Dokumentacja w zakresie ochrony danych osobowych zgodnie z Rozporządzeniem UE - RODO

Podstawa prawna

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
(Dz. U. UE 2016 poz. L119)

RODO - Rozporządzenie o Ochronie Danych Osobowych

GDPR - General Data Protection Regulation

Jest stosowane od 25 maja 2018r.

Dotyczy przetwarzania i prawa do ochrony danych osobowych
osób przebywających na terytorium Unii Europejskiej

Bezpośrednia stosowalność przepisów RODO, bez konieczności dodatkowej implementacji do polskiego porządku prawnego. Częściowa swoboda doprecyzowania/ograniczenia RODO przez prawo krajowe.

Dane osobowe -przykłady

- imię, nazwisko
- adres e-mail
- numer PESEL
- ID komputera
- numer telefonu
- wizerunek nagrany przez kamerę monitoringu
- głos nagrany w trakcie rozmowy z konsultantem
- odcisk palca
- dane z dowodu tożsamości
- dane o geolokalizacji
- czynniki szczególne określające tożsamość np.: genetyczną lub kulturową

Rozporządzenie RODO a przepisy krajowe

Ustawa z 10 05.2018 o ochronie danych osobowych poz. 1000 (UODO)

Obowiązuje od 25 maja 2018r.

Uchyla ustawę z dnia 29 sierpnia 1997 r.

o ochronie danych osobowych.

Ustawa określa:

– zadania Administratora
– wyznaczanie inspektora ochrony danych
– warunki i tryb udzielania akredytacji podmiotowi certyfikującemu
– opracowywanie i zatwierdzanie kodeksu postępowania
– sposób powołania Prezesa Urzędu Ochrony Danych
– postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych
– kontrola przestrzegania przepisów o ochronie danych osobowych
– odpowiedzialność cywilna

KODEKS

Regulacje wewnętrzne

Polityka Ochrony Danych Osobowych

1. Wstęp
2. Definicje i skróty
3. Cel ,podstawa prawna, zakres polityki
4. Podstawowe zasady przetwarzania danych osobowych przez Zakład
   Przetwarzanie danych osobowych
   Przetwarzanie szczególnych kategorii danych osobowych
   Zasady przetwarzania danych
   Obowiązki wobec osób których dane osobowe są przetwarzane
   Podstawy przetwarzania danych
   Przetwarzanie danych w celach zdrowotnych
   Przetwarzanie danych w celach innych niż zdrowotne
   Administrator

Regulacje wewnętrzne

Polityka Ochrony Danych Osobowych

5. Bezpieczeństwo
   Bezpieczeństwo przetwarzania danych osobowych
   Sposób przepływu danych pomiędzy poszczególnymi systemami informatycznymi
   Postępowanie w przypadkach stwierdzenia naruszenia ochrony danych osobowych
   Podstawowe środki techniczne i organizacyjne stosowane w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych
   Podmioty przetwarzające
   Szkolenia jako element zapewnienia bezpieczeństwa danych osobowych
   Sprawy organizacyjne
   Rejestr czynności przetwarzania
6. Znajomość Polityki
7. Załączniki
8. Dokumenty powiązane

Załączniki

Zał. Nr 1 – Zgoda na przetwarzanie danych osobowych; /mar. kl. nau./
Zał. Nr 2 – Zgoda na przetwarzanie danych osobowych;
Zał. Nr 3 – Klauzula informacyjna;
Zał. Nr 4 – **Upoważnienie do przetwarzania danych osobowych(3 egz.);**
Zał. Nr 4a – Upoważnienie do przetwarzania danych osobowych dla pracowników;
Zał. Nr 5 – Rejestr osób upoważnionych;
Zał. Nr 6 – Zobowiązanie do zachowania poufności danych osobowych;
Zał. Nr 7 – **Umowa powierzenia danych osobowych;**
Zał. Nr 8 – Rejestr naruszenia danych osobowych;
Zał. Nr 9 – Wzór zgłoszenia naruszenia ochrony danych osobowych;
Zał. Nr 10 – Wzór wniosku przełożonego o nadanie uprawnień dla użytkownika w systemie informatycznym;
Zał. Nr 11 – Oświadczenie o poufności;
Zał. Nr 12 – **Rejestr czynności przetwarzania**;
Zał. Nr 13 – Zgoda na przetwarzanie danych osobowych;
Zał. Nr 14 – Klauzula informacyjna w ramach zamówień publicznych.

DOKUMENTY POWIĄZANE

Procedura postępowania w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych;

* **Procedura zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych;**
* Metodyka oceny ryzyka;
* Prawa Pacjenta
* Procedura do działalności kadrowej zgodne z RODO;
* Procedura obsługi i korzystania z monitoringu wizyjnego;
* Procedura reagowania na incydenty bezpieczeństwa informacji;
* **Procedura postępowania w czasie przetwarzania danych osobowych pacjentów w rejestracji i gabinetach lekarskich i na oddziałach szpitalnych;**
* **Procedura czystego biurka i czystego ekranu;**
* Procedura pracy zdalnej z danymi osobowymi;
* Procedura pozyskania zgody na przetwarzanie danych osobowych;
* Procedura przechowywania danych osobowych w archiwum;
* Procedura usuwania danych;

Procedura postępowania w sytuacji naruszenia bezpieczeństwa przetwarzania danych osobowych

Celem niniejszego dokumentu jest określenie zasad postępowania **użytkowników**, **Inspektora Ochrony Danych (IOD) i Administratora** w przypadku **naruszenia bezpieczeństwa** przetwarzania danych w systemach informatycznych i nieinformatycznych do przetwarzania danych.

Przez naruszenie bezpieczeństwa przetwarzania danych osobowych należy rozumieć wszelkie zaistniałe zdarzenia w szczególności są to wszelkie sytuacje, w których nastąpiła **utrata (np. kradzież lub zniszczenie), nieuzasadniona modyfikacja danych lub części danych (nawet, jeśli możliwe jest całkowite odtworzenie utraconych danych), a także możliwość dostępu do danych dla osób nie posiadających upoważnienia do ich przetwarzania. Na możliwość wystąpienia** naruszenia bezpieczeństwa przetwarzania danych osobowych mogą wskazywać:

* nietypowy stan pomieszczeń przetwarzania (naruszone plomby, otwarte pomieszczenia, okna, drzwi od szaf, biurek, włączone urządzenia, rozerwane meble półki, szuflady);
* zaginięcie sprzętu lub nośników informacji (płyt CD/DVD, pendrive USB, inne nośniki).
* nieuzasadnione modyfikacje lub usunięcie danych;
* nieprawidłowe lub nietypowe działanie systemu informatycznego (nietypowe komunikaty wyświetlane na monitorze.

Procedura Zarządzania systemami informatycznymi

Procedura Zarządzania Systemem Informatycznym, została opracowana **w celu uregulowania zasad użytkowania, zarządzania i administrowania Systemami Informatycznymi** w Zakładzie.

Procedura obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, a w szczególności bezpośrednich przełożonych osób przetwarzających dane osobowe.

Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych w systemie informatycznym musi zostać przeszkolony przez IOD , co potwierdza w oświadczeniu stanowiącym załącznik nr 6.

Podstawą nadania uprawnień w systemie jest prawidłowo wypełniony **wniosek przełożonego** zawarty w załączniku nr 1 do niniejszej instrukcji – *formularz nr 1/I-01/KP-20* „Wniosek przełożonego o nadanie uprawnień dla użytkownika systemu informatycznego 3 egz.). Odwołanie uprawnień.

Zasady przetwarzania danych art. 5 RODO

1. **Zasada legalności** (zgodność z prawem, rzetelność i przejrzystość) art. 5 ust.1 a) RODO. ADO musi zawsze wykazać podstawę prawną przetwarzania;
2. **Zasada celowości** (przetwarzanie zgodnie z konkretnym celem) art. 5 ust. 1 b) RODO. Dane osobowe mogą być przetwarzane wyłącznie w **konkretnym celu** i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tym celem, a podmiot danych musi być o tym celu poinformowany;
3. **Zasada adekwatności** (minimalizacja ilości danych) art. 5 ust. 1 c) RODO. Można zbierać tylko tyle danych ile jest adekwatne do realizacji celu. **Nie można zbierać „na zapas" bo „może się przydadzą"**
4. **Zasada poprawności merytorycznej** (prawidłowość i aktualność) art. 5 ust. 1 d) RODO. ADO **musi dbać o poprawność danych i je aktualizować** jak tylko podmiot danych poinformuje ADO o takiej zmianie;
5. **Zasada ograniczonego czasu** (retencja przechowywania) art. 5 ust. 1 e) RODO**. Można przetwarzać dane osobowe tylko tak długo jak istnieje cel.**

Wezwania chorych do gabinetu

1. Wezwanie z wykorzystaniem **numeru identyfikacyjnego**, nadanego zgodnie ze wskazaniami art. 36 ust. 5 ustawy o działalności leczniczej, znaku/pseudonimu numerycznego. Pacjent wzywany jest wówczas do gabinetu po tym unikalnym numerze
2. Wezwanie **po numerze** nadanym podczas rejestracji. Wpisanie tych numerów do dokumentacji medycznej następuje z jednoczesnym przekazaniem ich pacjentowi. Pacjent wzywany jest wówczas do gabinetu po tym unikalnym numerze.
3. Wezwanie **po godzinie** wizyty. Wizyty umawiane są na konkretną godzinę w sposób uniemożliwiające pokrywania 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..
6. Jeśli jest to możliwe, w szczególności gdy osoba wykonująca zawód medyczny zna pacjenta, można zrezygnować ze wskazanych wyżej sposobów wezwań.
7. **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.**

Komunikacja z pacjentem dotycząca monitorowania stanu zdrowia pacjenta

1. W trakcie obchodu lekarskiego/pielęgniarskiego, na sali mogą przebywać **wyłącznie osoby uprawnione**, tj. personel medyczny, opiekun faktyczny, opiekunowie ustawowi pacjenta małoletniego, Na życzenie pacjenta w trakcie udzielania świadczenia może być obecna osoba bliska.
2. 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.
3. Lekarz podczas udzielania świadczeń zdrowotnych **ma obowiązek poszanowania intymności i godności osobistej pacjenta**, w szczególności w czasie udzielania mu świadczeń zdrowotnych, dlatego też prowadzona rozmowa dotycząca stanu zdrowia pacjenta powinna **być prowadzona na osobności**.
4. W sytuacjach, w których stan pacjenta uniemożliwia przeprowadzenie takiej rozmowy poza salą chorych, przewagę ma prawo pacjenta do uzyskania informacji o swoim stanie zdrowia.
5. Jeżeli na sali pozostają inni pacjenci to przekazywanie informacji powinno odbywać się w jak najbardziej dyskretny sposób - zastosowanie parawanu, przyciszenie głosu.

Wizyty lekarskie

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.
2. Osoby biorące udział w obchodzie inne niż udzielające świadczeń zdrowotnych, np. inni lekarze, pielęgniarki, fizjoterapeuci, biorą udział w obchodzie **bez zgody** pacjenta, jeżeli są osobami wykonującymi zawód medyczny, tylko wtedy, gdy jest to **niezbędne ze względu na rodzaj świadczenia**. Jeżeli nie spełniają tego wymogu, to mogą brać udział w obchodzie wyłącznie za zgodą pacjenta. Lekarz powinien uzyskać zgodę pacjenta na udział studentów w udzielaniu świadczeń zdrowotnych (może to być zgoda w formie ustnej).
3. 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.
4. Lekarz **nie powinien** na sali chorych **zwracać się po imieniu i nazwisku** do pacjenta. Można natomiast zwracać się do pacjenta używając chociażby zwrotu **„Pan/Pani" wraz z dodaniem imienia**, co jednocześnie zagwarantuje poszanowanie godności pacjenta. Wyjątkiem są przypadki, gdy lekarz nie może zidentyfikować pacjenta w inny sposób, niż poprzez użycie jego nazwiska, bądź gdy jest to konieczne dla podejmowania nagłych czynności ratowania życia bądź zdrowia.

Zabezpieczenia danych osobowych

1) **Sprzątanie** oraz czynności konserwacyjne powinno odbywać się w obecności oraz pod nadzorem upoważnionego personelu.
2**) Należy zamykać drzwi za każdym razem** w chwili opuszczenia pomieszczenia przez osoby upoważnione. Wskazanym działaniem będzie również proszenie o zastępstwo inną osobę upoważnioną oraz każdorazowe zabezpieczanie dokumentów i komputera, np. poprzez stosowanie wygaszacza ekranu, który po wznowieniu pracy będzie wymagał ponownego zalogowania się do systemu.
3) **Należy trwale i na bieżąco niszczyć** dokumenty zawierające dane osobowe. Dokumenty powinny być niszczone w sposób uniemożliwiający odczytanie treści na nich zawartych lub odtworzenie dokumentu.
4) Po skończonej pracy należy stosować „**zasadę czystego biurka”** czyli wszelkie dokumenty zawierające dane osobowe należy chować w szafkach/szufladach zamykanych na klucz; klucz do nich należy przechowywać w szyfrowanym kluczniku lub w innym miejscu wyznaczonym przez Administratora.

.

.

Zabezpieczenia danych osobowych

5) Należy zobowiązać personel do **zamykania drzwi** za każdym razem w chwili opuszczenia pomieszczenia przez osoby upoważnione. Wskazanym działaniem będzie również proszenie o zastępstwo inną osobę upoważnioną oraz każdorazowe zabezpieczanie dokumentów i komputera, np. poprzez stosowanie **wygaszacza ekranu**, który po wznowieniu pracy będzie wymagał ponownego zalogowania się do systemu.
6) W zeszycie, w którym kwitowany **jest odbiór dokumentacji** zasłaniać dane osobowe innych osób, składających swój podpis wcześniej.

Zgromadzone dokumenty w podajniku drukarki, wnioski klientów zawierające dane osobowe porzucone na biurku czy lista płac pracowników leżąca obok - takie przypadki to gotowa recepta na utratę lub wyciek danych osobowych.

Rekomendacje dotyczące weryfikacji tożsamości

Osoba udzielająca zdalnych świadczeń zdrowotnych może więc zapytać rozmówcę o podstawowe informacje, które jest w stanie zweryfikować na podstawie posiadanej dokumentacji, np. numer PESEL, ostatni problem zdrowotny, który był przyczyną odwiedzin w podmiocie leczniczym.

W związku z tym zasadne jest stosowanie pytań kontrolnych:

*Proszę o podanie Pana/Pani imienia i nazwiska.

*Proszę o podanie drugiego imienia.

*Proszę o podanie nr. PESEL – a w przypadku niepamiętania tego numeru:

*Proszę o podanie daty urodzenia, miejsca zamieszkania, adresu e-mail, danych osoby upoważnionej do pobierania dokumentacji medycznej etc.

Jeżeli połączenie odbywa się za pośrednictwem systemu umożliwiającego transmisję obrazu (rozmowa wideo), można poprosić rozmówcę o ukazanie dokumentu potwierdzającego tożsamość w sposób zapewniający jego widoczność dla drugiej strony.

Niezależnie od przepisów związanych z ochroną danych osobowych , wykorzystywanie danych osobowych powinno następować zawsze z poszanowaniem prywatności , intymności oraz godności pacjenta w tym jego prawa do zachowania w tajemnicy informacji o nim związanych.

Dziękuję za uwagę