Instrukcja Ochrony Danych Osobowych
w podmiocie wykonującym działalność leczniczą – PWDL
praktyce zawodowej lekarskiej:
Praktyka Lekarska Barbara Szynol-Woźniak
wydana w dniu 2018.05.16

Niniejsza „Instrukcja Ochrony Danych Osobowych" w PWDL: Indywidualna Specjalistyczna Praktyka Lekarska Barbara Szynol-Woźniak ma na celu opisanie zasad i procedur stosowanych przez Administratora w celu spełnienia wymagań Rozporządzenia PE i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych zwanego w dalszej części polityki RODO.

Administrator deklaruje, że proces przetwarzania danych osobowych uwzględnia zasady, o których mowa w Motywie 39 RODO oraz artykule 5 ust. 1 ppkt a) – e) RODO.

Administrator zaznacza, że niniejsza polityka to jeden ze środków o charakterze organizacyjnym, za pomocą którego wykazuje się zgodność przetwarzania danych osobowych z RODO.

Administrator deklaruje pełną świadomość charakteru, rodzaju i kontekstu przetwarzanych danych osobowych w PWDL, w tym ich sensytywności

Podstawy prawne:

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
2. Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U. t.j. Dz. U. z 2016 r. poz. 1638, 1948, 2260, z 2017 r. poz. 2110, 2217.
3. Ustawa z dnia 06 kwietnia 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2017 r. poz. 1318, 1524),
4. Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach zdrowotnych finansowanych ze świadczeń publicznych (t.j. Dz. U. z 2017 r. poz. 1938, 2110, 2217, 2361, 2434),
5. Ustawa z dnia 21 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2017 tj. poz.1845),
6. *Ustawa o Ochronie Danych Osobowych z dnia 10 maja 2018*
7. Niniejsza Polityka Ochrony Danych Osobowych
8. Pozostałe przepisy regulujące system ochrony danych osobowych, w tym przepisy wydane na podstawie art. 40 RODO.

Spis treści:

1. *Inwentaryzacja danych,*
2. *Zgodność z prawem procesu przetwarzania danych,*
3. *Upoważnienia do przetwarzania danych osobowych,*
4. *Poufność procesu przetwarzania danych,*
5. *Współpraca z podmiotami zewnętrznymi.*
6. *Udostępnianie danych osobowych.*
7. *Uprawnienia osób, których dane osobowe są przetwarzane w PWDL.*

II Ryzyko w PWDL:

1. *Analiza ryzyka,*
2. *Zarządzanie ryzykiem.*

III Rejestr czynności przetwarzania.
IV Instrukcja postępowania w przypadku naruszenia systemu ochrony danych osobowych
V Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego – plan ciągłości działania
VI Postępowanie dyscyplinarne
VII Szkolenia personelu
VIII Wykaz zabezpieczeń
IX Instrukcja zarządzania systemem informatycznym

I. Weryfikacja posiadanych danych osobowych i zasady ich przetwarzania

1. Inwentaryzacja danych

1.1 Poprzez dane osobowe w PWDL, zgodnie z art. 4 pkt 1) RODO należy rozumieć wszystkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, którą można w sposób pośredni lub bezpośredni zidentyfikować, z uwzględnieniem identyfikatorów. Dane te mogą dotyczyć pracowników PWDL, jego pacjentów lub osoby współpracujące z PWDL.

1.2 Dane osobowe w PWDL są zorganizowane w struktury za pomocą których Administrator może ocenić ryzyko ich przetwarzania.

1.3 Dane osobowe opisane są z uwzględnieniem, co najmniej poniższych informacji:

a) Nazwa przetwarzanych danych osobowych,
b) Cele przetwarzania,
c) Zakres przetwarzania,
d) Odbiorcy danych,
e) Zakres czynności przetwarzania,
f) Zasoby służące do przetwarzania danych osobowych,
g) Informacja o konieczności wpisu do rejestru czynności przetwarzania,
h) Informacja o konieczności przeprowadzenie oceny skutków dla ochrony danych na zbiorze,

i) Okres przechowywania.

1.4 Szczegółowo opis danych osobowych został przedstawiony w **załączniku nr 1**.

2.Legalność procesu przetwarzania danych osobowych

2.1 Administrator swoimi działania i organizacją PWDL zapewnia, że:

a) dane osobowe w PWDL przetwarzane są w sposób legalny, na podstawie art. 6 ust. 1 ppkt a) i c) oraz art. 9 ust. 2 ppkt h) w związku z art. 3 ust. 1 i 2 ustawy o działalności leczniczej oraz art. 24 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a także 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.

b) zakres pozyskiwanych danych wynika z przepisów prawa, o których mowa w punkcie 2.1 a) niniejszego dokumentu i jest adekwatny do zdefiniowanych celów przetwarzania,

c) określono konkretny czas przez jaki dane są przetwarzane (załącznik nr 1),

d) wobec osób, których dane są przetwarzane wykonano obowiązek informacyjny, zgodnie z art. 12-14 RODO, a wzór klauzuli informacyjnej znajduje się w **załączniku 1 b**,

e) obowiązek informacyjny wobec pacjentów PWDL jest wykonywany poprzez umieszczenie na tablicy informacyjnej przy okienku rejestracyjnym, w poczekalni oraz na stronie internetowej stosownych informacji.

f) z wszystkimi współpracującymi podmiotami gospodarczymi podpisano, na mocy art. 28 RODO, umowy powierzenia przetwarzania danych osobowych lub w umowach podstawowych wprowadzono uregulowania odnoszące się do obowiązków zapewnienia przestrzegania przepisów RODO przez te podmioty,

2.2 Dane osobowe w PWDL są pozyskiwane bezpośrednio od pacjentów lub od innych podmiotów uczestniczących w udzielaniu tym pacjentom świadczeń zdrowotnych.

3. Upoważnienia do przetwarzania danych osobowych:

3.1 Administrator do przetwarzania danych osobowych w PWDL dopuszcza jedynie osoby posiadające stosowane upoważnienia. Wzór stosownych upoważnień stanowi **załącznik nr 1 c**.

3.2 Administrator jest odpowiedzialny za proces nadawania i wycofywania upoważnień do przetwarzania danych osobowych w PWDL.

3.3 Zmiana uprawnień w zakresie przetwarzania danych osobowych odbywa się na wniosek bezpośredniego przełożonego zgodnie z załącznikiem nr 1 c 1.

3.4 W PWDL prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych, w sposób umożliwiający prawidłową identyfikację historii i prawidłowości procesu przetwarzania danych osobowych. Rejestr jest prowadzony na druku zgodnym z **załącznikiem nr 1 d**.

4. Poufność procesu przetwarzania danych osobowych.

4.1 Każda z osób dopuszczona do przetwarzania danych osobowych lub współpracująca z PWDL jest zobowiązana do:

a) przetwarzania danych osobowych jedynie w zakresie i jedynie w celu w jakim zostało im wydane upoważnienie lub podpisano umowę powierzenia przetwarzania danych osobowych,

b) zachowania w tajemnicy informacji i danych osobowych, do których posiada dostęp,

c) niewykorzystywania dostępnych danych osobowych do celów sprzecznych z zakresem upoważnienia lub umowy powierzenia przetwarzania danych osobowych.

d) zachowania poufności procesów i metod zabezpieczeń danych osobowych w PWDL.

e) ochrony informacji i danych osobowych przed przypadkowym, niepożądanym ujawnieniem, modyfikacjom, utratą, zniszczeniem danych osobowych czy też nieuprawnionym dostępem osób niepożądanych,

4.2 Osobami, które są dopuszczone do przetwarzania danych osobowych w PWDL (poza kryterium zatrudnienia lub współpracy z PWDL:

4.2.1 przedstawiciele zawodów medycznych, z zastrzeżeniem art. 24 ust. 2 pkt 2 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta

4.2.2 personel pomocniczy przy udzielaniu świadczeń zdrowotnych, a także osoby odpowiedzialne za czynności związane z prawidłowym funkcjonowaniem systemów teleinformatycznych, w których przetwarzana jest dokumentacja medyczna,

4.3 Osoby dopuszczone do przetwarzania danych osobowych w PWDL, przed przystąpieniem do pracy, odbyły szkolenie z zasad ochrony danych osobowych w PWDL.

4.4 Osoby, które zostają dopuszczone do przetwarzania danych osobowych, a które zapoznały się treścią niniejszej Instrukcji zobowiązane zostały do

podpisania tzw. oświadczenia o poufności, którego wzór stanowi **załącznik nr 1 e**.

4.5 W PWDL zabronione jest udzielanie wszelkich informacji zawierających dane osobowe osobom, których tożsamości nie można zweryfikować. Weryfikacja tożsamości może odbywać się poprzez żądanie okazania dokumentu tożsamości lub innego dokumentu zawierającego zdjęcie wnioskodawcy lub poprzez wykorzystanie informacji zawartej w dokumentacji medycznej, która jest znana jedynie wnioskodawcy. Do tego celu należy wykorzystać metodę pytań bezpośrednich, w których wnioskodawca udzieli poprawnych informacji w co najmniej dwóch zapytaniach.

4.6 W PWDL niedopuszczalne jest przekazywania wszelkich informacji zawierających dane osobowe podmiotom, instytucjom czy też organom, które nie mogą się wykazać prawidłową podstawą prawną dostępu do danych osobowych.

4.7 W przypadku konieczności wydania dokumentów zawierających dane osobowe (np. wynik badań, recepty itp.) należy każdorazowo weryfikować tożsamość odbierającego za pomocą mechanizmu, o którym mowa w punkcie 4.5, a w przypadku, kiedy odbierającym nie jest adresat dokumentu należy zażądać upoważnienia.

4.8 W PWDL zakazuje się wywoływania pacjentów z użyciem ich imion i nazwisk i wprowadza się system ich anonimizacji.

4.9 Organizacja rejestracji i poczekalni PWDL umożliwia zachowanie poufności osobom przebywającym bezpośrednio przy rejestracji.

4.10 Udzielanie świadczeń zdrowotnych w PWDL odbywa się w miejscach specjalnie do tego wyznaczonych. Zabrania się udzielania informacji dotyczących pacjentów na korytarzach, w poczekalni lub innych nieprzystosowanych do tego miejscach w PWDL.

4.11 Zabrania się eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp.

4.12 Wydruki i inne dokumenty zawierające dane osobowe są przechowywane w pomieszczeniach do tego wyznaczonych. Na stanowiskach pracy mogą być dostępne jedynie dokumenty dotyczące danego pacjenta. Stosowana jest zasada tzw. czystego biurka.

4.13 Po zakończeniu pracy wszelka dokumentacja zawierająca dane osobowe jest przechowywana w szafach zamykanych na klucz lub w pomieszczeniach o ograniczonym dostępie osób postronnych, do których dostęp jest utrudniony poprzez zastosowanie zabezpieczeń fizycznych takich jak: zamki w drzwiach, kraty w oknach, systemy kontroli dostępu itp.

4.14 Wszelkie dokumenty zawierające dane osobowe niszczone są z użyciem niszczarek.

4.15 Zaleca się zwrócenie szczególnej uwagi pracownikom PWDL na sytuację przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, przy kopiarkach, przy drukarkach itp.

4.16 Administrator jest zobowiązany do corocznej weryfikacji posiadanych zbiorów danych osobowych, które mają na celu wyeliminowanie danych, do których ustały podstawy przetwarzania.

5. Współpraca z podmiotami zewnętrznymi

5.1 W działalności PWDL jest dopuszczalna współpraca z podmiotami zewnętrznymi, którym udostępnia się dane osobowe, których Administratorem jest PWDL- Praktyka Lekarska Barbara Szynol-Woźniak

5.2 Powierzenie przetwarzania danych osobowych może odbywać się jedynie na podstawie umowy lub innego instrumentu prawnego, zgodnie z zasadami określonymi w art. 28 RODO.

5.3 W PWDL prowadzona jest ewidencja podmiotów, z którymi podpisano umowy powierzenia, którego wzór stanowi **załącznik nr 1 f**.

5.4 Ewidencja ta zawiera, co najmniej:

a) nazwę, adres siedziby i dane kontaktowe podmiotu,

b) datę podpisania umowy,

c) przedmiot umowy,

d) informacja o rodzajach zbiorów, które obejmuje umowa przetwarzania.

6. Udostępnianie danych

6.1 PWDL udostępnia dane osobowe jedynie na podstawie obowiązujących przepisów prawa i w granicach prawa.

6.2 Dane osobowe pacjentów, które znajdują się w dokumentacji medycznej są udostępniane na zasadach, w trybie i na sposób określony w przepisach art. 26 i 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

6.3 Ewidencja udostępnionej dokumentacji medycznej prowadzona jest na podstawie art. 27 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta i zawiera, co najmniej: imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna, sposób udostępnienia dokumentacji medycznej;, zakres udostępnionej dokumentacji medycznej, imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w przypadkach, o których mowa w art. 26 ust. 3 i 4, także nazwę uprawnionego organu lub podmiotu, imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną, datę udostępnienia dokumentacji medycznej.

6.4 Wzór ewidencji, o której mowa w punkcie 6.3 stanowi **załącznik nr 1g**.

6.5 PWDL udostępnia również dane, na podstawie innych przepisów niż te, o których mowa w punkcie 6.2 jedynie na pisemny wniosek i za potwierdzeniem.

6.6 Wzór ewidencji udostępnionych danych w trybie, o którym mowa w punkcie 6.5 stanowi **załącznik nr 1 h**.

6.7 PWDL przekazując dane drogą pocztową przekazuje je listem poleconym za potwierdzeniem odbioru, w dwóch niezależnie zamkniętych kopertach.

6.8 W przypadku udostępniania dokumentów za pomocą korespondencji mailowej PWDL ma obowiązek szyfrować przekazywane pliku, zgodnie z **załącznikiem nr 9**. Instrukcja szyfrowania plików znajduje się w rejestracji PWDL.

7 Uprawnienia osób, których dane osobowe są przetwarzane w PWDL.

7.1 PWDL zapewnia osobom, których dane osobowe przetwarza do realizacji wszystkich przysługujących im praw na mocy art. 15 i 16 RODO.

7.2 PWDL wprowadza na podstawie art. 9 ust. 1 pkt h) RODO ograniczenia w realizacji praw osób, których dane przetwarza, a wynikających z art. 17, 18, 20 i 21 RODO, szczególnie powołując się na zapisy art. 29 ustawy z dnia 06 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta

7.3 W przypadku zastosowania trybu, o którym mowa w punkcie 7.2 należy taką sytuację pisemnie wyjaśnić osobie, która wniosła sprawę w zakresie realizacji jej praw.

II. Ryzyko w PWDL

1. Analiza ryzyka

1.1.W PWDL przeprowadzana jest analiza ryzyka. Analiza ryzyka może odbywać się dla wszystkich wyodrębnionych zbiorów danych osobowych lub dla procesów przetwarzania.

1.2 Analiza ryzyka przeprowadzana jest w celu określenia, oceny i minimalizacji zagrożeń, których efektem ma być wdrożenie optymalnych i adekwatnych zabezpieczeń.

1.3 Analiza ryzyka przeprowadzona jest corocznie, nie później niż do dnia 31 marca lub w przypadku wprowadzenia nowych procedur lub rozwiązań organizacyjnych w PWDL, zgodnie z procedurą analizy ryzyka opisaną w opisaną w Załączniku nr 2

2. Polityka zarządzania ryzykiem

2.1 Czynności, o których mowa w punkcie II stanowią politykę zarządzania ryzykiem w PWDL.

2.2 Za nadzór nad realizacją polityki zarządzania ryzykiem odpowiada Administrator.

2.3. Polityką zarządzania ryzykiem administruje wyznaczony pracownik.

2.4 Wyznaczony pracownik ma obowiązek sporządzenia corocznego raportu związanego z ryzykiem w PWDL nie później niż do 30 kwietnia.

III. Rejestr czynności przetwarzania

1. Dla zbiorów, w których przetwarzane są dane, o których mowa w art. 9 ust. 1 RODO prowadzony jest rejestr czynności przetwarzania.
2. Rejestr, o którym mowa w punkcie 1 niniejszego rozdziału może być również prowadzony dla innych zbiorów. Szczegółowa informacja o zbiorach, dla których prowadzony jest rejestr czynności przetwarzania zawarta jest w Załączniku nr 1.
3. Rejestr czynności przetwarzania winien zawierać co najmniej informacje, o których mowa w art. 30 RODO tj.:
   3.1 Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
   3.2 cele przetwarzania;
   3.3 opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   3.4 kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione,
   3.5 jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
   3.6 jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.
4. Rejestr czynności przetwarzania jest prowadzony w oparciu o **załącznik nr 4**.

IV. Zasady postępowania w przypadku naruszenia systemu ochrony danych

1. Każda osoba, której Administrator wydał upoważnienie do przetwarzania danych osobowych, ma obowiązek natychmiastowego powiadamiania o występującym zagrożeniu lub wystąpieniu incydentu związanego z systemem ochrony danych osobowych w PWDL.
2. Powiadomienie to może mieć charakter ustny lub pisemny.
3. Adresatem takiego powiadomienia jest Administrator.

4. Po otrzymaniu takiego powiadomienia Administrator podejmuje niezwłocznie czynności w celu ustalenia stanu faktycznego.
5. Po dokonaniu czynności zabezpieczających, Administrator, ma za zadanie przeprowadzić postępowanie wyjaśniające, które:
   5.1 ustali ostateczny zakres, przyczyny wystąpienia oraz skutki, zarówno dla PWDL, jak i osób, których dane dotyczyły,
   5.2 podejmuje niezbędne czynności mające na celu przywrócenie prawidłowości działania systemu ochrony danych osobowych w PWDL,
   5.3 opracowuje działania naprawcze i zapobiegawcze, których zadaniem jest wyeliminowanie niepożądanych zdarzeń w przyszłości,
   5.4 wskazuje osoby odpowiedzialne za wystąpienie sytuacji.
6. Powyższe czynności są dokumentowane przez Administratora za pomocą formularza, którego wzór stanowi **załącznik nr 5**.
7. Rejestr formularzy, o których mowa w punkcie 6 niniejszego rozdziału prowadzi administrator.

V. Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu technicznego lub fizycznego

1. Administrator wyznaczył następujące obszary krytyczne dla organizacji systemu ochrony danych osobowych:
   1.1 brak zasilania w PWDL,
   1.2 awaria systemu informatycznego,
   1.3 awaria sprzętu do przetwarzania danych osobowych,
   1.4 brak dostępu do sieci internetowej,
   1.5 brak dostępu do pomieszczeń, w których przetwarzane są dane osobowe.

2. Wobec zdefiniowanych obszarów krytycznych opracowano Plan ciągłości działania stanowiący **załącznik nr 6**.

VI Postępowanie dyscyplinarne

1. Pracownicy PWDL i podmioty współpracujące mają bezwzględny obowiązek stosowania przepisów prawa i przepisów wewnętrznych obowiązujących w PWDL w zakresie ochrony danych osobowych.
2. W przypadku wystąpienia incydentu, naruszenia procedur czy też zaniechania czynności wynikających z obowiązków w zakresie ochrony danych

osobowych, wszystkie takie czynności będą traktowane jako ciężkie naruszenie zasad i stosunków formalnych panujących w PWDL.

3. Administrator, jako Pracodawca, ma prawo do potraktowania działań, o których mowa w punkcie 2 powyżej jako działań podlegającej sankcjom karnym wynikającym z RODO lub innych przepisów krajowych w zakresie organizacji procesu ochrony danych osobowych i jest uprawniony do złożenia stosownych doniesień do organów nadzorczych.

VII Szkolenia personelu

1. Każdy pracownik/współpracownik PWDL, przed przystąpieniem do pracy na zbiorach danych osobowych PWDL musi zostać przeszkolony w zakresie przepisów związanych z ochroną danych osobowych.
2. Za przeprowadzenie szkoleń odpowiada Administrator.
3. Każde szkolenie musi być udokumentowane listą obecności, na której poza imionami i nazwiskami jego uczestników z ich podpisami musi być opisany zakres szkolenia.
4. Administrator przeprowadza szkolenia w miarę potrzeb, po każdej zmianie przepisów mających znaczenie dla procesów ochrony danych osobowych w PWDL oraz nie rzadziej niż raz na 12 miesięcy.

VIII Wykaz zabezpieczeń

1. W PWDL prowadzony jest wykaz zabezpieczeń organizacyjnych, technicznych, fizycznych i personalnych, w którym w sposób usystematyzowany opisano procedury zabezpieczeń.
2. Wykaz, o którym mowa w punkcie powyżej prowadzi Administrator PWDL.
3. Wykaz prowadzony jest w formie papierowej i elektronicznej, zgodnie z **załącznikiem nr 8**.
4. Wykaz winien być aktualizowany każdorazowo po wprowadzeniu nowych rozwiązań w PWDL oraz po analizie ryzyka w PWDL, o ile jej wynik tego wymaga.

IX Instrukcja zarządzania systemem informatycznym

1. Instrukcja stanowi zestaw procedur opisujących zasady zabezpieczania danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.
2. Za nadzór nad jej przestrzeganiem odpowiada Administrator i Informatyk.
3. Szczegółowo opis procedur zawarty jest w **załączniku nr 9** do niniejszego dokumentu.