telemedyczna Grupa Robocza

Rondo Organizacji Narodów Zjednoczonych 1/XXI p.

00-124 Warszawa

Szanowna Pani

dr Edyta Bielak–Jomaa

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

OŚWIADCZENIE

Działając w imieniu Fundacji Telemedycznej Grupy Roboczej, niniejszym oświadczamy, że Fundacja Telemedyczna Grupa Robocza (dalej: TGR), organizacja branżowa zrzeszająca świadczeniodawców, producentów wyrobów medycznych, dostawców usług IT oraz ekspertów prawno-medycznych działających wspólnie na rzecz rozwoju telemedycyny w Polsce, na podstawie art. 40 ust. 2 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, brała zynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora achrony zdrowia"* w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks). Członkowie TGR konsultowali treść Kodeksu. TGR deklaruje poparcie dla idei utworzenia Kodeksu w proponowanym kształcie.

TGR wyraża tym samym zainteresowanie i zgodę na współdziałanie wraz z organizacjami branżowymi w ramach Komitetu sterującego, o którym mowa w pkt. 7.1. Kodeksu i ustala zgodnie z pkt. 7.1.2.2. Kodeksu, iż Polska Federacja Szpitali będzie wnioskodawcą występującym o zatwierdzenie Kodeksu.

ZA ZGODNOŚĆ Z ORYGINAŁEM
Warszawa
dnia 13. 11. 2018
Tomasz Kaczyński
Radca Prawny WA-8646

Andrzej Osuch

Michał Czarnuch

ZWIĄZEK PRACODAWCÓW
TECHNOLOGII CYFROWYCH
LEWIATAN

Warszawa, dnia 7 października 2018 r.

Piotr Marczuk
Prezes Zarządu Związku Pracodawców
Technologii Cyfrowych Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

Szanowna Pani
dr Edyta Bielak–Jomaa
Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, Związek Pracodawców Technologii Cyfrowych Lewiatan (dalej: ZPTC Lewiatan), organizacji zrzeszającej grupę wiodących firm IT w Polsce, na podstawie art. 40 ust. 2 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 brał czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks). Członkowie ZPTC Lewiatan konsultowali treść Kodeksu, ZPTC deklaruje swoje poparcie dla idei utworzenia Kodeksu w proponowanym kształcie.

ZPTC wyraża tym samym tym samym zgodę na współdziałanie z innymi organizacjami branżowymi w ramach Komitetu sterującego, o którym mowa w pkt. 7.1. Kodeksu i ustalają zgodnie z pkt. 7.1.2.2. Kodeksu, iż Polska Federacja Szpitali będzie wnioskodawcą występującym o zatwierdzenie Kodeksu.

Prezes ZPTC Lewiatan

Piotr Marczuk

ZA ZGODNOŚĆ Z ORYGINAŁEM
Warszawa
dnia 13. 11. 2018
Tomasz Kaczyński
Radca Prawny WA-8646

POROZUMIENIE ZIELONOGÓRSKIE
Federacja Związków Pracodawców Ochrony Zdrowia
65-048 Zielona Góra al. Niepodległości 16 p.10 tel./fax 0/68 325 72 97, 609 726 946, biuro.pz@op.pl

PZ/CF/18/064

Zielona Góra, dnia 6 listopada 2018 r.

Szanowna Pani
dr Edyta Bielak–Jomaa
Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2
00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że Federacja Związków Pracodawców Ochrony Zdrowia Porozumienie Zielonogórskie (dalej: PZ) działająca w 15 województwach, skupiająca 13 tysięcy lekarzy sprawujących opiekę nad 12 milionami pacjentów, stanowiąca największą organizację pracodawców ochrony zdrowia w Polsce, na podstawie art. 40 ust. 2 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 brała czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks). Członkowie PZ konsultowali treść Kodeksu, PZ deklaruje swoje poparcie dla idei utworzenia Kodeksu w proponowanym kształcie.

PZ wyraża tym samym tym samym zgodę na współdziałanie z innymi organizacjami branżowymi w ramach Komitetu sterującego, o którym mowa w pkt. 7.1. Kodeksu i ustala zgodnie z pkt. 7.1.2.2. Kodeksu, iż Polska Federacja Szpitali będzie wnioskodawcą występującym o zatwierdzenie Kodeksu.

Federacja Związków Pracodawców Ochrony Zdrowia
Porozumienie Zielonogórskie
Jacek Krajewski
Prezes Federacji PZ

ZA ZGODNOŚĆ Z ORYGINAŁEM
Warszawa
dnia 13.11.2018
Tomasz Kaczyński
Radca Prawny WA-8646

Federacja Związków Pracodawców Ochrony Zdrowia
Porozumienie Zielonogórskie
Marek Twardowski
Wiceprezes Federacji PZ

STANOWISKO Nr 61/18/VIII
PREZYDIUM NACZELNEJ RADY LEKARSKIEJ
z dnia 8 listopada 2018 r.

w sprawie projektu „ *Kodeksu branżowego dla sektora ochrony zdrowia*"

Prezydium Naczelnej Rady Lekarskiej, po zapoznaniu się z projektem „*Kodeksu branżowego dla sektora ochrony zdrowia*" (wersja z 30 października 2018 r.), powstałego w ramach inicjatywy www.rodowzdrowiu.pl, przekazanym przez przedstawiciela podmiotów wspierających - Kancelarię Domański, Zakrzewski, Palinka potwierdza poparcie dla idei jego utworzenia oraz ogólnego kierunku przyjętych w tym Kodeksie rozwiązań.

Prezydium Naczelnej Rady Lekarskiej w dniu 22 czerwca 2018 r. podjęło uchwałę Nr 12/18/P-VIII w sprawie przystąpienia Naczelnej Izby Lekarskiej w charakterze podmiotu wspierającego do prac nad powstaniem i aktualizowaniem Kodeksu branżowego dla sektora ochrony zdrowia. Treść Kodeksu była konsultowana przez samorząd lekarski, a uwagi do kolejnych wersji projektu przekazane zostały w Stanowisku Nr 9/18/VIII Prezydium Naczelnej Rady Lekarskiej z dnia 22 czerwca 2018 r. oraz Stanowisku Nr 31/18/VIII Prezydium Naczelnej Rady Lekarskiej z dnia 14 września 2018 r. Przedstawiciele Naczelnej Izby Lekarskiej brali czynny udział w procesie tworzenia „Kodeksu branżowego dla sektora ochrony zdrowia".

Jednocześnie uznając za uzasadnione wprowadzenie limitów przetwarzania, których przekroczenie oznacza przetwarzanie danych na dużą skalę Prezydium Naczelnej Rady Lekarskiej w dalszym ciągu postuluje konieczność dostosowania owych limitów do realiów udzielania świadczeń zdrowotnych przez średnie lub małe podmioty lecznicze i zwiększenie podanej liczby Unikalnych Pacjentów powyżej proponowanej (600). Przyjęte w projektowanym Kodeksie ilości graniczne, których przekroczenie miałoby oznaczać przetwarzanie szczególnych kategorii danych osobowych na dużą skalę są w ocenie Prezydium Naczelnej Rady Lekarskiej zbyt małe.
W ocenie Prezydium Naczelnej Rady Lekarskiej Kodeks powinien ponadto zawierać

stwierdzenie, iż incydentalne, występujące w jednym kwartale i nie wynikające z przyczyn strukturalnych przekroczenie podanej w punkcie 5.1.1.2 liczby Unikalnych Pacjentów (600 czy większej liczby – zgodnie z postulatem Prezydium Naczelnej Rady Lekarskiej), nie powoduje od razu uznania takiego PWDL za przetwarzającego dane na dużą skalę. Brak takiego zastrzeżenia może powodować niejasną sytuację prawną co do obowiązku zatrudniania inspektorów ochrony danych przez PWDL, u których liczba pacjentów, na rzecz których realizują świadczenia ma na przemian tendencje wzrostowe i spadkowe, balansujące wokół ustalonego w Kodeksie limitu przetwarzania na dużą skalę.

ZASTĘPCA SEKRETARZA
Artur Drobniak

PREZES
Andrzej Matyja

Krajowa Izba Fizjoterapeutów

Krajowa Izba Fizjoterapeutów
The Polish Chamber of Physiotherapists
Plac Stanisława Małachowskiego 2
00-066 Warszawa

Prezes
Krajowej Rady Fizjoterapeutów
Dr hab. n. med. Maciej Krawczyk

Warszawa, dnia 05 listopada 2018 r.

DA-SB.54.2018.PA.1

Szanowna Pani
dr Edyta Bielak–Jomaa
Prezes Urzędu Ochrony Danych Osobowych
ul. Stawki 2; 00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że przedstawiciele Krajowej Izby Fizjoterapeutów brali czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* przygotowanego w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks), konsultowali treść Kodeksu, deklarują swoje poparcie dla idei jego utworzenia i uznają za zasadne przyjęcie Kodeksu.

Prezes
Krajowej Rady Fizjoterapeutów

dr hab. n. med. Maciej Krawczyk

NACZELNA IZBA PIELĘGNIAREK I POŁOŻNYCH

Naczelna Rada Pielęgniarek i Położnych

NIPiP-NRPiP-DS.015.231.2018.MG

Warszawa, dnia 7 listopada 2018 r.

Zofia Małas
Prezes Naczelnej Rady Pielęgniarek i Położnych
ul. Pory 78, lok 10
02-757 Warszawa

Szanowna Pani
dr Edyta Bielak–Jomaa
Prezes Urzędu Ochrony Danych
Osobowych
ul. Stawki 2
00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że przedstawiciele Naczelnej Izby Pielęgniarek i Położnych brali czynny udział w procesie tworzenia „*Kodeksu branżowego dla sektora ochrony zdrowia*" przygotowanego w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks), konsultowali treść Kodeksu, deklarują swoje poparcie dla idei jego utworzenia i uznają za zasadne przyjęcie Kodeksu w proponowanym kształcie.

Prezes NRPiP

Zofia Małas

02-757 Warszawa, ul. Pory 78, lok. 10
tel.: (22) 327 61 61, fax (22) 327 61 60
www.nipip.pl, e-mail: nipip@nipip.pl

CSIOZ
Centrum Systemów Informacyjnych
Ochrony Zdrowia

Warszawa, 2018-11-06

2018-18853

Pani
dr Edyta Bielak–Jomaa
Prezes Urzędu Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

Szanowna Pani Prezes,

pragnę poinformować Panią Prezes, że przedstawiciele Centrum Systemów Informacyjnych Ochrony Zdrowia (Centrum) brali czynny udział w procesie tworzenia „Kodeksu branżowego dla sektora ochrony zdrowia" w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks), konsultowali treść Kodeksu, Centrum deklaruje swoje poparcie dla idei utworzenia Kodeksu i uznaje za zasadne przyjęcie Kodeksu w proponowanym kształcie.

Z poważaniem,

Dyrektor
Centrum Systemów Informacyjnych
Ochrony Zdrowia
(-) Bartłomiej Wnuk

Sporządził: Kosakowska Zuzanna

ul. Stanisława Dubois 5A | 00-184 Warszawa
tel.: +48 22 597-09-27 | fax: +48 22 597-09-37
biuro@csioz.gov.pl | www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/SkrytkaESP
NIP: 5251575309 | REGON: 001377706

Kraków, dnia 30 października 2018 r.

Halina Kutaj - Wąsikowska

Dyrektor Centrum Monitorowania Jakości

w Ochronie Zdrowia

ul. Kapelanka 60

30-347 Kraków

Szanowna Pani

dr Edyta Bielak–Jomaa

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

OŚWIADCZENIE

Niniejszym oświadczam, że przedstawiciele Centrum Monitorowania Jakości w Ochronie Zdrowia brali czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektoro ochrony zdrowio"* w ramach inicjatywy www.rodowzdrowiu.pl (dalej: Kodeks), konsultowali treść Kodeksu, deklarują swoje poparcie dla jego zatwierdzenia.

DYREKTOR
Centrum Monitorowania Jakości
w Ochronie Zdrowia
Halina Kutaj-Wąsikowska

CZŁONEK ZARZĄDU
WOJEWÓDZTWA WIELKOPOLSKIEGO
Maciej Sytek

Poznań, 22 października 2018 r.

POPARCIE DLA KODEKSU BRANŻOWEGO Z ART. 40 RODO

Niniejszym oświadczam, że przedstawiciele Samorządu Województwa Wielkopolskiego brali czynny udział w procesie tworzenia *„Kodeksu branżowego dla sektora ochrony zdrowia"* i deklarują swoje poparcie dla idei utworzenia powyższego dokumentu w proponowanym kształcie.

CZŁONEK ZARZĄDU
Maciej Sytek

Warszawa, dnia 26.07.2017 r.

List intencyjny

w sprawie współpracy nad kodeksem branżowym sektora ochrony zdrowia

dotyczącym ochrony danych osobowych

Zważywszy, że

- 25 maja 2018 roku obowiązywać zacznie Rozporządzenie 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, dalej jako: „RODO");
- artykuł 40 RODO zachęca do opracowywania przez organizacje branżowe kodeksów postępowania, które służyć będą doprecyzowaniu zakresu zastosowania przepisów RODO;
- organizacje pracodawców z branży ochrony zdrowia, organizacje Pacjentów oraz strona publiczna dostrzegają konieczność zapewnienia z jednej strony szczególnej ochrony przetwarzania danych medycznych Pacjentów, a z drugiej strony dostępu do tych danych w zakresie niezbędnym do efektywnej realizacji procesu terapeutycznego oraz rozwoju badań naukowych.

Sygnatariusze niniejszego listu widzą zasadność stworzenia oraz deklarują chęć współpracy nad opracowaniem kodeksu branżowego dla sektora ochrony zdrowia dotyczącego ochrony danych osobowych, który może pozwolić na osiągnięcie wskazanych wyżej celów oraz celu nadrzędnego – dobra Pacjenta. Opracowywanie kodeksu będzie opierało się na dialogu i współpracy organizacji branżowych sektora ochrony zdrowia, organizacji reprezentujących pacjentów i strony publicznej, a finalna treść kodeksu zostanie uzgodniona przez strony tworzące kodeks oraz wspierające jego powstanie.

Podmioty tworzące kodeks branżowy (organizacje branżowe)

Podmioty wspierające ideę powstania kodeksu branżowego

Członek Zarządu
Województwa Dolnośląskiego
Jerzy Michalak