KODEKS POSTĘPOWANIA
DLA SEKTORA OCHRONY ZDROWIA

WYDANY ZGODNIE Z ART. 40 RODO

DOTYCZĄCY PODMIOTÓW WYKONUJĄCYCH DZIAŁALNOŚĆ LECZNICZĄ
I PODMIOTÓW PRZETWARZAJĄCYCH

Warszawa, dnia 11 grudnia 2023 r.

Wnioskodawca:

PFSz
Polska Federacja Szpitali

Podmiot monitorujący:

KPMG

SPIS TREŚCI

1. WSTĘP

1.1. Celem Kodeksu jest zapewnienie adekwatnego poziomu ochrony Pacjentów, w związku z przetwarzaniem ich danych osobowych, ze szczególnym uwzględnieniem ochrony zdrowia i życia Pacjentów, jako dóbr o nadrzędnym znaczeniu.

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

1.3. Stosowanie Kodeksu stanowi okoliczność potwierdzającą wywiązywanie się z obowiązków nałożonych przez RODO na Administratorów danych oraz Podmioty przetwarzające, które działają na rynku podmiotów wykonujących działalność leczniczą. Tym samym Kodeks służy realizacji zasady rozliczalności.

1.4. Kodeks zawiera zbiór zasad mających służyć podnoszeniu poziomu ochrony danych osobowych, zgodnych z RODO i ustawodawstwem krajowym, który obejmuje 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.

1.5. Mając na uwadze specyfikę działalności poszczególnych PWDL, a także 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 oraz zgodnie z wymaganiami określonymi w 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 UODO.

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

1.7.1. strony publicznej – Centrum E-Zdrowia[1], 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 dla ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w działalności polskiego rynku PWDL, podmioty opracowujące Kodeks deklarują współpracę na rzecz:

1.8.1. podnoszenia poziomu ochrony danych osobowych w działalności polskiego rynku PWDL;

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 przyczyni się do skutecznego rozwoju e-zdrowia w Polsce, przy jednoczesnym zachowaniu właściwych i aktualnych standardów bezpieczeństwa oraz zapewnieniu 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] Dawniej jako Centrum Systemów Informacyjnych Ochrony Zdrowia (CSIOZ).

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 oraz 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

2.1. Wykaz skrótów

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

(b) **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;

(c) **Badanie naukowe –** badanie naukowe, o którym mowa w motywie 159 RODO, pojęcie to obejmuje również Eksperyment medyczny, w tym Badanie kliniczne;

(d) **Dokumentacja medyczna –** dokumentacja medyczna, o której mowa w przepisach ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz wydanych na jej podstawie aktach wykonawczych, a także określona w przepisach odrębnych;

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

(f) **Kodeks –** niniejszy dokument;

(g) **Opiekun faktyczny –** opiekun faktyczny w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta;

(h) **Osoba bliska -** małżonek, krewny lub powinowaty do drugiego stopnia w linii prostej, Przedstawiciel ustawowy, osoba pozostająca we wspólnym pożyciu lub osoba wskazana przez Pacjenta;

(i) **Osoba wykonująca zawód medyczny** - 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, farmaceuta, technik farmacji, psycholog, psychoterapeuta, logopeda, felczer, optometrysta, dietetyk, a także osoby wykonujące inne zawody wskazane w przepisach wykonawczych wydanych na podstawie art. 190 ust. 1 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. W przypadku, gdy w Kodeksie mowa o pielęgniarce lub lekarzu, rozumie się przez to również odpowiednio położną i lekarza dentystę;

(j) **Pacjent –** osoba zwracająca się o udzielenie świadczeń zdrowotnych lub korzystającą ze świadczeń zdrowotnych udzielanych przez podmiot udzielający świadczeń zdrowotnych lub Osobę wykonującą zawód medyczny;

(k) **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;

(l) **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. lub wniosku, o którym mowa w pkt. 7.4.1., które to zostały pozytywnie rozpatrzone zgodnie z procedurą wskazaną w Kodeksie**;**

(m) **Podmiot wykonujący działalność leczniczą (PWDL)** – podmiot leczniczy lub lekarz, pielęgniarka, położna lub fizjoterapeuta, wykonujący zawód w ramach działalności leczniczej jako praktykę zawodową, o których mowa w przepisach ustawy o działalności leczniczej;

(n) **Podmiot przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

(o) **Profilaktyka zdrowotna –** wszelkie działania mające na celu zapobieganie niekorzystnym zjawiskom w obszarze zdrowia Pacjenta;

(p) **Przedstawiciel ustawowy –** osoba umocowana do działania w cudzym imieniu na podstawie ustawy zgodnie z art. 96 Kodeksu cywilnego;

(q) **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;

(r) **Organ lub/i podmiot publiczny –** organy i podmioty sektora finansów publicznych w rozumieniu art. 9 ustawy o finansach publicznych oraz instytuty badawcze;

(s) **UODO –** Urząd Ochrony Danych Osobowych;

(t) **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.

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

2.2. Źródła prawa

(a) RODO;

(b) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej, dalej jako: „**dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej**”;

(c) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2009 r. Nr 52 poz. 417 z późn. zm., dalej jako: **„ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta”**);

(d) Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. z 2011 r. Nr 112 poz. 654 z późn. zm., dalej jako: „**ustawa o działalności leczniczej**”);

(e) Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 1964 r. Nr 16 poz. 93 z późn. zm., dalej jako: „**Kodeks cywilny**”);

(f) Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2009r. Nr 157 poz. 1240 z późn. zm., dalej jako: **„ustawa o finansach publicznych”**);

(g) Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U. z 1994 r. Nr 111 poz. 535 z późn zm.., dalej jako: **„ustawa o ochronie zdrowia psychicznego”**);

(h) Ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy (Dz.U. z 1997 r. Nr 96 poz. 593 z późn zm., dalej jako: **„ustawa o służbie medycyny pracy”**);

(i) Ustawa z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz.U. z 2006 r. Nr 191 poz. 1410 z późn. zm., dalej jako: „**ustawa o Państwowym Ratownictwie Medycznym”**);

(j) Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (Dz.U. z 2017 r. poz. 2217 z późn. zm., dalej jako: **„ustawa o podstawowej opiece zdrowotnej”**);

(k) Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. z 2004 r. Nr 210 poz. 2135 z późn. zm., dalej jako: **„ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych”**);

(l) Ustawa z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz.U. z 1997 r. Nr 106 poz. 681 z późn. zm., dalej jako: **„ustawa o publicznej służbie krwi”**);

(m) Ustawa z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (Dz.U. z 2005 r. Nr 169 poz. 1411 z późn. zm., dalej jako: **„ustawa o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów”**);

(n) Ustawa z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. z 2008 r. Nr 234 poz. 1570 z późn. zm., dalej jako: **„ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi”**);

(o) Ustawa z dnia 25 czerwca 2015 r. o leczeniu niepłodności (Dz.U. z 2015 r. poz. 1087 z późn. zm., dalej jako: **„ustawa o leczeniu niepłodności”**);

(p) Ustawia z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r. Nr 113 poz. 657 z późn. zm.**,** dalej jako: **„ustawa o systemie informacji w ochronie zdrowia”**);

(q) Ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (Dz.U. z 1999 r. Nr 60 poz. 636 z późn.

zm., dalej jako: „**ustawa o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa**”);

(r) Ustawa z dnia 6 września 2001 r. Prawo farmaceutyczne (Dz.U. z 2001 r. Nr 126 poz. 1381 z późn. zm., dalej jako: **„Prawo farmaceutyczne”)**;

(s) Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz.U. z 1997 r. Nr 28 poz. 152 z późn. zm., dalej jako: **„ustawa o zawodach lekarza i lekarza dentysty”);**

(t) Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 r. poz. 1000 z późn. zm., dalej jako: **„ustawa o ochronie danych osobowych”**);

(u) Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 1960 r. Nr 30 poz. 168 z późn. zm., dalej jako: **„Kodeks postępowania administracyjnego**”).

Nowelizacje oraz teksty jednolite powyższych aktów prawnych dostępne są w Dzienniku Ustaw Rzeczypospolitej Polskiej[2] oraz w Internetowym Systemie Aktów Prawnych[3].

[2] www.dziennikustaw.gov.pl
[3] www.isap.sejm.gov.pl

3. ZAKRES KODEKSU

3.1. Kryterium podmiotowe stosowania Kodeksu

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

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 na zlecenie PWDL przetwarzają 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.

3.1.5. Stosowanie Kodeksu jest dobrowolne.

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 PWDL 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;

3.2.1.2. przetwarzanie danych w innych celach.

3.2.2. Kodeks nie reguluje czynności przetwarzania prowadzonych w kilku państwach członkowskich w rozumieniu art. 40 ust. 7 RODO. PWDL lub Podmiot przetwarzający, którzy zaangażowani są w czynności przetwarzania w kilku państwach członkowskich w dalszym ciągu mogą uzyskać status Podmiotów przestrzegających Kodeksu. Status

ten będzie dotyczyć czynności przetwarzania, w zakresie, w jakim nie są one realizowane w kilku państwach członkowskich.

3.2.3. 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 PWDL są bezpośrednio właściwe przepisy RODO pozostające w związku z przepisami krajowego prawa medycznego. 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, określonego w szczególności w pkt. 4.1.4 i 4.1.5.

4.1.2. W szczególności PWDL może 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; oraz

4.1.2.2. przepisów polskich ustaw z obszaru prawa medycznego, pozostających w związku z celami zdrowotnymi przetwarzania i 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.

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:

(a) ustawie o ochronie zdrowia psychicznego;

(b) ustawie o służbie medycyny pracy;

(c) ustawie o Państwowym Ratownictwie Medycznym;

(d) ustawie o podstawowej opiece zdrowotnej;

(e) ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;

(f) ustawie. o publicznej służbie krwi;

(g) ustawie o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów;

(h) ustawie o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi;

(i) ustawie o leczeniu niepłodności;

(j) ustawie o systemie informacji w ochronie zdrowia.

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 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 do celów:

4.2.2.1. Profilaktyki zdrowotnej

4.2.2.1.1. cel ten obejmuje przetwarzanie związane z procesem udzielania świadczeń zdrowotnych realizowanych na potrzeby Profilaktyki zdrowotnej;

4.2.2.1.2. Profilaktyka zdrowotna może być realizowana w ramach działań własnych PWDL wobec Pacjentów PWDL, jak również w ramach programów profilaktycznych utworzonych i realizowanych na podstawie odrębnych przepisów przez Organy i podmioty publiczne.

4.2.2.1.3. Profilaktyka zdrowotna może obejmować w szczególności:

a) działania podejmowane w celu prewencji chorób, w szczególności:

4.2.2.1.3.a.1. kierowanie zaproszeń na badania przesiewowe, w tym realizowane w ramach programów badań przesiewowych ustanowionych przez organy publiczne, w szczególności przez ministra właściwego do spraw zdrowia, jednostki samorządu terytorialnego lub Narodowy Fundusz Zdrowia; realizowane w ramach programów zdrowotnych, programów polityki zdrowotnej lub programów pilotażowych, o których mowa w art. 48 i nast. ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;

4.2.2.1.3.a.2. kierowanie zaproszeń na wykonanie szczepień, w szczególności szczepień zalecanych, zgodnie z obowiązującym Programem Szczepień Ochronnych[4].

b) działania niezbędne do zapewnienia Pacjentowi ciągłości świadczeń zdrowotnych, w szczególności:

4.2.2.1.3.b.1. komunikacja dotycząca zasadności wykonania wizyty kontrolnej u lekarza, lekarza dentysty lub innej Osoby wykonującej zawód medyczny, w przypadku upływu określonego, uzasadnionego wskazaniami medycznymi czasu od ostatniej wizyty Pacjenta w PWDL;

4.2.2.1.3.b.1. komunikacja i udzielanie porad patronażowych, wykonywanie wizyt patronażowych, badań bilansowych i testów przesiewowych;

4.2.2.1.3.b.2. telekonsultacje medyczne, w tym realizowane w celu zapewnia koordynowanej opieki medycznej;

4.2.2.2. Kierowanie zaproszeń na wykonanie szczepień, w szczególności szczepień obowiązkowych – podstawowych i uzupełniających, zgodnie z obowiązującym Programem Szczepień Ochronnych. Przetwarzanie danych osobowych Pacjenta do celów Profilaktyki zdrowotnej w zakresie działań podejmowanych w celu prewencji chorób może mieć miejsce, kiedy jest uzasadnione czynnikami ryzyka oraz wynika ze wskazań aktualnej wiedzy medycznej, wskazań statystycznych lub też, jeżeli wynika ono z przepisów prawa dotyczących Profilaktyki zdrowotnej;

4.2.2.3. Przetwarzanie danych osobowych Pacjenta do celów Profilaktyki zdrowotnej w zakresie działań do zapewnienia Pacjentowi ciągłości świadczeń zdrowotnych jest niezbędne wtedy, kiedy jest uzasadnione stanem zdrowia Pacjenta lub czynnikami ryzyka lub rokowaniami co do niego zawartymi w Dokumentacji medycznej, którą dysponuje PWDL oraz wynika ze wskazań aktualnej wiedzy medycznej;

4.2.2.3.1. przetwarzanie danych osobowych Pacjenta do celów Profilaktyki zdrowotnej realizowane jest z zapewnieniem jednoznacznego oddzielenia procesu przetwarzania danych osobowych w ramach Profilaktyki zdrowotnej od procesu marketingu i sprzedaży, w szczególności poprzez:

a) nieangażowanie w przetwarzanie danych osobowych do celów Profilaktyki zdrowotnej personelu zajmującego się marketingiem i sprzedażą, w szczególności w zakresie działań niezbędnych do zapewnienia Pacjentowi ciągłości świadczeń zdrowotnych.

[4] Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi przewiduje obowiązkowe szczepienia ochronne oraz zalecane szczepienia ochronne. Zgodnie z art. 17 ust. 11 wskazanej ustawy, program szczepień ochronnych na dany rok ogłaszany jest przez Głównego Inspektora Sanitarnego w formie komunikatu w dzienniku urzędowym ministra właściwego do spraw zdrowia.

W przetwarzanie danych osobowych powinny być zaangażowane Osoby wykonujące zawód medyczny. Na polecenie i pod nadzorem Osoby wykonującej zawód medyczny, w przetwarzanie danych osobowych do celów Profilaktyki zdrowotnej w niezbędnym do tego zakresie, mogą być zaangażowane także osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych[5];

b) oddzielenie komunikacji prowadzonej do celów Profilaktyki zdrowotnej od komunikacji marketingowej kierowanej do Pacjenta;

c) zapewnienie, aby w treści komunikacji dotyczącej Profilaktyki zdrowotnej, wykorzystywane były obiektywne informacje zgodne z aktualną wiedzą medyczną. Zachęta do skorzystania ze Świadczeń zdrowotnych powinna odnosić się wyłącznie do możliwych do uzyskania korzyści zdrowotnych, które wynikają z prowadzonej Profilaktyki zdrowotnej, a nie do korzyści wynikających z ceny świadczenia, wykorzystywanego sprzętu czy innych przymiotów świadczenia lub korzyści mających przemawiać za skorzystaniem z usług danego PWDL. Zachęta do skorzystania ze Świadczeń zdrowotnych nie może również być oparta na wywołaniu u Pacjenta poczucia strachu, na wypadek, gdyby z takiego świadczenia nie skorzystał.

4.2.2.3.2. PWDL informuje Pacjenta o zasadach realizacji świadczeń zdrowotnych w ramach realizowanej Profilaktyki zdrowotnej, w szczególności o zasadach kierowania do Pacjenta komunikacji za pomocą systemów teleinformatycznych lub systemów łączności. Pacjent może w każdym czasie w dowolnej formie skutecznie sprzeciwić się kierowaniu do niego komunikacji w ramach realizacji Profilaktyki zdrowotnej, chyba że co innego wynika z obowiązujących przepisów dotyczących realizacji Profilaktyki zdrowotnej. PWDL utrwala zgłoszony przez Pacjenta sprzeciw w dokumentacji medycznej. Wskazany sprzeciw stanowi odmowę zgody na udzielenie świadczenia zdrowotnego, o której mowa w art. 15 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

4.2.2.3.3. PWDL informuje Pacjenta o zasadach realizacji świadczeń zdrowotnych w ramach realizowanej Profilaktyki zdrowotnej oraz o możliwości zgłoszenia sprzeciwu, o którym mowa w pkt. 4.2.2.3.2 oraz o konsekwencji takiego sprzeciwu, pkt 6.3.2. stosuje się odpowiednio;

4.2.2.3.4. przetwarzanie danych w celu Profilaktyki zdrowotnej odbywa się co do zasady:

[5] W szczególności Osoba wykonująca zawód medyczny może podjąć decyzję o nawiązaniu kontaktu z Pacjentem lub Pacjentami w taki sposób, że wiadomość zostanie przesłana przez osobę wykonującą czynności pomocnicze przy udzielaniu świadczeń zdrowotnych w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

a) w zakresie działań podejmowanych w celu prewencji chorób - na podstawie art. 6 ust. 1 lit. e) RODO w związku z zadaniem realizowanym w interesie publicznym w dziedzinie zdrowia;

b) w zakresie działań niezbędnych do zapewnienia Pacjentowi ciągłości świadczeń zdrowotnych - 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;

4.2.2.3.5. przetwarzanie związane z procesem udzielania świadczeń zdrowotnych, realizowanych na potrzeby Profilaktyki zdrowotnej, należy wykazać w rejestrze czynności przetwarzania.

4.2.2.4. medycyny pracy, w tym oceny zdolności pracownika do pracy,

4.2.2.4.1. 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;

4.2.2.4.2. przetwarzanie danych w tym celu odbywa się co do zasady na podstawie art. 9 ust. 2 lit. h) RODO w związku z art. 6 i 11 ustawy o służbie medycyny pracy;

4.2.2.5. diagnozy medycznej i leczenia,

4.2.2.5.1. cel ten obejmuje w szczególności przetwarzanie związane z procesem udzielania świadczeń zdrowotnych (diagnostycznych i leczniczych), w tym prowadzenie Dokumentacji medycznej, jak również komunikację po udzieleniu świadczenia w celu oceny stanu zdrowia Pacjenta. Wspomniana wyżej komunikacja stanowi element tego Świadczenia zdrowotnego, gdy jest uzasadniona względami medycznymi, w szczególności rodzajem wykonanego Świadczenia zdrowotnego, wynikiem badania lub rozpoznaniem;

4.2.2.5.2. przetwarzanie danych w tym celu odbywa się co do zasady 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;

4.2.2.6. zapewnienia opieki zdrowotnej oraz zarządzania systemami i usługami opieki zdrowotnej,

4.2.2.6.1. cel ten obejmuje w szczególności przetwarzanie związane z:

a) rejestracją Pacjenta w PWDL;

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

c) 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;

d) odbieraniem i archiwizacją oświadczeń woli Pacjentów;

e) pozyskiwaniem informacji zarządczych/ zarządzaniem PWDL;

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

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

h) 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);

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

4.2.2.7. zapewnienia zabezpieczenia społecznego oraz zarządzania systemami i usługami zabezpieczenia społecznego,

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

4.2.2.7.2. przetwarzanie danych w tym celu odbywa się na podstawie art. 9 ust. 2 lit h) RODO, co do zasady 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 zdrowotnych upoważnione są osoby, o których mowa w art. 9 ust. 3 RODO. Osobami tymi będą osoby wskazane w pkt. 4.7.

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

4.3.1. Dane osobowe Pacjenta, mogą być przetwarzane przez PWDL bez wymagania 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).

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

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. 4.4.1., 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. Co do zasady gromadzenie danych obejmujących adres e-mail lub numer telefonu jest adekwatne do celów zdrowotnych, mimo że nie są to dane minimalne, wymagane przez przepisy prawa.

4.4.3. Zakwalifikowanie przetwarzanych przez PWDL danych osobowych Pacjenta jako niestanowiących Dokumentacji medycznej, np. danych zawartych w dokumentacji rozliczeniowej, raportach zarządczych[6], ankietach ds. jakości itp. nie przesądza o możliwości ich przetwarzania zgodnie z pkt. 4.2.2. Oznacza to, iż dane osobowe Pacjenta nieujęte w Dokumentacji medycznej mogą również być przetwarzane w celach zdrowotnych.

4.5. Przetwarzanie danych na podstawie zgody Pacjenta.

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[7]:

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, realizowanych na zasadach określonych w Kodeksie, nawet jeżeli skutkiem tego przetwarzania jest zwiększenie popytu na usługi świadczone przez PWDL (nie wyklucza to możliwości, stosownie do

[6] Np. raporty dotyczące rachunku kosztów.

[7] Przetwarzanie danych przez PWDL na podstawie zgody będzie rzadką sytuacją i będzie następować tylko w określonych przypadkach – co do zasady PWDL przetwarzają dane osobowe bez zgody Pacjenta (por. pkt 4.5.). Rekomenduje się prowadzenie rejestru udzielonych zgód. Dobrą 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, daty przyjęcia zgody.

sytuacji, przetwarzania danych osobowych zwykłych w celach marketingowych także w oparciu o inną podstawę- uzasadniony interes Administratora)[8];

4.5.1.2. przetwarzanie danych realizowane jest w związku z realizacją Badań klinicznych[9], 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 nienależących do szczególnych kategorii danych osobowych ma być zgoda Pacjenta**,** o której mowa w art. 6 ust. 1 lit. a) RODO, 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[10]. W przypadku upoważnienia do dostępu do Dokumentacji medycznej, uwzględnia się dodatkowo przepisy dotyczące Dokumentacji medycznej.

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. W przypadku, gdy podstawą prawną przetwarzania szczególnych kategorii danych osobowych jest zgoda, o której mowa w art. 9 ust. 2 lit. a) RODO, zgoda powinna zostać wyrażona poprzez złożenie wyraźnego oświadczenia woli w formie ustnej lub

[8] Zwracamy uwagę, że Administrator może przetwarzać dane osobowe zwykłe w celach marketingowych niekiedy 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 RODO. 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).

[9] Zgodnie z przepisami wykonawczymi wydanymi na podstawie art. 37g ustawy Prawo farmaceutyczne.

[10] W przypadku upoważnienia do dostępu do dokumentacji medycznej, uwzględnia się dodatkowo przepisy dotyczące dokumentacji medycznej, wydane na podstawie art. 30 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

pisemnej lub za pomocą systemu teleinformatycznego. Zgoda musi spełniać kryteria zgody wyraźnej zgodnie z wytycznymi Europejskiej Rady Danych Osobowych[11]. Zgody na przetwarzanie szczególnych kategorii danych osobowych nie można domniemywać na podstawie innych czynności (niedopuszczalne jest powoływanie się na udzielenie przez Pacjenta zgody dorozumianej).

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

4.5.6. Z uwagi na fakt, że relacja pomiędzy Pacjentem, a Osobą wykonującą zawód medyczny lub osobą wykonującą czynności pomocnicze przy udzielaniu świadczeń zdrowotnych lub PWDL ma charakter niesymetryczny i jest oparta na zaufaniu - PWDL i jego personel zobowiązani są 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.

4.5.7. Pacjent ma prawo wycofać zgodę w każdym momencie. Wycofanie zgody powinno następować w równie prosty sposób, jak jej wyrażenie i bez ponoszenia przez Pacjenta kosztów. 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.

4.5.8. 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, rejestrowanie rozmów telefonicznych lub posiadanie skryptów rozmów telefonicznych, dokonywanie kopii zapasowych (backupów lub zrzutów z ekranu), odznaczenie odpowiednich symboli (tricków) w bazach danych, posiadanie stosownych polityk i procedur wewnętrznych oraz notatek z przebiegu spotkań.

4.5.9. 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, w szczególności treść obowiązku informacyjnego realizowanego zgodnie z art. 13 RODO.

[11] Wytyczne 5/2020 w sprawie zgody na mocy rozporządzenia 2016/679, dostęp: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pl.pdf

4.5.10. 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.), 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;

4.6.2.3. inny PWDL udostępniający dane na potrzeby zachowania ciągłości usług medycznych, w tym w ramach podwykonawstwa udzielania świadczeń, 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)[12];

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 przy wykorzystaniu środków technicznych i organizacyjnych PWDL, w tym:

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

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;

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.

4.6.5. Z PWDL innymi 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

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 oraz

czynności związane z zapewnieniem bezpieczeństwa tego systemu, na podstawie upoważnienia Administratora[13].

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

4.7.2.1. PWDL jako Administrator, może zdecydować o nadawaniu upoważnień do przetwarzania danych osobowych Osobom wykonującym zawód medyczny przetwarzającym dane Pacjentów w ramach wykonywania zawodu jako jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania[14].

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.

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

[13] 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.

[14] Nadając upoważnienia, PWDL uwzględnia stanowiska UODO w przedmiocie nadawania upoważnień, w tym stanowiska opublikowane na stronie internetowej UODO, np. https://archiwum.uodo.gov.pl/pl/225/1578.

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), a nie w ramach upoważnienia zbiorczego[15].

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[16], 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[17].

4.8.2. Podmiot, któremu udostępniane są dane osobowe Pacjenta w sposób wskazany w pkt. 4.8.1. jest, bądź staje się ich Administratorem[18].

4.8.3. PWDL może w celu udostępniania danych osobowych Pacjenta, które są zawarte 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. Serwery te mogą w szczególności stanowić element platform wymiany danych obsługiwanych przez podmioty świadczące usługę prowadzenia

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

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

[17] 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.

[18] 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 najbliższe.

repozytorium. Działania takie w przypadku przetwarzania danych na obszarze Europejskiego Obszaru Gospodarczego nie wymagają uzyskania od Pacjentów zgody na przetwarzanie danych osobowych.

4.8.4. W przypadku udostępniania Pacjentowi informacji dotyczących pojedynczego Świadczenia zdrowotnego, zawartych w Dokumentacji medycznej, 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;

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

4.8.6. Upoważnienie zawiera co najmniej następujące elementy:

4.8.6.1. jednoznaczną identyfikację Pacjenta (przykładowy katalog danych do identyfikacji wskazany został w załączniku nr 2 do Kodeksu);

4.8.6.2. jednoznaczną identyfikację osoby udzielającej upoważnienia;

4.8.6.3. jednoznaczną identyfikacja osoby, której udzielane jest upoważnienie, poprzez wskazanie imienia i nazwiska tej osoby (w przypadku osoby fizycznej), bądź nazwy lub firmy i adresu jej siedziby (w przypadku osoby prawnej). PWDL może utrwalić dodatkowe informacje o osobie upoważnionej wyłącznie, gdy:

a) w PWDL znajduje się więcej niż jeden Pacjent lub osoba upoważniona o tym samym imieniu i nazwisku (przykładowy katalog danych do identyfikacji wskazany został w załączniku nr 2 do Kodeksu);

b) osoba udzielająca upoważnienia samodzielnie i niezależnie od PWDL podaje dodatkowe dane osobowe o osobie upoważnionej (PWDL nie ingeruje w treść oświadczenia woli);

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. 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. Próbki materiału biologicznego, takie jak: komórki, tkanki, płyny ustrojowe, wydzieliny i wydaliny[19] nie stanowią danych osobowych**,** jeżeli nie są powiązane z danymi pozwalającymi na ustalenie tożsamości osoby, od której zostały pobrane**.**

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

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 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. W takiej sytuacji PWDL ocenia pod kątem adekwatności do konkretnej sytuacji i okoliczności, w szczególności okoliczności wskazanych w pkt. 4.10.2., oraz stanu Pacjenta, zakres danych, który może zostać przekazany.

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;

[19] 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).

4.10.2.2. 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[20];

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

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 pkt z uzasadnieniem zaistnienia stanu zagrożenia dla życia lub zdrowia Pacjenta;

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 połączenie na numer telefonu uprzednio wskazany przez Pacjenta w Dokumentacji medycznej;

4.10.3.3.3. zadawanie pytań kontrolnych dotyczących Pacjenta osobie trzeciej, która powinna znać na nie odpowiedzi;

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. Monitoring wizyjny

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

4.11.1. PWDL może dokonywać przy użyciu kamer obserwacji miejsc, w których prowadzi działalność leczniczą oraz utrwalać obraz pozyskany przy użyciu tych kamer, w tym zawierający dane osobowe (monitoring). Monitoring oraz nagrywanie udzielania świadczeń zdrowotnych, o którym mowa w punkcie 4.12, może się odbywać jedynie na podstawie zgody albo innej podstawy prawnej.

4.11.2. Głównym celem prowadzenia przez PWDL monitoringu jest zapewnienie bezpieczeństwa Pacjentom oraz personelowi PWDL. Przed zastosowaniem monitoringu, PWDL zobowiązany jest do dokonania oceny ryzyka, w tym analizy skuteczności stosowania monitoringu pod kątem postanowionych mu celów[21] (poprawa bezpieczeństwa) oraz wpływu monitoringu na realizację praw Pacjentów, takich jak ochrona prywatności, poszanowanie godności oraz intymności. W przypadku wysokiego ryzyka naruszenia praw i wolności Pacjentów, niezbędne będzie przeprowadzenie oceny skutków dla ochrony danych, o której mowa w art. 35 RODO, nawet jeśli przetwarzanie nie jest przetwarzaniem na dużą skalę, o którym mowa w art. 35 ust. 3 lit. b) RODO.

4.11.3. PWDL uprawniony jest do stosowania monitoringu w miejscach:

4.11.3.1. ogólnodostępnych, takich jak: recepcja, szatnia na okrycia wierzchnie lub obuwie, poczekalnia, stołówka, wejścia do budynku, ciągi komunikacyjne[22], jeżeli jest to niezbędne dla zapewnienia bezpieczeństwa Pacjentów oraz personelu PWDL, w tym zapobieżenia incydentom zagrażającym temu bezpieczeństwu (np. agresywne zachowania, pobicia);

4.11.3.2. udzielania świadczeń zdrowotnych oraz pobytu Pacjentów w zakresie wynikającym z przepisów odrębnych (oddziały dziecięce, oddziały psychiatryczne, zespół porodowy, stacje dializ, anestezjologia i intensywna terapia, pokoje łóżkowe**,** jeżeli jest to konieczne w procesie leczenia i dla zapewnienia Pacjentom bezpieczeństwa[23]).

[21] Monitoring nie może wzbudzać u Pacjenta błędnego poczucia bezpieczeństwa (np. słaba jakość kamer, która uniemożliwia wykorzystanie nagrań lub montowanie atrap kamer), jak również budzić u pacjenta obawę naruszenia jego godności lub intymności (np. skierowanie kamery na konkretnego Pacjenta, podczas gdy monitoringowi powinno podlegać całe pomieszczenie). Nieuprawnione jest także montowanie przez PWDL kamer ukrytych, które nie mogą zostać przez Pacjenta zidentyfikowane jako sprzęt rejestrujący obraz.

[22] Do ciągów komunikacyjnych, które mogą być monitorowane zalicza się również np. korytarz na oddziale, w tym na SOR.

[23] Monitorowanie pokoi łóżkowych realizowane zgodnie z przepisami wykonawczymi wydanymi na podstawie art. 22 ust. 3 ustawy o działalności leczniczej, powinno być rozumiane jako możliwość bieżącego podglądu bez nagrywania, chyba że nagranie zgodnie ze wskazaniami wiedzy medycznej stanowić ma część dokumentacji medycznej.

4.11.4. PWDL przetwarza dane osobowe przy użyciu monitoringu w oparciu o następujące podstawy prawne:

4.11.4.1. w zakresie wynikającym z pkt. 4.11.3.1.:

a) w stosunku do danych niebędących danymi, o których mowa w art. 9 ust. 1: art. 6 ust. 1 lit. e) lub f)[24] RODO w związku z art. 23 a ust. 1 pkt 1 ustawy o działalności leczniczej;

b) w stosunku do danych Pacjentów będących danymi, o których mowa w art. 9 ust. 1 podstawę prawną przetwarzania stanowić będzie art. 9 ust. 2 lit. i) RODO w związku z art. 23 a ust. 1 pkt 2 ustawy o działalności leczniczej, tj. zapewnienie bezpieczeństwa opieki zdrowotnej.

4.11.4.2. w zakresie wynikającym z pkt**.** 4.11.3.2. – art. 9 ust. 2 lit. h) RODO jako realizacja celów zdrowotnych oraz przepisów 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[25].

4.11.5. Dane osobowe, uzyskane w wyniku prowadzenia monitoringu, PWDL przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje je przez okres nie dłuższy niż 3 miesiące. Po upływie tego okresu nagranie zawierające dane osobowe, podlega zniszczeniu lub anonimizacji, chyba że przepisy odrębne stanowią inaczej.

4.11.6. PWDL zobowiązany jest zapewnić, aby dostęp do nagrań monitoringu wizyjnego pomieszczeń oraz do nagrań wskazanych w pkt. 4.11.6. zawierających dane osobowe, został zabezpieczony przy użyciu odpowiednich środków technicznych oraz organizacyjnych.

4.11.7. Powyższe punkty (4.11.1-4.11.6) nie mają zastosowania do monitoringu, w szczególności monitoringu pracowników, prowadzonego na podstawie przepisów prawa pracy.

4.12. Nagrywanie udzielania świadczeń zdrowotnych

4.12.1. Niezależnie od postanowień pkt**.** 4.11.1-4.11.5. PWDL może dokonywać utrwalenia przebiegu całości przeprowadzanych na rzecz Pacjenta zabiegów lub ich części przy użyciu sprzętu rejestrującego obraz lub obraz i dźwięk:

4.12.1.1. w celach zdrowotnych, jeżeli jest to uzasadnione rodzajem wykonywanego Świadczenia zdrowotnego jako dokumentacji z przebiegu udzielanego Świadczenia zdrowotnego i włączenia utrwalonego obrazu lub obrazu i dźwięku do Dokumentacji medycznej Pacjenta. W takim przypadku utrwalona treść stanowi integralną część Dokumentacji medycznej i jest przechowywana

[24] Z wyłączeniem organów publicznych w ramach realizacji swoich zadań.
[25] Np. Przepisy wykonawcze wydane na podstawie art. 22 ust. 3 i ust. 5 ustawy o działalności leczniczej.

zgodnie z przepisami regulującymi sposób prowadzenia oraz przechowywania Dokumentacji medycznej[26];

4.12.1.2. w innych celach niż cele zdrowotne[27], jednakże za wyraźną zgodą Pacjenta, o której mowa w art. 9 ust. 2 lit. a) pobraną zgodnie z pkt. 4.5.

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

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

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, w szczególności, 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:

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 miejscu wezwania.

5.2. Inspektor Ochrony Danych

5.2.1. PWDL powołują Inspektora Ochrony Danych zgodnie z zasadami określonymi w art. 37 ust. 1 RODO, preambule RODO oraz wytycznymi krajowych i europejskich organów właściwych w zakresie ochrony danych osobowych.

[26] Utrwalanie realizowane w celach zdrowotnych obejmuje np. przebieg zabiegów endoskopowych, monitorowanie pola operacyjnego, badanie zaburzeń snu.
[27] Np. cele badań naukowych, cele komercyjne, szkoleniowe.

5.2.2. PWDL wskazane w pkt. 5.1.1., z wyłączeniem Organów i podmiotów publicznych, nie są zobligowane do powoływania Inspektora Ochrony Danych na podstawie przesłanki wskazanej w art. 37 ust. 1 lit. c) RODO. Pomimo nieprzetwarzania danych na dużą skalę w rozumieniu pkt. 5.1.1., powołanie Inspektora Ochrony Danych może być konieczne także na podstawie innych przesłanek wskazanych w art. 37 ust. 1 RODO.

5.2.3. W przypadku, gdy wskutek zmiany skali przetwarzania danych osobowych PWDL zobowiązany jest do powoływania Inspektora Ochrony Danych na podstawie przesłanki wskazanej w art. 37 ust. 1 lit. c) RODO na potrzeby stosowania Kodeksu przyjmuje się, że powołanie Inspektora Ochrony Danych na podstawie przesłanki wskazanej w art. 37 ust. 1 lit. c) RODO oznacza obowiązek jego dalszego utrzymania.

5.2.4. Inspektorem Ochrony Danych w PWDL może być członek personelu PWDL niezależnie od formy świadczenia pracy lub przedstawiciel zewnętrznego podmiotu, który dysponuje wiedzą fachową na temat prawa w dziedzinie ochrony danych osobowych i działalności leczniczej oraz posiada znajomość specyfiki sektora ochrony zdrowia. Osoba taka nie jest zobligowana do legitymizowania się ukończeniem określonych studiów lub nabyciem określonych uprawnień (brak obowiązku posiadania formalnego wykształcenia).

5.2.5. Inspektor Ochrony Danych nie może zajmować w PWDL stanowiska związanego z określaniem sposobów i celów przetwarzania danych. Aspekt ten powinien być analizowany osobno i indywidualne dla każdego PWDL z uwzględnieniem jego celów i zadań, struktury organizacyjnej oraz organizacji i zadań poszczególnych jednostek lub komórek organizacyjnych, określonych w regulaminie organizacyjnym PWDL[28].

5.2.6. Osoba wykonująca zawód medyczny nie może być Inspektorem Ochrony Danych w prowadzonej przez siebie praktyce zawodowej prowadzonej w ramach jednoosobowej działalności gospodarczej.

5.2.7. Inspektor Ochrony Danych wykonuje zadania określone w art. 39 RODO. Inspektor Ochrony Danych może wykonywać w PWDL także zadania niezwiązane z pełnieniem tej funkcji tylko w takim zakresie, w jakim nie stanowi to przeszkody, w szczególności ze względu na zaangażowanie czasowe oraz możliwy konflikt interesów, dla rzetelnego wypełniania zadań Inspektora Ochrony Danych.

5.2.8. Inspektor Ochrony Danych jest włączany we wszystkie sprawy dotyczące ochrony danych osobowych. W szczególności powinien mieć możliwość konsultowania projektów zmian w obowiązujących procedurach, politykach z tego zakresu, a także możliwość konsultowania projektów zawieranych umów, które wiążą się z udostępnianiem danych osobowych.

[28] Z określaniem sposobów i celów przetwarzania danych wiążą się zazwyczaj stanowiska kierownicze, takie jak dyrektor PWDL, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT.

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

5.3.1. 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).

5.3.2. 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.

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

5.3.3.1. wynikają one z przeprowadzonej właściwie analizy ryzyka; oraz

5.3.3.2. 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 nr 6 do Kodeksu, w odniesieniu do zagadnień objętych tymi normami/standardami.

5.3.4. Przyjmuje się, że warunek wskazany w pkt. 5.3.2. oraz wskazany w pkt. 5.3.3. może być w całości lub części spełniony poprzez wdrożenie alternatywnego (uproszczonego) podejścia wskazanego w załączniku nr 7 do Kodeksu w odniesieniu do PWDL, które:

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

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

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

5.3.6. PWDL ustanawia wewnętrzne zasady stwierdzania oraz postępowania w przypadku podejrzenia i stwierdzenia naruszenia ochrony danych osobowych;

5.3.7. PWDL dokumentuje wszelkie podejrzenia naruszenia ochrony danych oraz wszelkie naruszenia ochrony danych osobowych;

5.3.8. PWDL ustanawia wewnętrzne zasady, np. w formie procedur postępowania, realizacji obowiązków wynikających z art. 25 RODO, tj. zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

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

5.4.1. PWDL, które nie przetwarzają na dużą skalę danych w związku ze spełnianiem kryteriów określonych w pkt. 5.1., nie muszą przeprowadzać oceny skutków dla ochrony danych w oparciu o okoliczność wskazaną w art. 35 ust. 3 lit**.** b) RODO.

5.4.2. 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.

5.4.3. 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. 5.3.

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

5.4.5. 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.

5.4.6. 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 do Kodeksu bądź załącznik nr 7 do Kodeksu. Administrator danych może stosować inne równoważne metodyki analizy ryzyka zapewniające nie mniejszą skuteczność w zarządzaniu ryzykiem niż standardy zaproponowane w Kodeksie.

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

5.4.7.1. wynikają one z przeprowadzonej właściwie analizy ryzyka oraz

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

5.4.8. Administrator może stosować środki techniczne lub organizacyjne, inne niż wskazane w załącznikach do Kodeksu o nr 5, 6 lub 7, jeżeli są one adekwatne do ryzyka

naruszenia praw i wolności osób fizycznych oraz zapewniają analogiczny poziom ochrony danych osobowych.

5.5. Powierzenie przetwarzania danych

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

5.5.2. 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.

5.5.3. 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. 5.3. PWDL i dokumentuje proces tej oceny.

5.5.4. Przyjmuje się, że Podmiot przetwarzający będący Podmiotem przestrzegającym Kodeksu spełnia wymogi określone w pkt. 5.3.

5.5.5. 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[29], pod warunkiem spełnienia wymogów wskazanych w pkt. 5.5.2. Powyższe nie ogranicza wyboru, przez Administratora, konkretnych (preferowanych) rozwiązań technicznych i organizacyjnych wykorzystywanych przez Podmiot przetwarzający[30].

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

5.5.6.1. 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;

5.5.6.2. każdy Podmiot przetwarzający świadczący usługi innemu Podmiotowi przetwarzającemu zapewnia przetwarzanie zgodne z wymogami RODO, w tym

[29] Np. hosting, chmura obliczeniowa (prywatna, hybrydowa, publiczna).

[30] W sprawach nieuregulowanych w Kodeksie dotyczących zasad przetwarzania dokumentacji medycznej w formie elektronicznej zaleca się wykorzystanie dobrych praktyk wypracowanych przez Centrum E-Zdrowia (dawne CSIOZ).

wdrożenie odpowiednich środków technicznych i organizacyjnych zgodnie z pkt. 5.5.2.

5.5.7. 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.

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

5.5.9. W przypadkach uzasadnionych zasadami ochrony danych osobowych przyjętych przez Podmiot przetwarzający i Administratora, prawo wskazane w pkt. 5.5.7. 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.

5.6. Szkolenia jako element zapewnienia bezpieczeństwa danych osobowych

5.6.1. 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.

5.6.2. 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.

5.6.3. 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).

5.6.4. Wskazane w poprzednich punktach działania muszą mieć charakter cykliczny i być udokumentowane przez PWDL lub Podmiot przetwarzający. 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 pkt. 6.2.

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 1 miesiąc, jeżeli zakres danych przetwarzanych przez PWDL bądź inne okoliczności związane z przetwarzaniem nie ulegały zmianie od czasu złożenia poprzedniego żądania (ustawiczny charakter żądania);

6.1.6.2. żądania o informacje dzielone sztucznie na kilka, kilkanaście lub więcej żądań[31];

6.1.6.3. żądanie szczególnego, niestandardowego formatu odpowiedzi, w szczególności formatu nienależącego do powszechnie używanych formatów plików[32];

6.1.6.4. żądania udzielenia odpowiedzi w języku innym niż polski;

6.1.7. Za ewidentnie nieuzasadnione lub nadmierne żądania Pacjenta, które uzasadniają odmowę ich zrealizowania, uznaje się również: żądanie informacji, których przekazanie spowodowałyby nieuprawnione ujawnienie tajemnicy przedsiębiorstwa, tajemnicy zawodowej personelu medycznego lub danych osobowych innego Pacjenta lub innej tajemnicy prawnie chronionej;

6.1.8. PWDL jest zobowiązany 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[33];

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:

[31] Np. odrębne żądania udostępnienia co drugiego zdania na stronach parzystych i nieparzystych, żądania udostępnienia co drugiej strony dokumentacji, żądania udostępnienia danych zebranych w dni nieparzyste itp., kilkanaście żądań dotyczących jednej hospitalizacji.
[32] Np. .txt, .pdf, .odt, .sxw, .doc, .rtf, .jpeg, .xml, .xls.
[33] Np. osoba nieprzytomna lub wymagająca pilnej interwencji lekarskiej.

6.2.3.1. dacie dokonania weryfikacji tożsamości; oraz

6.2.3.2. rodzaju dokumentu, na podstawie którego została ona dokonana,

6.2.3.3. w przypadku, gdy w PWDL jest więcej osób o tym samym imieniu i nazwisku - numerze PESEL osoby okazującej dowód tożsamości, jeżeli został nadany, a w przypadku osób, które nie mają nadanego numeru PESEL - rodzaju i numerze dokumentu potwierdzającego tożsamość.

6.2.3.4. Co do zasady PWDL nie jest uprawniony do dokonywania i utrwalania kopii dokumentu potwierdzającego tożsamość.

6.2.4. W sytuacji, w której w imieniu Pacjenta, w okolicznościach wskazanych w pkt. 6.2.1., występuje Przedstawiciel ustawowy, tożsamość Pacjenta może być potwierdzona również przez Przedstawiciela ustawowego w drodze oświadczenia i okazania dowodu tożsamości Przedstawiciela ustawowego zgodnie z pkt. 6.2.3. PWDL może utrwalić informację o dacie dokonania weryfikacji oraz o rodzaju dokumentu Przedstawiciela ustawowego, na podstawie którego została ona dokonana.

6.2.5. W sytuacji, w której Pacjentowi towarzyszy Opiekun faktyczny, który wyraża zgodę na badanie, 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. 6.2.3. PWDL może utrwalić informację o dacie dokonania weryfikacji oraz rodzaju dokumentu Opiekuna faktycznego, na podstawie którego została ona dokonana.

6.2.6. 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, elektronicznego dowodu osobistego, 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. 6.2.3. Takie okazanie może być dokonane np. w trakcie wideotransmisji. Nie należy utrwalać ani przechowywać obrazu zawierającego kopię okazanego dowodu tożsamości, w przypadku stosowania rozwiązań przewidujących

czasowe utrwalenie obrazu, powinien być on niezwłocznie usunięty, nie później niż w pierwszym dniu roboczym po dniu okazania dokumentu tożsamości.

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. 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, przy czym, dane inne niż imię i nazwisko utrwala się w przypadku wielości osób o tych samych danych osobowych.

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[34].

6.3.2. Obowiązek informacyjny może być zrealizowany poprzez:

6.3.2.1. umieszczenie klauzul informacyjnych w dokumentach przekazywanych Pacjentowi w trakcie rozpoczęcia udzielania Świadczeń zdrowotnych (umowa o świadczenie usług medycznych, deklaracja POZ, zgoda na udzielenie świadczenia zdrowotnego), zawierających co najmniej szczegółowe informacje na temat celów przetwarzania, tożsamości Administratora i opisu praw osoby, której dane dotyczą oraz odesłanie do miejsca, w którym można uzyskać pełną informację o przetwarzaniu danych (warstwowe podejście do realizacji obowiązku informacyjnego) oraz

6.3.2.2. podjęcie wskazanych poniżej działań przez PWDL:

6.3.2.2.1. 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

[34] Dobrą praktyką jest angażowanie się przez PWDL w akcje i inicjatywy, skierowane do Pacjentów, których celem jest podniesienie świadomości dotyczącej zasad przetwarzania danych osobowych. Autorzy Kodeksu rekomendują zaangażowanie się Podmiotów przestrzegających Kodeksu w kampanię „RODO dla Pacjenta" www.rododlapacjenta.pl

e-mail lub sms, oraz umieszczenie informacji na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez Pacjentów (w szczególności ciągi komunikacyjne lub izba przyjęć lub rejestracja lub poczekalnia); lub

6.3.2.2.2. 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. lub jeżeli wizyta w miejscu wezwania została zamówiona za pomocą systemów teleinformatycznych lub systemów łączności, wystarczające jest umieszczenie klauzul informacyjnych zgodnie z pkt. 6.3.2.2.1 w tych systemach.

6.3.4. W odniesieniu do Pacjentów, dla których świadczenie odbywa się za pomocą systemów teleinformatycznych lub systemów łączności, do spełnienia obowiązku informacyjnego wskazanego w art. 13 RODO, wystarczające jest umieszczenie klauzul informacyjnych w tych systemach zgodnie z pkt. 6.3.2.2.1.

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[35].

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.

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

[35] Wskazanie, że jest to wersja z dnia „X" itp.

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) RODO.

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

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 wskazanej ustawy[36].

6.5.2. Pacjent ma prawo swobodnego wyboru podstawy oraz zakresu żądania związanego z dostępem do informacji na jego temat przetwarzanych przez PWDL. Pierwsze udostępnienie pacjentowi Dokumentacji medycznej, niezależnie od podstawy prawnej udostępnienia, stanowi udostępnienie pierwszej kopii danych osobowych podlegających przetwarzaniu w zakresie danych w niej zawartych w rozumieniu art. 15 ust. 3 RODO.

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. 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,

[36] 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.

6.5.5.2. 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 pkt. 6.1.;

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 RODO nie jest równoznaczne z obowiązkiem udostępniania danych w formacie i strukturze właściwej dla Dokumentacji medycznej.

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 pkt. 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 RODO 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)[37].

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.

[37] 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.

6.5.12. Kopię danych, w tym kopię Dokumentacji medycznej, zgodnie z art. 15 ust. 3 RODO 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.

6.5.13. PWDL dowolnie zabezpiecza transmisję danych w postaci elektronicznej zgodnie z przeprowadzoną analizą ryzyka. Poziom bezpieczeństwa 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. uprzedniego poinformowania Pacjenta o zagrożeniach, dotyczących ochrony danych osobowych, związanych z proponowanym kanałem komunikacji;

6.5.14.2. utworzenia plików zawierających zaszyfrowane informacje za pomocą bezpiecznych programów do szyfrowania;

6.5.14.3. wprowadzenia hasła zabezpieczającego plik w chwili tworzenia tego pliku;

6.5.15. 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. 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[38].

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;

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;

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 – prawo do „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.

[38] 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.

6.7.2. 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.

6.7.5. W odniesieniu do osób wskazanych w pkt. 6.4. pkt. 6.7.1.-6.7.4. stosuje się odpowiednio.

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

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.

6.8.2. Ograniczenie przetwarzania ma na celu zabezpieczenie danych przed dalszą możliwością ich przetwarzania, z 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 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. udostępnianie danych na potrzeby przeprowadzania kontroli przez uprawnione z mocy prawa organy lub podmioty;

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

6.8.4. W odniesieniu do osób wskazanych w pkt. 6.4. 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.

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 przetwarzanie prowadzone jest 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, np. .txt, .pdf, .odt, .sxw, .doc, .rtf, .xml, .xls.

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 pkt. 6.2.

6.9.9. Prawo do przenoszenia danych nie może negatywnie wpływać na prawa i wolności innych osób. 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).

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 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:

6.11.1.1. profilowanie, które nie skutkuje podejmowaniem decyzji opierających się wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych i wywołujących wobec Pacjenta 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 Pacjenta 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. pkt 6.10.1. dot. sprzeciwu wobec przetwarzania danych osobowych).

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;

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[39];

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)[40];

[39] Np. Skala CHA2DS2–VASc.
[40] Np. na potrzeby wykonywania badań diagnostycznych.

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;

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 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. Podmioty wskazane w pkt. 1.6. oraz inne zrzeszenia i inne podmioty reprezentujące PWDL oraz Podmioty przetwarzające 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.;

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 UODO 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 UODO 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. 7.4.15.

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.;

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;

7.1.2.9. w odniesieniu do Organów lub podmiotów publicznych:

a) podejmowanie decyzji o pozbawieniu statusu Podmiotu przestrzegającego Kodeksu na podstawie wniosku przedstawionego przez Jednostkę audytującą, a także rozstrzyganie odwołań od tych decyzji. Wniosek o pozbawienie statusu Podmiotu przestrzegającego Kodeksu składa się do Komitetu sterującego wraz z raportem z audytu monitoringowego, potwierdzającym stwierdzenie naruszenia Kodeksu,

b) rozpatrywanie wniosków i skarg na sposób wdrożenia lub wdrażania Kodeksu lub naruszenie Kodeksu przez PWDL lub Podmiot przetwarzający – o ile Jednostka audytująca nie będzie mogła zapewnić rozpatrzenia takich wniosków i skarg,

c) wydawanie rekomendacji i wytycznych w zakresie monitorowania stosowania Kodeksu, w tym wzorów procedur i innych dokumentów, w tym list kontrolnych audytów monitoringowych,

d) okresowo, nie rzadziej niż co 12 miesięcy, udzielanie UODO zbiorczych informacji o działaniach wymienionych w punktach wskazanych wyżej i powodach ich podjęcia oraz informacji dotyczących stosowania Kodeksu, opracowanych na podstawie danych przekazanych przez Jednostki audytujące.

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 głosowania 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 dotyczyć 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 wybranemu członkowi 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 akredytację Prezesa UODO, 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. Do podstawowych zadań i obowiązków Podmiotu monitorującego należy:

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

7.2.3.2. monitorowanie przestrzegania przepisów Kodeksu;

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

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

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

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

7.2.3.7. informowanie UODO o działaniach wymienionych w punktach wskazanych wyżej i powodach ich podjęcia;

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

7.2.4. Szczegółowy zakres zadań i obowiązków Podmiotu monitorującego zawarte są w innych punktach Kodeksu, umowach wskazanych w pkt. 7.4.8. oraz w procedurach wskazanych w art. 41 ust. 2 pkt. b) i c) RODO.

7.2.5. 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 wniosku składanego co najmniej w formie elektronicznej, skierowanego do Podmiotu monitorującego, zgodnie z którym PWDL lub Podmiot przetwarzający oświadczają, że spełniają wymogi wnikające z Kodeksu.

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

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

7.3.2.2. 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;

7.3.2.3. wskazanie sposobu dalszego monitorowania przestrzegania przepisów Kodeksu.

7.3.3. Wzór wniosku 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. 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.

7.3.6. Metodyka przeprowadzania audytu wstępnego określona zostanie przez Podmiot monitorujący, przy czym powinna ona uwzględniać co najmniej ocenę spełnienia poszczególnych obowiązków wynikających z Kodeksu, który zakres wskazany został w kwestionariuszu, o którym mowa w pkt. 7.4.2.1. i 7.4.3.

7.3.7. 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.

7.3.8. Audyt wstępny realizowany jest na podstawie umowy zawartej między Podmiotem monitorującym a:

7.3.8.1. samorządami zawodowymi – w odniesieniu do PWDL w formie praktyk zawodowych prowadzonych przez zrzeszone w ramach tych samorządów osoby (chyba, że samorządy zawodowe występować będą jako Podmiot monitorujący w stosunku do PWDL w formie praktyk zawodowych);

7.3.8.2. członkami Komitetu sterującego – w odniesieniu do PWDL lub Podmiotów przetwarzających będących jego członkami;

7.3.8.3. bezpośrednio PWDL lub Podmiotami przetwarzającymi, ubiegającymi się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu.

7.3.9. Audyt wstępny przeprowadzany jest niezwłocznie, nie później niż 12 miesięcy od dnia złożenia wniosku przez PWDL nieprowadzący szpitala lub Podmiot przetwarzający oraz nie później niż 24 miesiące od dnia złożenia wniosku przez PWDL prowadzący szpital.

7.3.10. 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. Podmiot monitorujący niezwłocznie informuje PWDL lub Podmiot przetwarzający, a także Komitet sterujący o wynikach ponownego audytu wstępnego.

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

7.3.11.1. informację o uzyskaniu statusu Podmiotu przestrzegającego Kodeksu oraz treść zaświadczenia wskazanego w pkt 7.3.10.;

7.3.11.2. informację o możliwości złożenia i zasadach rozpatrywania wniosku lub skargi na naruszenie Kodeksu przez Podmiot przestrzegający Kodeksu;

7.3.11.3. informację o utracie statusu Podmiotu przestrzegającego Kodeksu.

7.3.12. Podmiot przestrzegający Kodeksu informuje Komitet sterujący, Jednostkę audytującą oraz Podmiot monitorujący, bez zwłoki, nie później niż w terminie 7 dni, o wszelkich decyzjach Prezesa UODO 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 7.3.1, jak również o istotnych dla ochrony danych osobowych zmianach stanu faktycznego opisanych w załącznikach do wniosku.

7.3.13. W odniesieniu do Organów lub podmiotów publicznych, które uzyskały status Podmiotu przestrzegającego Kodeksu, dalsze monitorowanie jest prowadzone przez Jednostkę audytującą w ramach mechanizmów monitorowania i oceny kontroli zarządczej - w szczególności poprzez audyt wewnętrzny albo w ramach nadzoru sprawowanego przez podmiot tworzący lub organ rejestrowy - w szczególności poprzez kontrolę i ocenę działalności podmiotu.

7.3.13.1. Jednostka audytująca będąca audytorem wewnętrznym lub usługodawcą prowadzącym audyt wewnętrzny, realizuje dalsze monitorowanie w formie zadań zapewniających, na podstawie przepisów art. 272-296 ustawy o finansach publicznych oraz przepisów wykonawczych, w szczególności rozporządzenia Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (t.j. Dz.U. z 2018 r. poz. 506) („rozporządzenie w sprawie audytu wewnętrznego") i Standardów audytu wewnętrznego dla jednostek sektora finansów publicznych (Dz. Urz. MRiF z 2016 r. poz. 28) („standardy audytu wewnętrznego");

7.3.13.2. Dalsze monitorowanie uwzględniane jest w planie audytu, na zasadach określonych w rozdziale 2 rozporządzenia w sprawie audytu wewnętrznego;

7.3.13.3. Planowanie i realizacja dalszego monitorowania oraz informowanie o jego wynikach odbywa się zgodnie z zasadami określonymi w rozdziale 3 rozporządzenia w sprawie audytu wewnętrznego. Z realizacji zadań w zakresie dalszego monitorowania, jednostka audytująca będąca audytorem wewnętrznym lub usługodawcą prowadzącym audyt wewnętrzny sporządza sprawozdanie z zadania zapewniającego.

7.3.13.4. Jednostka audytująca będąca podmiotem tworzącym Podmiot przestrzegający Kodeksu realizuje dalsze monitorowanie w formie kontroli i oceny działalności tego podmiotu, na podstawie przepisów art. 121 i 122 ustawy o działalności leczniczej. Dalsze monitorowanie odbywa się w formie kontroli w trybie zwykłym, o której mowa w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (t. j. Dz. U. z 2020 r. poz. 224) („ustawa o kontroli w administracji rządowej").

7.3.13.5. Dalsze monitorowanie uwzględniane jest w okresowym planie kontroli, na zasadach określonych w art. 12 ustawy o kontroli w administracji rządowej.

7.3.13.6. Planowanie i realizacja dalszego monitorowania oraz informowani o jego wynikach odbywa się zgodnie z zasadami określonymi w rozdziale 2 ustawy o kontroli w administracji rządowej. Z realizacji zadań w zakresie dalszego monitorowania jednostka audytująca będąca pomiotem tworzącym sporządza wystąpienie pokontrolne.

7.3.14. Jednostka audytująca określa terminy i sposoby dalszego monitorowania przestrzegania przepisów Kodeksu w corocznych planach audytu lub okresowych planach kontroli.

7.3.15. Zalecane jest uwzględnienie celu zapewnienia zgodności z postanowieniami Kodeksu w planie działalności Podmiotu przestrzegającego Kodeksu, sporządzanym na podstawie przepisów art. 70 ustawy o finansach publicznych.

7.3.16. Jednostka audytująca jest zobowiązana zapewnić niezależność i obiektywizm w realizacji dalszego monitorowania, wiedzę fachową w dziedzinie będącej przedmiotem kodeksu oraz procedury gwarantujące unikanie konfliktu interesów.

7.3.17. W przypadku powzięcia przez Komitet sterujący informacji o braku zgodności Jednostki audytującej z wymaganiami określonymi w poprzednim punkcie, Komitet sterujący przekazuje Jednostce audytującej (a do wiadomości 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 udzielonej przez Jednostkę audytującą oraz podjętych działań zaradczych Komitet sterujący może podjąć dalsze kroki, w tym zawiesić lub pozbawić posiadania statusu Podmiotu przestrzegającego Kodeksu.

7.3.18. Jednostka audytująca jest zobowiązana do przyjęcia procedury określającej szczegółowe zasady prowadzenia monitorowania przestrzegania przepisów Kodeksu, obejmujące co najmniej następujące postanowienia:

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

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

7.3.18.3. 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.

7.3.19. Dalsze monitorowanie może mieć formę ankiety monitoringowej, wywiadów telefonicznych lub wizyty na miejscu.

7.3.20. Wybór zakresu i formy audytu monitoringowego powinien uwzględniać wyniki audytów monitoringowych z lat poprzednich, skalę przetwarzania szczególnych danych osobowych, czynniki ryzyka zidentyfikowane na etapie audytu wstępnego i liczbę lokalizacji jednostek organizacyjnych zakładów leczniczych.

7.3.21. Monitorowanie w formie ankiety monitoringowej przeprowadza się nie rzadziej niż raz do roku. Ankieta obejmuje w szczególności zagadnienia dotyczące zmian, jakie zaszły w ostatnim okresie w systemie ochrony danych osobowych Członka Kodeksu, w tym wykonanych przeglądów i aktualizacji polityk i procedur, zmian w strukturze organizacyjnej podmiotu, istotnych modyfikacji systemów IT, w których przetwarzane są dane osobowe, zidentyfikowanych naruszeń ochrony danych, sposobu wdrożenia zmian przepisów prawa oraz bieżących wytycznych lub rekomendacji Europejskiej

Rady Ochrony Danych oraz Prezesa Urzędu Ochrony Danych. Monitorowanie w formie wywiadów telefonicznych lub wizyty na miejscu przeprowadza się nie rzadziej niż raz na 5 lat. Badaniem tym objęty jest pełny zakres wymogów nałożonych przez Kodeks na PWDL oraz Podmioty przetwarzające, określony w kwestionariuszu stanowiącym załącznik nr 10 do Kodeksu.

7.3.22. W ramach monitorowania przestrzegania przepisów Kodeksu oraz okresowego przeglądu funkcjonowania Kodeksu, Jednostka audytująca 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 Jednostka audytująca, przy czym procedura ta powinna uwzględniać funkcjonujące w PWDL zasady przyjmowania skarg oraz:

7.3.22.1. musi być prosta i przejrzysta;

7.3.22.2. 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 Jednostka audytująca informuje osobę składającą skargę lub wniosek, z podaniem przyczyny opóźnienia;

7.3.22.3. powinna zawierać możliwość składania skarg i wniosków w formie elektronicznej, telefonicznej, na piśmie i ustnie w siedzibie Jednostki audytującej bez konieczności dopełnienia szczególnej formy. Jednostka audytująca określi zasady identyfikacji osoby składającej skargę. Jednostka audytująca określi zasady postępowania ze skargami składanymi anonimowo;

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

7.3.22.5. zawiera informację o możliwości złożenia skargi do Prezesa UODO oraz Komitetu sterującego na działania bądź zaniechania Jednostki audytującej.

7.3.23. Jednostka audytująca podaje do publicznej wiadomości wzór skargi na naruszenie Kodeksu oraz na sposób wdrożenia lub wdrażania Kodeksu przez Podmiot przestrzegający Kodeksu. Stosowanie wzoru skargi przez podmioty skarżące ma charakter fakultatywny – złożenie skargi w sposób inny niż przy wykorzystaniu wzoru nie może być powodem jej nierozpatrzenia.

7.3.24. Komitet sterujący wyda wzory procedur, o których mowa w pkt 7.3.15 i 7.3.21 oraz szczegółowe rekomendacje i wytyczne w zakresie monitorowania stosowania Kodeksu, w tym wzór skargi, o którym mowa w pkt 7.3.22 oraz wzory list kontrolnych audytów monitoringowych.

7.3.25. W przypadku ustalenia wysokiego prawdopodobieństwa naruszenia przepisów Kodeksu bądź stwierdzenia naruszania przepisów Kodeksu przez Podmiot przestrzegający Kodeksu, Jednostka audytująca 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 udzielonej przez Podmiot przestrzegający Kodeksu oraz podjętych działań zaradczych może:

7.3.25.1. wystąpić do Komitetu sterującego z wnioskiem o zawieszenie posiadania 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;

7.3.25.2. wystąpić do Komitetu sterującego z wnioskiem o pozbawienie PWDL lub Podmiotu przetwarzającego 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 7.3.24.1.

7.3.26. Informacja o działaniach podjętych zgodnie z pkt 7.3.24. przekazywana jest Komitetowi sterującemu oraz Podmiotowi monitorującemu bez zbędnej zwłoki.

7.3.27. Informacja o zawieszeniu wskazana w pkt 7.3.24.1. jest podawana do wiadomości publicznej. Zawieszenie posiadania statusu Podmiotu przestrzegającego Kodeksu jest równoznaczne z tymczasową utratą statusu Podmiotu przestrzegającego Kodeksu. Po usunięciu naruszeń, o których mowa w punkcie 7.3.24 oraz uzyskaniu potwierdzenia usunięcia naruszeń od Jednostki audytującej, zawieszony podmiot odzyskuje od dnia potwierdzenia usunięcia naruszeń status Podmiotu przestrzegającego Kodeksu.

7.3.28. Podmiot monitorujący, Komitet sterujący, PWDL odraz Podmiot przetwarzający niezwłocznie po otrzymaniu informacji o pozbawieniu statusu Podmiotu przestrzegającego Kodeks, dokonują stosownej zmiany informacji wskazanych w pkt 7.3.11.

7.3.29. Jednostka audytująca corocznie, w terminach określonych przez Komitet sterujący, przekazuje Komitetowi sterującemu:

7.3.29.1. Wyniki czynności sprawdzających przeprowadzonych planowo w danym roku;

7.3.29.2. Wyniki czynności sprawdzających przeprowadzonych w związku z uzyskaniem informacji o naruszeniu zasad przestrzegania Kodeksu przez Podmiot przestrzegający Kodeksu;

7.3.29.3. Zbiorczą informację o złożonych wnioskach oraz skargach na naruszenie Kodeksu lub na sposób wdrożenia lub wdrażania Kodeksu przez Podmiot przestrzegający Kodeksu wraz z informacją o wynikach rozpatrzenia wniosków i skarg.

7.4. Podjęcie się stosowania Kodeksu przez PWDL oraz Podmioty przetwarzające inne, niż Organy lub 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. 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 zostanie przez Podmiot monitorujący, 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. i 7.4.3.

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 (chyba, że samorządy zawodowe występować będą jako Podmiot monitorujący w stosunku do PWDL w formie praktyk zawodowych);

7.4.8.2. członkami Komitetu sterującego – w odniesieniu do PWDL lub Podmiotów przetwarzających będących jego 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, nie później niż 12 miesięcy od dnia złożenia wniosku przez PWDL nieprowadzący szpitala lub Podmiot przetwarzający oraz nie później niż 24 miesiące od dnia złożenia wniosku przez PWDL prowadzący szpital.

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. Podmiot monitorujący niezwłocznie informuje PWDL lub Podmiot przetwarzający, a także Komitet sterujący o wynikach ponownego audytu wstępnego.

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

7.4.11.1. informację o uzyskaniu statusu Podmiotu przestrzegającego Kodeksu oraz treść zaświadczenia wskazanego w pkt. 7.4.10.;

7.4.11.2. 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.;

7.4.11.3. 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 wszelkich decyzjach Prezesa UODO 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, w tym związane z nimi opłaty, jeżeli będą pobierane, określa Podmiot monitorujący, 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, 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. Podmiot monitorujący określi zasady identyfikacji osoby składającej skargę. Podmiot monitorujący określi zasady postępowania ze skargami składanymi anonimowo;

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 UODO oraz Komitetu sterującego na działania bądź zaniechania Podmiotu monitorującego.

7.4.16. Podmiot monitorujący opracowuje wzór skargi na naruszenie Kodeksu oraz na sposób wdrożenia lub wdrażania Kodeksu przez Podmiot przestrzegający Kodeksu oraz podaje go do publicznej wiadomości. Stosowanie wzoru skargi przez podmioty

skarżące ma charakter fakultatywny – złożenie skargi w sposób inny niż przy wykorzystaniu wzoru nie może być powodem jej nierozpatrzenia.

7.4.17. 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:

7.4.17.1. 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;

7.4.17.2. 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. 7.4.17.1.;

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

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

7.4.20. Informacja o zawieszeniu wskazana w pkt. 7.4.17.1. jest podawana do wiadomości publicznej. Zawieszenie posiadanie statusu Podmiotu przestrzegającego Kodeksu jest równoznaczne z tymczasową utratą statusu Podmiotu przestrzegającego Kodeksu. Po usunięciu naruszeń, o których mowa w punkcie 7.4.17. oraz uzyskania potwierdzenia usunięcia naruszeń od Podmiotu monitorującego, zawieszony podmiot odzyskuje od dnia potwierdzenia usunięcia naruszeń status Podmiotu przestrzegającego Kodeksu.

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

7.5. Dodatkowe zasady podjęcia się stosowania Kodeksu

7.5.1. Komitet sterujący może przyjąć dodatkowe zasady dotyczące podjęcia się stosowania Kodeksu przez PWDL lub Podmioty przetwarzające, dotyczące w szczególności:

7.5.1.1. wzoru i trybu zawarcia umów wskazanych w pkt. 7.3.8. i 7.4.8.;

7.5.1.2. ustalenia oznaczenia słownego lub graficznego statusu Podmiotu przestrzegającego Kodeksu oraz wzoru zaświadczenia, o którym mowa w pkt. 7.3.10 i 7.4.10.;

7.5.1.3. 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. 7.3.10. i 7.4.10. oraz innych informacji w szczególności przy wykorzystaniu dedykowanego systemu teleinformatycznego;

7.5.1.4. pokrywania kosztów administracyjnych funkcjonowania Komitetu sterującego, przy czym nie mogą być one wyższe w skali roku niż ogłaszana przez GUS wartość przeciętnego miesięcznego wynagrodzenia w sektorze przedsiębiorstw bez wypłat nagród z zysku za ostatni kwartał roku po którym ustalana jest opłata, dodatkowo koszty powinny być uzależnione od rodzaju i wielkości PWDL lub Podmiotu przetwarzającego. Koszty muszą być przy tym znane PWDL lub Podmiotowi przetwarzającemu ubiegającemu się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu jeszcze przed uzyskaniem statusu Podmiotu przestrzegającego Kodeksu. W przypadku wzrostu kosztów administracyjnych funkcjonowania Komitetu sterującego lub zmiany rodzaju i wielkości PWDL lub Podmiotu przetwarzającego, koszty mogą ulec zmianie na zasadach określonych przez Komitet sterujący i przekazanych PWDL lub Podmiotowi przetwarzającemu ubiegającemu się o uzyskanie statusu Podmiotu przestrzegającego Kodeksu jeszcze przed uzyskaniem statusu Podmiotu przestrzegającego Kodeksu.

7.6. Współpraca na rzecz okresowego przeglądu stosowania Kodeksu

7.6.1. Okresowy przegląd stosowania Kodeksu dokonywany jest przez Komitet sterujący samodzielnie lub we współpracy z Podmiotami monitorującymi. Przegląd stosowania Kodeksu następuje nie rzadziej niż raz na 6 miesięcy, w tym w szczególności w przypadku zmian prawnych istotnie wpływających na zasady ochrony danych osobowych lub funkcjonowanie PWDL.

7.6.2. 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.

7.6.3. W ramach okresowego przeglądu stosowania Kodeksu:

7.6.3.1. Podmioty monitorujące przekazują Komitetowi sterującemu oraz Prezesowi UODO informacje dotyczące stosowania Kodeksu:

7.6.3.1.1. nie rzadziej niż co 12 miesięcy oraz;

7.6.3.1.2. na każde żądanie Komitetu sterującego lub Prezesa UODO.

7.6.3.2. Jednostki audytujące przekazują Komitetowi sterującemu informacje dotyczące stosowania Kodeksu:

7.6.3.2.1. nie rzadziej niż co 12 miesięcy oraz

7.6.3.2.2. na każde żądanie Komitetu sterującego.

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

7.6.4.1. PWDL oraz Podmiotów przetwarzających;

7.6.4.2. Jednostek audytujących;

7.6.4.3. podmiotów wskazanych w pkt. 1.7.;

7.6.4.4. Pacjentów i organizacji zrzeszających Pacjentów;

7.6.4.5. podmiotów z sektora administracji publicznej;

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

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

7.6.5.2. organizowanie wydarzeń poświęconych stosowaniu Kodeksu.

7.6.6. Komitet sterujący nie rzadziej niż raz na 6 miesięcy dokonuje oceny zasadności złożenia do Prezesa UODO wniosku o zmianę lub rozszerzenie Kodeksu.

7.6.7. 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.

7.7. Zapobieganie konfliktom interesów

7.7.1. Podmiot monitorujący oraz Jednostka audytująca są zobowiązane zapewnić zachowanie niezależności i bezstronności w realizacji zadań i obowiązków.

7.7.2. Do osoby wykonującej zadania i obowiązki w imieniu lub z upoważnienia Podmiotu monitorującego stosuje się odpowiednio przepisy Kodeksu postępowania administracyjnego dotyczące wyłączenia pracownika. Do osoby wykonującej zadania i obowiązki w imieniu lub z upoważnienia Jednostki audytującej stosuje się odpowiednio postanowienia standardu 1100 standardów audytu wewnętrznego lub przepisy art. 19 ustawy o kontroli w administracji rządowej.

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

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

7.7.4.1. nie wydaje Podmiotowi monitorującemu wiążących poleceń;

7.7.4.2. opinia udzielona przez Komitet sterujący, o której mowa w pkt. 7.1.2.3. i 7.1.2.4. może być oparta wyłącznie na merytorycznych przesłankach.

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 zapewniają 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 PWDL w których przetwarzanie danych nie jest uznane za przetwarzanie na dużą skalę.
8. **Załącznik nr 8**: Wzór wniosku o uzyskanie statusu Podmiotu przestrzegającego Kodeksu przez Organy i podmioty publiczne.
9. **Załącznik nr 9:** Wzór wniosku o uzyskanie statusu Podmiotu przestrzegającego Kodeksu przez PWDL oraz Podmioty przetwarzające inne niż Organy i podmioty publiczne.
10. **Załącznik nr 10:** Wzór kwestionariusza, który dołącza się do wniosku, o którym mowa w załączniku nr 8 lub załączniku nr 9.

Załącznik nr 1

Wzór zgody na przetwarzanie danych osobowych

Oznaczenie osoby wyrażającej zgodę: [____][41],

Wyrażam zgodę na przetwarzanie moich danych osobowych [____][42] w celu [____][43] przez Administratora, tj. [____][44]. Przyjmuję do wiadomości, iż mam prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

_____

Podpis i data[45]

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

Oznaczenie osoby wyrażającej zgodę: [____][46],

Wyrażam zgodę na przetwarzanie moich danych osobowych w celach:

- ☐ [*cel nr 1*], zakres danych [____][47]
- ☐ [*cel nr 2*], zakres danych [____][48]

[41] Zakres danych potrzebnych do zidentyfikowania osoby składającej oświadczenie powinien być adekwatny do celu przetwarzania danych. Oznaczeniem takim może być w szczególności, jeśli w związku z celem przetwarzania nie jest wystarczające, np. wskazanie jedynie adresu e-mail lub numeru telefonu, imię i nazwisko osoby udzielającej zgody, a także fakultatywnie dodatkowe informacje (rekomendujemy datę urodzenia albo PESEL, albo adres miejsca zamieszkania- przy wykorzystaniu jednej z tych kategorii informacji), pozwalające na jednoznaczne ustalenie tożsamości osoby. Niepodanie fakultatywnych dodatkowych informacji nie ma wpływu na ważność zgody. PWDL nie może podać w formularzu zgody wskazanych pól jako obligatoryjnych, wskazując, że stanowią one warunek skuteczności udzielonej zgody. Pola fakultatywne powinny być oznaczone odpowiednią informacją (np.*) i przypisem dolnym, wskazującym na fakultatywny/nieobowiązkowy charakter. Określając zakres danych, należy pamiętać o zasadach adekwatności, stosowności i minimalizacji danych zgodnie z art. 5 ust. 1 lit. c) RODO.

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

[43] 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).

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

[45] Podpis osoby udzielającej zgody. W przypadku zgody wyrażanej w postaci elektronicznej, podpis może zostać zastąpiony zaznaczeniem wyraźnie oznakowanego pola wyboru, jeżeli Administrator będzie w stanie wykazać fakt i datę jego zaznaczenia.

[46] Por. przypis nr 40.

[47] 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".

[48] Jak we wcześniejszym przypisie.

przez Administratora, tj. [____][49].Przyjmuję do wiadomości, iż mam prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

_____

Podpis i data[50]

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.

[49] W tym miejscu należy podać nazwę Administratora danych osobowych oraz jego adres.
[50] Podpis osoby udzielającej zgody.

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.

1. **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 Przedstawiciela ustawowego (opcjonalne, ale zalecane): PESEL, seria i numer dowodu tożsamości.

2. **Przykładowy zakres danych identyfikujących osobę upoważnioną, co do której przyjmuje się, że jednoznacznie identyfikują wskazaną osobę.**

Zgodnie z przepisami wykonawczymi wydanymi na podstawie art. 30 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, niezbędnymi danymi osoby upoważnionej, które muszą zostać podane, jeśli jest to osoba fizyczna, jest imię i nazwisko.

Dodatkowo w przypadku, gdy w PWDL znajduje się więcej niż jeden Pacjent lub osoba upoważniona o tym samym imieniu i nazwisku, PWDL może poprosić o dodatkowe informacje dotyczące osoby upoważnionej i je utrwalić (o ile Pacjent posiada takowe informacje), które pozwolą na jej jednoznaczną identyfikację. 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) data i miejsce urodzenia;
2) numer dokumentu tożsamości (dowodu osobistego, paszportu, prawa jazdy legitymacji szkolnej).

3. Przykładowa treść oświadczeń zgodna z przepisami prawa

JEŻELI UPOWAŻNIA PACJENT	*Imię osoby upoważnionej*:* *Nazwisko osoby upoważnionej*:* *Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne)* *Działając na podstawie art. 26 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta w związku z przepisami wykonawczymi wydawanymi na podstawie art. 30 ust. 1 wskazanej ustawy:* □ *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 PWDL. *Imię Pacjenta:* *Nazwisko:* *PESEL lub data i miejsce urodzenia:* *Data złożenia oświadczenia:……..* _____
JEŻELI UPOWAŻNIA PRZEDSTAWICIEL USTAWOWY	*Imię osoby upoważnionej*:* *Nazwisko osoby upoważnionej*:* *Dodatkowe informacje pozwalające na ustalenie tożsamości osoby upoważnionej (opcjonalne):* *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 lub data i miejsce urodzenia:* W pełnym zakresie/ w zakresie ograniczonym 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): PESEL, seria i numer dowodu tożsamości Przedstawiciela ustawowego.* *Data złożenia oświadczenia:…….*

Załącznik nr 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?	Należy dążyć 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, 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 taśmy w jaskrawych barwach w celu wyznaczenia obszaru przed stanowiskiem rejestracji, w którym przebywa tylko osoba obsługiwana 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 może dochodzić 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 takich środków jak np.: 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 PWDL 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 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?	Należy dążyć 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 osobie udzielającej Świadczenia zdrowotnego 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. W sytuacji, w której 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 lub innych Osób wykonujących zawód medyczny przyjmujących Pacjentów?	Tak. Zamieszczenie imion i nazwisk oraz specjalizacji lekarza lub innej Osoby wykonującej zawód medyczny na drzwiach gabinetów nie narusza RODO. Informacje o imieniu i nazwisku Osoby wykonującej zawód medyczny oraz jej specjalizacji są zwykłymi danymi osobowymi. Zgodnie z art. 6 ust. 1 lit. c RODO podstawą przetwarzania 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 pozostające 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 Osoby wykonującej zawód medyczny, w tym w szczególności imię nazwisko, informacja o posiadanej specjalizacji, czy też umiejętności z zakresu węższych dziedzin medycyny lub udzielania określonych świadczeń zdrowotnych zawarte są w rejestrach prowadzonych odpowiednio przez właściwe samorządy zawodowe.
Czy lekarz lub inna osoba wykonująca zawód medyczny może na sali chorych rozmawiać z Pacjentem o jego chorobie, gdy nie ma gwarancji, że 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 nieprzeprowadzenie rozmowy w trybie natychmiastowym mogłoby narazić Pacjenta na uszczerbek, możliwe jest przeprowadzenie rozmowy w każdym miejscu. Jeżeli sytuacja wskazana w pytaniu nie dotyczy bieżących czynności medycznych lub obchodu, rozmowa taka powinna być przeprowadzona w miejscu, w którym nie przebywają inne osoby nieuprawnione np. inni Pacjenci (dotyczy to zarówno sali chorych jak i korytarza szpitalnego). W myśl ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz ustawy z o zawodach lekarza i lekarza dentysty, lekarz 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 wskazanego wymogu, 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 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	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

rozmów prowadzonych z Pacjentem zarówno przez personel medyczny, jak i administrację 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 oraz pozostały personel medyczny nie powinni 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 nie można 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 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). Zasadą powinna być identyfikacja Pacjenta na podstawie ww. znaku np. wskazanego na opasce. Informacje na ww. znaku mają być zapisane w taki sposób, aby 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 przepisach wykonawczych wydanych 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 pomyłki, 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. Ponadto jest to standard wynikający również *z* wymogów akredytacyjnych. W zakresie, w jakim oznaczanie produktów leczniczych, wyrobów medycznych i innych środków podawanych Pacjentowi nie wynika z obowiązujących regulacji prawnych, standardów lub wytycznych podmiotów publicznych, w tym w szczególności standardów akredytacji, powinno być poprzedzone analizą ryzyka i niezbędności takiego działania. PWDL może wdrożyć wewnętrzne zasady oznaczania produktów leczniczych, wyrobów medycznych i innych środków podawanych Pacjentowi.
Czy podmiot leczniczy może uzależnić wgląd do Dokumentacji medycznej osoby trzeciej od posiadania upoważnienia udzielonego przez Pacjenta, którego dotyczy dokumentacja, opatrzonego	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 upoważnienia. W związku z powyższym, w przypadku, gdy Pacjent upoważnienia udziela bezpośrednio w obecności personelu, dopuszczalna powinna być każda forma takiego oświadczenia.

własnoręcznym podpisem albo złożonym w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym?	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 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 o działalności leczniczej. W przypadku, gdy stosowanie kart jest niezbędne, w szczególności na oddziałach ratunkowych, konieczne jest ich zabezpieczenie poprzez: a) zastosowanie ramek chroniących dane osobowe zamieszczanych na kartach przyłóżkowych; b) konstrukcja ramki powinna uniemożliwiać odczytanie danych; c) zastosowanie nakładki zabezpieczającej dane Pacjenta na karcie przyłóżkowej; d) odwrócenie kart przyłóżkowych.
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. pytanie 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 prawnie zdolna do wyrażenia zgody. W sytuacjach kryzysowych często nie ma też potrzeby udzielania szczegółowych informacji o stanie zdrowia.

Załącznik nr 4

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

1. Ocena ryzyka naruszenia praw i wolności osób fizycznych

Przeprowadzenie oceny ryzyka ma na celu:

a) zapewnienie zdolności do ciągłego zapewnienia poufności, integralności, dostępności oraz odporności systemów i usług przetwarzania danych osobowych;

b) definiowanie i wdrażanie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku;

c) ocenę czy stopień bezpieczeństwa jest odpowiedni, przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego 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. Ocena ta ma na celu utrzymanie ryzyka na akceptowalnym poziomie.

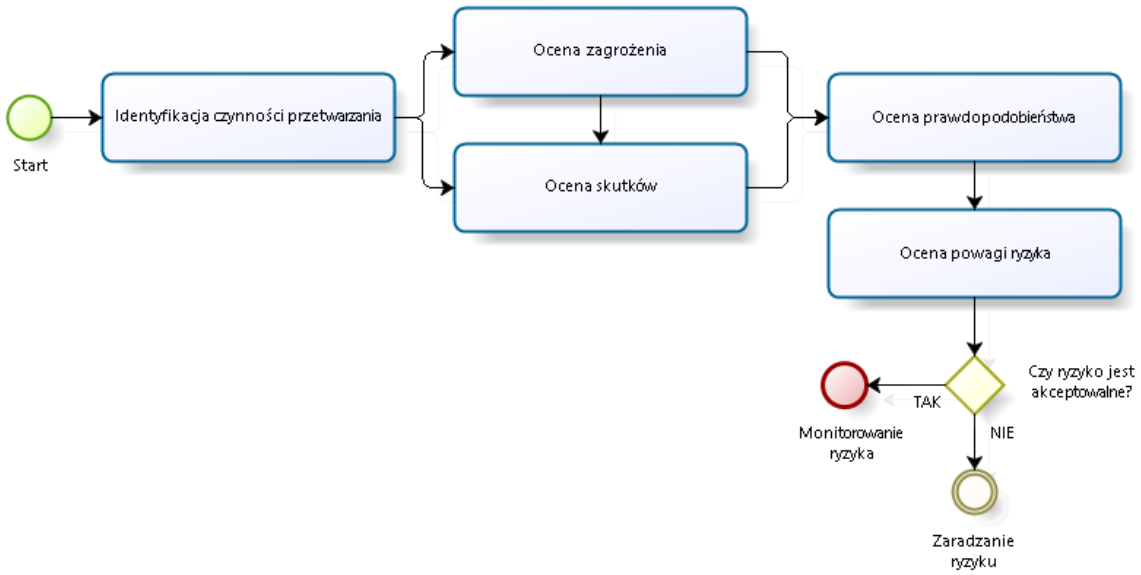
Powinno się badać oddzielnie ryzyko związane z prywatnością z punktu widzenia osoby, której dane dotyczą oraz ryzyko związane z prywatnością z punktu widzenia organizacji.

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, z tego względu, że 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.



2. 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 PWDL[51]:

- 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;
  f) zapewnienia zabezpieczenia społecznego oraz zarządzania systemami i usługami zabezpieczenia społecznego;

[51] 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.

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 zapewnienia 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[52].

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 są użytkowane obecnie;
- 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);

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

- jakie rodzaje sieci komputerowych użytkowane są w podmiocie (kable, Wi-Fi, światłowody itp.);
- jakie rodzaje nośników informacji w postaci papierowej są stosowane (wydruki, ksero itp.);
- jakie istnieją w podmiocie kanały przesytu 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 do Kodeksu.

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.

3. 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 realizowana 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.

4. 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.

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 Centrum E-Zdrowia (dawne CSIOZ)[53] oraz w normie PN-EN ISO/IEC 27799:2016.

5. 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.

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

[53]Dostęp:https://csioz.gov.pl/fileadmin/user_upload/rekomendacje_csioz_bezpieczenstwo_wrzesien2017_59cd1e951e9ba.pdf

Lp.	Katalog skutków naruszenia praw lub wolności osób fizycznych, podlegający ocenie
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, długotrwałe 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 prawdopodobne	Zagrożenie raczej nie wystąpi lub możliwość jego 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:

$$\boldsymbol{R = S * P}$$

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 skutków		Ocena prawdopodobieństwa				
		1	**2**	**3**	**4**	**5**
	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.

6. 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 zobowiązany jest dokonać tzw. uprzednich konsultacji z Prezesem UODO co do dalszego postępowania, określonych w art. 36 RODO.

7. Zabezpieczenia

Wynikiem procesu szacowania ryzyka jest wskazanie procesów, które będą wymagały wdrożenia 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 mapujące zabezpieczenia na zagrożenia i podatności występujące przy przetwarzaniu danych osobowych. Tabela ta została zawarta w załączniku nr 5 do Kodeksu.

Załącznik nr 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 systemów	Procedury logowania	Rejestrowanie zdarzeń	Polityka korzystania z zabezpieczeń kryptograficznych	Polityka bezpieczeństwa informacji w relacjach z dostawcami	Bezpieczeństwo w umowach z dostawcami	Zarządzanie uprzywilejowanymi prawami dostępu	Odebranie lub dostosowanie praw dostępu	Ochrona informacji zawartych w dziennikach	Zabezpieczanie aplikacji usługowych w sieciach publicznych	Ochrona transakcji usług aplikacyjnych i	Rozdzielanie środowisk rozwojowych, testowych i eksploatacyjnych	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	Fizyczna granica obszaru bezpiecznego	Zabezpieczenia wejścia fizycznego	Zabezpieczanie biur, pomieszczeń i urządzeń	Postępowanie ze sprzętem pozostającym bez nadzoru użytkownika	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																		x
Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat zdrowia pacjentów	x	x	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										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
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	x
Przekierowanie połączenia	x	x	x												x		x			x	x	x	x		x																				x	x
Awaria techniczna systemu lub	x	x															x			x				x	x	x														x	x					x

infrastruktury sieciowej																																															
Awaria środowiska wsparcia	x	x																		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									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	x						x	x
Błąd użytkownika	x	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	x
Samowolne uszkodzenia przez użytkowników	x	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

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.PN-ISO/IEC 29101:2017-07 Techniki bezpieczeństwa – Ramy architektury i prywatności.
10. PN-ISO/IEC 29134:2017- Techniki bezpieczeństwa – Wytyczne dotyczące oceny wpływu na prywatność.
11. 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

Rekomendacje w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania danych w PWDL, 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 PWDL, 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.

PWDL, w którym 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 PWDL jest odpowiedzialny za wszystkie działania opisane w poniższych punktach niniejszego załącznika.

2. Organizacja bezpieczeństwa informacji

2.1. Polityka Bezpieczeństwa Danych.

W PWDL 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		

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.**
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 załącznikami do Kodeksu bądź przy wykorzystaniu równoważnej metodyki bądź zgodnie z pkt. 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 powinny być przechowywane w zamkniętej szafie, spełniającej wymagania wskazane w pkt. 2, zlokalizowanej w innym miejscu niż obszar przetwarzania, spełniający wymagania wskazane w pkt. 1. W przypadku danych w formie elektronicznej wymóg ten jest spełniony 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, powinno być zabezpieczone przed skutkami pożaru co najmniej za pomocą wolnostojącej gaśnicy, której miejsce przechowywania jest odpowiednio oznaczone.

e) jeśli pomieszczenie, w którym przechowywana jest na stałe[54] Dokumentacja medyczna, wyposażone jest w okna, 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 nich[55].

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

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

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

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

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.

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) wprowadzić odpowiednie zabezpieczenia 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 przekazaniem do serwisu urządzeń należy wymontować nośniki informacji (dyski twarde);

g) 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 sprawdzić, czy sprzęt jest kompletny, nieuszkodzony, czy nie znajdują się na nim ślady zewnętrznej ingerencji;

i) nie pozostawiać sprzętu 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 fakt, że 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.

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

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

3.17. 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.

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

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

3.20. 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.

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

3.22. 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.

3.23. 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.

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

3.25. 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.

3.26. 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.

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

3.28. 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.

3.29. 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.

3.30. 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 poprzez posiadanie 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

Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu przez Organy i podmioty publiczne

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:

Adres strony internetowej:

Data złożenia oświadczenia:

Działając na podstawie pkt. 7.3.1. Kodeksu postępowania dla sektora ochrony zdrowia wydanego zgodnie z art. 40 RODO dotyczącego PWDL 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. Działalność prowadzona jest w ramach następujących zakładów leczniczych i jednostek organizacyjnych zakładów leczniczych:

Nazwa zakładu leczniczego	**Nazwa jednostki organizacyjnej zakładu leczniczego**	**Adres**	**Osoba kontaktowa**	**Adres e-mail**	**Nr telefonu**	**Liczba osób wykonujących zawody medyczne w jednostce organizacyjnej**

Wskazanie sposobu dalszego monitorowania przestrzegania przepisów Kodeksu:

☐ monitorowanie prowadzone w ramach mechanizmów monitorowania i oceny kontroli zarządczej, w szczególności poprzez audyt wewnętrzny (w ramach własnej, wydzielonej struktury lub zlecony firmie zewnętrznej);

☐ monitorowanie prowadzone w ramach nadzoru sprawowanego przez podmiot tworzący lub organ rejestrowy.

Dane kontaktowe Jednostki audytującej:

Imię i nazwisko osoby kontaktowej:

Stanowisko służbowe:

Numer telefonu:

Adres e-mail:

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.

Załącznik nr 9

Wzór wniosku o uzyskanie statusu podmiotu przestrzegającego Kodeksu przez PWDL oraz Podmioty przetwarzające inne niż Organy i podmioty publiczne

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:

Adres strony internetowej:

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 PWDL 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. Działalność prowadzona jest w ramach następujących zakładów leczniczych i jednostek organizacyjnych zakładów leczniczych:

Nazwa zakładu leczniczego	**Nazwa jednostki organizacyjnej zakładu leczniczego**	**Adres**	**Osoba kontaktowa**	**Adres e-mail**	**Nr telefonu**	**Liczba osób wykonujących zawody medyczne w jednostce organizacyjnej**

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

Załącznik nr 10

Wzór kwestionariusza, który dołącza się do wniosku, o którym mowa w załączniku nr 8 lub 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)[56]**
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 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	
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 obowiązki związane z przetwarzaniem danych, w tym czy zawiera umowy powierzenia przetwarzania danych z właściwymi podmiotami.	

[56] 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.

		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[57].	
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 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).	PWDL	Należy w szczególności zweryfikować, 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	PWDL	Należy zweryfikować, czy podmiot wdrożył zalecenia wskazane w załączniku nr 3 do Kodeksu.	

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

Pacjentów w związku z przetwarzaniem danych osobowych.			
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[58]), należy również ocenić relacje tego podmiotu z podprocesorami). Należy w szczególności ocenić spełnienie pkt. 5.4.6. i 5.4.8. 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 dane osobowe, należy również zweryfikować czy PWDL lub Podmiot przetwarzający prowadzą udokumentowane i cykliczne działania w obszarze zwiększenia wiedzy w zakresie bezpieczeństwa danych osobowych.	

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

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, 22 RODO)	
Zgodność z prawem procesów wykorzystujących profilowanie lub inne zautomatyzowane przetwarzanie danych	PWDL	Należy w szczególności ocenić, czy PWDL podejmuje decyzje opierające się wyłącznie na zautomatyzowanym przetwarzaniu danych, które to decyzje istotnie wpływają na Pacjentów lub osoby trzecie i zweryfikować zgodność z prawem takiego przetwarzania.	