KODEKS POSTĘPOWANIA

DOTYCZĄCY OCHRONY DANYCH OSOBOWYCH PRZETWARZANYCH W MAŁYCH PLACÓWKACH MEDYCZNYCH

POROZUMIENIE ZIELONOGÓRSKIE

JAMANO
PRAWO ▪ BIZNES

Warszawa, 9 listopada 2022 r.

Spis treści

Słowniczek

Poniższym pojęciom, używanym w niniejszym dokumencie, przypisuje się następujące znaczenia:

ADO – administrator danych osobowych (w RODO nazywany jest administratorem) - osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jest nim MPM, reprezentowana przez kierownictwo.

Dane osobowe - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej[1].

EROD (Europejska Rada Ochrony Danych) - organ, którego celem jest zapewnienie spójnego stosowania RODO.

Grupa Robocza Art. 29 - niezależny organ doradczy Komisji Europejskiej w zakresie ochrony danych osobowych i prywatności. Z dniem 25 maja 2018 r. zastąpiona przez EROD.

IOD (inspektor ochrony danych) – osoba fizyczna, wyznaczona przez ADO w celu wsparcia w realizacji obowiązków wynikających z RODO.

MPM – mała placówka medyczna (lub małe placówki medyczne). Do MPM na potrzeby niniejszego opracowania zalicza się podmioty wykonujące działalność leczniczą[2] – realizujące w szczególności świadczenia w rodzaju Podstawowa Opieka Zdrowotna oraz Ambulatoryjna Opieka Specjalistyczna.

NFZ - Narodowy Fundusz Zdrowia.

PZ - Federacja Związków Pracodawców Ochrony Zdrowia „Porozumienie Zielonogórskie".

RODO – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

SIM – System Informacji Medycznej w rozumieniu ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U.2022.1555 t.j.).

u.o.d.o. - ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019.1781 t.j.).

UoDL – ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U.2022.633 t.j.).

UoPPiRPP – ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U.2022.1876 t.j.).

---

[1] Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

[2] Podmiot wykonujący działalność leczniczą w rozumieniu art. 2 ust. 1 pkt 5 UoDL. Chodzi tu również lekarzy lub pielęgniarek oraz fizjoterapeutów wykonujących zawód w ramach działalności leczniczej jako praktykę zawodową, o których mowa w w/w przepisach.

1. Wstęp

1.1 Jakie są cele kodeksu postępowania dla MPM?

Niniejszy dokument stanowi kodeks postępowania w rozumieniu art. 40 RODO. Głównym celem kodeksu jest zatem doprecyzowanie zasad ochrony danych zawartych w RODO i podniesienie poziomu ochrony danych osobowych przez MPM.

Kodeks został opracowany dla MPM, aby wesprzeć je we właściwym stosowaniu przepisów RODO. To właśnie na MPM, jako administratorach danych, spoczywa obowiązek zapewnienia, że przetwarzanie danych osobowych pacjentów spełnia wymogi RODO.

Dokument zawiera praktyczne wskazówki dotyczące realizacji konkretnych obowiązków wynikających z RODO, uwzględniające specyfikę funkcjonowania MPM – w szczególności branżowe przepisy regulujące działalność leczniczą. Sektorowe zorientowanie wytycznych zawartych w kodeksie pozwoli na dopasowanie ich do oczekiwań i praktyki sektora małych placówek medycznych oraz umożliwi łatwiejsze i skuteczniejsze wdrożenie i stosowanie przepisów RODO.

Niniejszy kodeks ma również na celu zwiększenie zaufania pacjentów do MPM i gwarancję, że placówki, które przystępują do kodeksu, zapewniają bezpieczeństwo danych osobowych na odpowiednio wysokim poziomie poprzez stosowanie odpowiednich zasad i instrumentów prawnych ochrony danych przy uwzględnieniu ryzyka dla praw lub wolności pacjentów wynikającego z przetwarzania ich danych osobowych.

Kodeks ma zastosowanie jedynie do danych osobowych przetwarzanych w związku z działalnością leczniczą MPM (pacjentów, osób upoważnionych, osób bliskich, itp.). Dokument nie dotyczy przetwarzania danych osobowych pracowników, współpracowników, kandydatów do pracy w MPM lub innych osób, których dane gromadzi MPM.

1.2 Dlaczego kodeks postępowania dla MPM jest potrzebny?

RODO zmienia sposób, w jaki musimy myśleć o danych osobowych – zwiększa ich bezpieczeństwo oraz ochronę szeroko rozumianej prywatności. Nie od dziś wiadomo, że niewłaściwe przetwarzanie danych osobowych może wiązać się z bardzo poważnymi konsekwencjami dla osób, których te dane dotyczą. W obliczu dynamicznego rozwoju nowych technologii konsekwencje naruszeń bezpieczeństwa danych są coraz większe. Dlatego RODO nakazuje systematyczną analizę ryzyka wystąpienia tych negatywnych konsekwencji, jakie wiąże się z przetwarzaniem danych osobowych. To powoduje, że ochrona danych osobowych musi być procesem żywym, stale monitorowanym i poprawianym – tak by zastosowane środki bezpieczeństwa zawsze odpowiadały zmieniającym się wyzwaniom i zagrożeniom.

Wobec powyższego, na szczególną ochronę zasługują dane wrażliwe (nazywane w RODO szczególnymi kategoriami danych), jakimi są m.in. informacje dotyczące stanu zdrowia. Są to dane wprost przypisane do konkretnych osób i niezmienne. Konsekwencje dostania się takich informacji w niepowołane ręce mogą być bardzo niekorzystne. Ważne jest zatem, by wszyscy administratorzy danych, którzy wykorzystują dane wrażliwe, posiadali

odpowiednią wiedzę na temat ich ochrony i świadomość potencjalnych rodzajów ryzyka, jakie wiążą się z niewłaściwym wykorzystaniem takich danych.

Dlatego też wszystkie operacje na danych, takie jak: zbieranie, przechowywanie, usuwanie, opracowywanie, udostępnianie itd. powinny opierać się na zasadach ochrony danych odzwierciedlających podstawowe wartości RODO:

- **Zasada rzetelności i legalności.** Zasada ta wymaga, by dane przetwarzano uczciwie i zgodnie z prawem. MPM zapewnia, że dane osobowe przetwarza w zgodzie z RODO (poprzez zapewnienie podstaw prawnych przetwarzania danych i realizację praw pacjentów) oraz wszystkimi przepisami regulującymi funkcjonowanie tego podmiotu.
- **Zasada przejrzystości.** Przetwarzanie danych osobowych powinno być zrozumiałe dla osób, których dane są przetwarzane. MPM uwzględnia zatem potrzeby i oczekiwania pacjentów oraz komunikuje się z nimi w jasny i zrozumiały sposób.
- **Zasada ograniczenia celu.** Zasada ta wymaga, by wszystkie dane osobowe gromadzić w oznaczonych celach i by nie przetwarzać ich w sposób niezgodny w tymi celami. Określenie celu ustanawia ramy, których administrator danych przekroczyć nie może. MPM nie zbiera danych „na zapas", dla przyszłych nieoznaczonych jeszcze celów.

  Podkreślić jednocześnie należy, że nie jest zbieraniem „na zapas" gromadzenie informacji o stanie zdrowia w trakcie wywiadu medycznego – jest to uzasadnione wymogami medycyny i koniecznością udzielenia pacjentowi niezbędnej pomocy.

- **Zasada minimalizacji danych.** Zebrane dane muszą być adekwatne do celu, który administrator chce osiągnąć. Zasada ta wymaga, by pozyskiwać jedynie te dane, które są niezbędne do realizacji celu. MPM nie dopuszcza zatem sytuacji, kiedy zbiera się takie dane, które jedynie potencjalnie mogą zostać użyte w przyszłości. Wszystkie dane niezbędne dla prawidłowej diagnozy i procesu leczenia, nawet jeśli mają posłużyć do jego osiągnięcia w przyszłości (w tym dane zebrane podczas wywiadu medycznego), będą jednak poprawne. MPM zapewnia również, że zasada minimalizacji danych uwzględniona będzie również we wszystkich procesach tworzenia nowych produktów, usług i systemów, tak by domyślnie ograniczać ilość zbieranych danych, zakres ich przetwarzania oraz okres ich przechowywania.
- **Zasada poprawności danych**. Zgodnie z tą zasadą wszelkie dane osobowe powinny być prawidłowe i aktualne. MPM podejmuje więc starania, by informacje, które przetwarza, były zgodne z prawdą i aktualne, a w razie potrzeby sprostowane lub usunięte. W praktyce oznacza to, że kiedy MPM dowiaduje się o zmianie danych, powinna niezwłocznie ten fakt odnotować w swoich bazach i dokumentacji.
- **Zasada ograniczenia przetwarzania.** Zgodnie z nią MPM nie przechowuje danych przez okres dłuższy, niż jest to niezbędne do realizacji celu, dla którego dane te zostały zebrane. To cel przetwarzania decyduje zatem o długości okresu przechowywania danych. Oczywiście zdarzają się sytuacje uzasadniające dalsze ich przechowywanie, np. do celów archiwalnych. W praktyce funkcjonowania MPM okres przechowywania danych będzie ściśle określony przepisami regulującymi przechowywanie dokumentacji medycznej.

- **Zasada integralności i poufności.** MPM dba o bezpieczeństwo danych osobowych i przetwarza je w sposób uniemożliwiający dostęp osobom nieupoważnionym, np. poprzez stosowanie szyfrowania danych oraz zapewniający ochronę przed przypadkową utratą, zniszczeniem lub uszkodzeniem.
- **Zasada rozliczalności.** Zgodnie z tą zasadą, MPM odpowiada za przestrzeganie wszystkich powyższych zasad i jest w stanie to wykazać. Rozliczalność oznacza wdrożenie odpowiednich środków gwarantujących wysoki poziom ochrony danych oraz sporządzenie stosownej dokumentacji pokazującej, w jaki sposób przestrzegane są obowiązki wynikające z RODO. **Niniejszy kodeks może pomóc w wykazaniu przez MPM przestrzegania przepisów RODO, a jego stosowanie może posłużyć za dowód wywiązywania się MPM z obowiązków nałożonych przez RODO na administratorów danych.** W niniejszym dokumencie dajemy bowiem wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie przepisów prawa.

1.3 Kto może przystąpić do kodeksu?

Kodeks stworzył PZ we współpracy z Jamano Sp. z o.o., firmą specjalizującą się w ochronie danych osobowych. Kodeks uwzględnia również uwagi podmiotów zainteresowanych, z którymi dokument konsultowano: Fundacji Panoptykon, Fundacji Urszuli Jaworskiej oraz Polskiego Towarzystwa Zdrowia Publicznego.

Kodeks ma zastosowanie do MPM będących członkami struktur regionalnych PZ. W celu przystąpienia do stosowania kodeksu, MPM składa w formie pisemnej (w tym elektronicznej) deklarację przystąpienia zawierającą przyjęcie zobowiązania do przestrzegania zasad i postanowień w nim zawartych.

PZ po pozytywnym wyniku kontroli wstępnej w MPM, dokonanej przez podmiot monitorujący (procedura została opisana poniżej), wpisuje MPM składającą taką deklarację na listę podmiotów stosujących kodeks. Lista podmiotów, które przystąpiły do kodeksu, PZ i podmiot monitorujący publikują na swoich stronach internetowych.

Jedynie te placówki, które zostaną wpisane na listę, o której mowa wyżej, mogą powoływać się na stosowanie postanowień niniejszego kodeksu w celu wykazywania zgodności z RODO.

Zważywszy na treść wyłączenia z art. 41 ust. 6 RODO, MPM, które posiadają status podmiotu publicznego[3] (w tym przede wszystkim samodzielne publiczne zakłady opieki zdrowotnej) – decyzją PZ - nie mogą przystąpić do Kodeksu.

1.4 W jaki sposób sprawdza się czy MPM stosują zasady kodeksu?

Przestrzeganie postanowień kodeksu w placówkach, które zdecydowały się do niego przystąpić, jest stale monitorowane. Na mocy decyzji PZ, podmiotem monitorującym stosowanie zasad kodeksu jest RS JAMANO Sp. z o.o. Sp. k. Podmiot monitorujący pełni swoją

[3] Do tej grupy należy zaliczyć także jednostki budżetowe, o których mowa w art. 4 ust. 1 pkt 3) UoDL. Zgodnie z wyrażoną w u.o.d.o koncepcją definiowania pojęcia podmiotów publicznych poprzez odwołanie do definicji podmiotów sektora finansów publicznych wykluczone z zakresu podmiotowego tego pojęcia są instytuty badawcze, o których mowa w art. 4 ust. 1 pkt 4) UoDL.

funkcję do czasu uzyskania akredytacji w celu monitorowania przestrzegania warunków kodeksu, w rozumieniu art. 41 RODO. Po uzyskaniu akredytacji, podmiot monitorujący realizuje swoje zadania jako autoryzowany podmiot monitorujący, bez konieczności ponownego wskazania przez PZ.

Podmiot monitorujący spełnia następujące wymagania:

- Osoby zaangażowane po jego stronie (zespół ekspertów) wykazują się wiedzą fachową i praktycznym doświadczeniem w dziedzinie będącej przedmiotem kodeksu (w tym RODO oraz przepisów szczególnych dotyczących branży medycznej, praktycznych aspektów funkcjonowania MPM oraz mechanizmów i procedur działania MPM) oraz bezstronnością. Osoby te zapewniają brak konfliktu interesów i właściwą niezależność w prowadzeniu czynności sprawdzających, w tym przede wszystkim, że nie były one członkami kadry konkretnego MPM oraz nie wdrażały tam dokumentacji RODO.
- Podmiot monitorujący zawiera umowy o współpracy z członkami zespołu ekspertów, gwarantujące im odpowiednie wynagrodzenie za realizację zadań podmiotu monitorującego.
- Podmiot monitorujący posiada zespół ekspertów, którzy w okresie trzech lat poprzedzających zatwierdzenie kodeksu przeprowadzili łącznie co najmniej 500 audytów ochrony danych w podmiotach leczniczych.
- Podmiot monitorujący zatrudnia zespół ekspertów, w którym co najmniej jedna osoba występowała w charakterze eksperta w zakresie ochrony danych osobowych na konferencjach i spotkaniach organizowanych przez PZ.
- Finansowanie realizacji zadań przez podmiot monitorujący odbywa się w sposób zapewniający jego pełną niezależność.

Podmiot monitorujący dysponuje również:

- Odpowiednimi procedurami pozwalającymi ocenić zdolność MPM do stosowania kodeksu, monitorować przestrzeganie jego przepisów oraz okresowo dokonywać przeglądu jego funkcjonowania, w tym przede wszystkim dysponuje odpowiednią metodologią prowadzenia czynności sprawdzających,
- Strukturami i profesjonalnym personelem (odpowiednim do planowanej liczby MPM, które przystąpią do kodeksu), które prowadzić efektywne bieżące monitorowanie stosowania zasad kodeksu przez MPM i rozpatrywać skargi na ich naruszenie.

Do zadań podmiotu monitorującego będzie należało:

- Prowadzenie kontroli wstępnej MPM, które przedłożyły deklarację przystąpienia do stosowania zasad kodeksu. Podmiot monitorujący przeprowadza, za pomocą środków komunikacji elektronicznej, sprawdzenie zgodności sposobów przetwarzania danych osobowych przez MPM z RODO. Kontrola wstępna obejmuje m.in. obszary: zakres pozyskiwanych danych osobowych, sposób realizacji obowiązków informacyjnych, posiadanie wymaganej przez przepisy prawa ochrony danych dokumentacji ochrony danych, okresy retencji danych osobowych, stosowane środki techniczne i organizacyjne.

- Bieżące monitorowanie stosowania przez MPM zasad kodeksu. Podmiot monitorujący przeprowadza czynności sprawdzające nie rzadziej niż raz w roku oraz wtedy, kiedy pozyska informację o możliwym naruszeniu przez MPM postanowień kodeksu; czynności sprawdzające mogą obejmować: udostępnienie przez MPM dokumentów lub informacji dotyczących przetwarzania danych osobowych lub przeprowadzenie czynności kontrolnych w miejscu przetwarzania danych osobowych (także w formie zdalnej).
- Przyjmowanie i obsługa skarg złożonych na MPM w związku z naruszeniem postanowień kodeksu. Podmiot monitorujący prowadzi postępowania związane ze skargami - analizuje treść skarg, w razie potrzeby przeprowadza czynności sprawdzające w MPM, prowadzi korespondencję ze skarżącym oraz podejmuje decyzje w sytuacji naruszenia przez MPM postanowień kodeksu. Rozpatrzenie skargi następuję w rozsądnym terminie, nie dłuższym jednak niż 3 miesiące od dnia jej złożenia.
- Publikowanie statystycznych raportów z prowadzonych postępowań skargowych.
- Prowadzenie, wspólnie z PZ, działań promujących kodeks.

W razie powzięcia informacji o naruszeniu postanowień kodeksu, podmiot monitorujący, wzywa placówkę do złożenia wyjaśnień w terminie 14 dni, wskazując na uchybienia. W zależności od stanu faktycznego, podmiot monitorujący może:

- nakazać osobom odpowiedzialnym za przetwarzanie danych w MPM przejście zdalnego szkolenia z zakresu ochrony danych;
- ostrzec MPM, przekazując tę informację do PZ;
- przeprowadzić czynności sprawdzające w MPM;
- zawiesić MPM w razie stwierdzenia uchybień do czasu ich usunięcia przez MPM; do tego czasu zawieszony MPM nie może powoływać się na stosowanie postanowień niniejszego kodeksu w celu wykazywania zgodności z RODO;
- zdecydować o wykreśleniu MPM z grupy podmiotów stosujących kodeks; PZ, MPM oraz podmiot monitorujący aktualizują odpowiednio informacje na swoich stronach internetowych w związku z usunięciem MPM z grupy podmiotów stosujących zasady kodeksu.

MPM informuje podmiot monitorujący o każdym przypadku złożenia przez MPM zawiadomienia o naruszeniu ochrony danych, o którym mowa w art. 33 RODO oraz fakcie prowadzenia czynności kontrolnych w MPM przez organ nadzorczy.

Podmiot monitorujący, w uzgodnieniu z PZ, może zdecydować o konieczności uiszczenia opłaty przez MPM na rzecz podmiotu monitorującego za wykonywanie zadań, o którym powyżej (opłata za monitorowanie zgodności przestrzegania zasad kodeksu postępowania). Przedmiotem uzgodnień są w szczególności zasady pobierania i wysokość opłaty. Wysokość opłaty i zasady jej pobierania są komunikowane MPM przed złożeniem wniosku o przystąpienie do kodeksu.

1.5 Czy kodeks będzie podlegał przeglądom?

PZ, przy wsparciu podmiotu monitorującego, stale analizuje zmiany w przepisach regulujących funkcjonowanie MPM oraz analizuje stosowanie kodeksu w praktyce funkcjonowania MPM i w razie konieczności dokonuje stosownych zmian w kodeksie – tak by jego zasady odpowiadały na aktualne problemy i zagrożenia dla ochrony danych osobowych pacjentów. W tym celu, nie rzadziej raz do roku, PZ oraz podmiot monitorujący organizują wspólne spotkanie, którego przebieg oraz ustalenia są niezwłocznie raportowane do Prezesa UODO.

Wszelkich zmian w kodeksie PZ dokonuje zgodnie z treścią art. 27 u.o.d.o.

1.6 Czy można złożyć skargę na MPM, która nie przestrzega kodeksu?

Każda MPM publikuje na swojej stronie internetowej (jeśli taką posiada) informację o przystąpieniu do kodeksu oraz jego treść. Tekst ten zawiera również informację o możliwości i sposobie złożenia do podmiotu monitorującego skargi na MPM w związku z naruszeniem postanowień kodeksu.

Możliwe jest także złożenie skargi na sam podmiot monitorujący w związku z niewywiązywaniem się tego podmiotu ze swoich zadań i obowiązków.

Podmiot monitorujący określa szczegółowe zasady rozpatrywania skarg (w tym sposób wnoszenia, zasady prowadzenia rejestru skarg oraz sposób powiadamiania Prezesa UODO o podjętych działaniach w związku ze skargami) i przekazuje MPM w celu umieszczenia tych informacji na stronach MPM. Zasady rozpatrywania skarg PZ i podmiot monitorujący publikują na swoich stronach internetowych.

1.7 Jakie są obowiązki podmiotu monitorującego wobec organu nadzorczego?

Podmiot monitorujący raz do roku informuje Prezesa UODO o wszelkich działaniach prowadzonych przez niego w odniesieniu do kodeksu postępowania, w tym szczególności o: liście i liczbie MPM, które przystąpiły do kodeksu; liczbie skarg, które wpłynęły do podmiotu monitorującego; najczęściej pojawiających się i najważniejszych problemach w treści skarg i sposobów ich załatwienia; informacji o czynnościach sprawdzających przeprowadzonych w następstwie stwierdzenia naruszenia kodeksu.

Podstawy prawne RODO:

Artykuł 5 - Zasady dotyczące przetwarzania danych osobowych

1. *Dane osobowe muszą być:*

   a) *przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");*

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu");

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");

d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw lub wolności osób, których dane dotyczą ("ograniczenie przechowywania");

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

2. Przetwarzanie danych osobowych zgodnie z prawem

2.1 Jakie są podstawy prawne przetwarzania danych osobowych przez MPM?

Przepisy RODO określają katalog przesłanek, które legalizują przetwarzanie danych. W praktyce MPM będzie mogła przetwarzać dane osobowe pacjentów przede wszystkim jeśli:

- jest to niezbędne do celów profilaktyki zdrowotnej i zapewnienia opieki zdrowotnej na podstawie odpowiednich przepisów prawa;
- pacjent wyraził zgodę na przetwarzanie jego danych osobowych;
- MPM posiada prawnie uzasadniony interes w przetwarzaniu danych (dotyczy badań jakości oraz marketingu bezpośredniego MPM, z wyłączeniem marketingu telefonicznego i elektronicznego).

Artykuł 25 UoPPiRPP określa minimalną zawartość dokumentacji medycznej, wskazując jakie dane osobowe pacjenta można przetwarzać: imię (imiona) i nazwisko, datę urodzenia, oznaczenie płci, adres miejsca zamieszkania, numer PESEL, jeżeli został nadany, w przypadku noworodka – numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość. Natomiast w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody – nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania. Zbieranie tych danych znajduje zatem uzasadnienie w przepisie prawa i pacjent jest zobowiązany do przekazania tych danych MPM.

Co istotne, MPM ma obowiązek prowadzenia dokumentacji medycznej zarówno dla świadczeń realizowanych w oparciu o umowę na podstawie umowy z NFZ, jak i usług komercyjnych.

Pacjent MPM może wyrazić odrębną zgodę na przetwarzanie jego danych osobowych w celu otrzymywania informacji marketingowych (takich jak informacje o nowych usługach, materiały edukacyjne), np. za pośrednictwem newslettera. Należy pamiętać, że przetwarzanie danych osobowych pacjenta w celach marketingowych możliwe jest na podstawie jego dobrowolnej, konkretnej, świadomej i jednoznacznej zgody (zgodnie z RODO). Pacjent ma także prawo wyboru kanału komunikacji wykorzystywanego do przesyłania informacji marketingowych, takiego jak wiadomość e-mail, rozmowa telefoniczna, wiadomość SMS (zgodnie z ustawą Prawo telekomunikacyjne oraz z ustawą o świadczeniu usług drogą elektroniczną). Przed pozyskaniem zgody pacjenta na kontakt w celach marketingowych, należy spełnić wobec niego obowiązek informacyjny zgodnie z wytycznymi zawartymi w niniejszym kodeksie (ze szczególnym uwzględnieniem informacji o możliwości wycofania zgody na kontakt marketingowy).

W celu pozyskania skutecznej zgody na przetwarzanie danych osobowych w celach marketingowych z wykorzystaniem preferowanego przez pacjenta kanału komunikacji, można zastosować poniższą propozycję treści oświadczenia:

Chcę otrzymywać informacje dotyczące produktów, usług oraz ofert promocyjnych MPM za pośrednict

- *połączeń głosowych*
- *wiadomości SMS*
- *wiadomości mailowych*

i wyrażam zgodę na przetwarzanie moich danych osobowych w tym celu.

Istotną kwestią jest także konieczność wykazania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w celach marketingowych (zgodnie z art. 7 ust. 1 RODO) – zgodnie z zasadą rozliczalności. Możliwe jest to w szczególności poprzez udokumentowanie faktu pozyskania zgody na działania marketingowe (np. poprzez uzyskanie pisemnej zgody pacjenta, nagranie rozmowy telefonicznej czy zapisanie logów systemowych podczas zaznaczania zgód na stronie internetowej).

Zgoda na kontakt za pośrednictwem numeru telefonu lub poczty elektronicznej nie jest wymagana w przypadku konieczności przekazania pacjentowi MPM informacji o zmianie terminu planowanej wizyty lub innych informacji związanych z koordynacją udzielania świadczeń zdrowotnych, tj. potwierdzenia wizyty, jej odwołania czy przekazania informacji o innych zmianach organizacyjnych mających wpływ na realizację świadczenia. Przekazanie takich informacji jest ściśle związane z udzielaniem świadczeń i nie wymaga zgody pacjenta.

Szczególną sytuacją jest wykorzystanie danych osobowych pacjentów MPM w celu prowadzenia marketingu bezpośredniego przy wykorzystaniu tradycyjnych form komunikacji (tj. adresu korespondencyjnego pacjenta). Takie dane osobowe pacjentów MPM mogą być przetwarzane dla celu marketingu bezpośredniego na podstawie prawnie uzasadnionego interesu administratora danych w przypadku istnienia relacji, na podstawie której pacjent może spodziewać się otrzymania informacji handlowej (np. pacjent wypełnił deklarację wyboru lekarza POZ w danym MPM). **Przy czym kontakt telefoniczny lub mailowy w celach marketingowych możliwy jest wyłącznie po uzyskaniu odrębnej zgody pacjenta na kontakt z wykorzystaniem danego kanału komunikacji.**

Przesyłanie informacji handlowych przez podmioty trzecie (np. podmioty współpracujące z MPM, partnerów biznesowych), możliwe jest po uzyskaniu odrębnej zgody pacjenta (z uwzględnieniem preferowanego przez pacjenta kanału komunikacji), przy czym konieczne jest wskazanie nazwy każdego z podmiotów. Należy pamiętać, że zgoda na przetwarzanie danych osobowych jest ważna do momentu jej wycofania. Pacjent powinien mieć możliwość wycofania zgody w dowolnym momencie, bez ponoszenia z tego powodu niekorzystnych konsekwencji. Pacjent ma także prawo do wniesienia sprzeciwu wobec przetwarzania jego danych w celach marketingowych realizowanych na podstawie prawnie uzasadnionego interesu MPM.

Wszystkie wskazane powyżej przesłanki mają charakter autonomiczny, co oznacza, że MPM może przetwarzać dane osobowe w określonym celu po spełnieniu tylko jednej z nich. W praktyce oznacza to, że MPM nie musi pozyskiwać dodatkowych zgód na przetwarzanie danych osobowych pacjentów lub potencjalnych pacjentów w celu udzielania świadczeń opieki zdrowotnej, bowiem posiada już prawo do przetwarzania danych osobowych na podstawie konkretnego przepisu prawa.

2.2 Kiedy przepis prawa będzie podstawą do przetwarzania danych?

Wykorzystanie danych o stanie zdrowia pacjentów oznacza, że MPM musi spełnić przynajmniej jedną przesłankę z art. 9 RODO, poświęconego podstawom wykorzystania szczególnych kategorii danych. Dla placówek medycznych taką przesłanką jest ta wskazana w art. 9 ust. 2 lit. h RODO, która dotyczy przetwarzania niezbędnego m.in. do celów profilaktyki zdrowotnej lub medycyny pracy oraz zapewnienia opieki zdrowotnej. Przepis ten nie stanowi jednak samodzielnej podstawy prawnej – funkcjonuje jedynie w połączeniu z odpowiednim przepisem polskiego prawa.

Należy szukać zatem stosownych przepisów polskich ustaw i rozporządzeń odnoszących się do szeroko rozumianego obszaru medycznego. W zależności od zakresu udzielanych świadczeń, wśród nich można wymienić w szczególności:

- UoPPiRPP,
- UoDL,
- ustawę o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
- ustawę o systemie informacji w ochronie zdrowia,
- ustawę o podstawowej opiece zdrowotnej,
- ustawę o zawodach lekarza i lekarza dentysty,
- ustawę o zawodach pielęgniarki i położnej,
- ustawę o służbie medycyny pracy,
- ustawę o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi,
- ustawę o leczeniu niepłodności,
- ustawę o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów,
- ustawę o publicznej służbie krwi,
- ustawę o opiece zdrowotnej nad uczniami.

W tych przepisach MPM znajdzie co do zasady jasne i precyzyjnie wskazania celu przetwarzania, rodzaje danych, które można zbierać oraz okresy ich przechowywania. Wszelkie rozważania dotyczące zasady ograniczonego celu i minimalizacji danych, poczynione wcześniej, będą miały szczególne zastosowanie do tej sytuacji.

Z uwagi na szczególny charakter danych dotyczących zdrowia, przepisy RODO przewidują również, że dane te mogą być przetwarzane wyłącznie przez pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej lub inną osobę podlegającą obowiązkowi zachowania tajemnicy zawodowej.

2.3 W jakich innych sytuacjach MPM może wykorzystywać dane osobowe pacjentów bez ich zgody?

Przepisy prawa są również podstawą do wysyłania zaproszeń na badania z zakresu profilaktyki zdrowotnej oraz zbierania danych o stanie zdrowia niezbędnych do realizacji programów zdrowotnych lub programów polityki zdrowotnej (programy finansowane ze środków publicznych). W zależności jednak od rodzaju badania profilaktycznego będziemy mieli do czynienia z inną podstawą przetwarzania z RODO.

Przy **profilaktyce ściśle związanej z ciągłością leczenia** przesłanką wykorzystania danych jest art. 9 ust. 2 lit. h RODO oraz stosowne przepisy, np. ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

Przykładem takiej profilaktyki jest kierowanie pacjenta chorego na cukrzycę na badanie okulistyczne z uwagi na ryzyko retinopatii cukrzycowej.

Na potrzeby takich działań możliwe jest więc wykorzystanie informacji o stanie zdrowia pacjenta.

Profilaktyka **niezwiązana z ciągłością leczenia** będzie z kolei realizowania na podstawie art. 6 ust. 1 lit. e RODO w związku z właściwymi przepisami prawa. Z tego rodzaju działaniem będziemy mieli do czynienia wówczas, gdy np. podmiot leczniczy przesyła pacjentowi za pomocą środków komunikacji na odległość informację o tym, że znajduje się on w przedziale wiekowym, gdzie statystycznie i zgodnie ze stanem wiedzy medycznej mogą u niego wystąpić różne choroby. Do realizacji wspomnianych działań nie stosuje się danych wrażliwych pacjenta.

Mając na względzie powyższe, w pojęciu profilaktyki związanej z ciągłością leczenia nie będzie mieścić się działanie polegające na informowaniu pacjenta o zalecanych zabiegach, które **nie są związane z udzielonym świadczeniem**.

Jeżeli zatem MPM będzie kierować do pacjenta informację o zalecanym badaniu wzroku ze względu na wiek pacjenta, a pozyskał jego dane w związku z udzieleniem mu świadczenia polegającego na złożeniu kości piszczelowej, to tego rodzaju działanie nie będzie mieścić się w pojęciu profilaktyki podejmowanej w celu zapewnienia ciągłości leczenia.

Przy badaniach profilaktycznych każdego rodzaju należy pamiętać o realizacji szczegółowych wytycznych (np. dotyczących kwalifikacji do w/w badań lub zakresu gromadzonych danych), określonych w przepisach wykonawczych do właściwej ustawy (np. rozporządzenia dotyczącego świadczeń gwarantowanych).

2.4 Czy można wykorzystywać dane pacjentów do przeprowadzania badania satysfakcji?

Wobec braku podstaw prawnych wykorzystywania danych pacjentów do celów związanych z prowadzeniem badań satysfakcji, chcąc przeprowadzić badanie ankietowe, MPM musi wykorzystać do tego celu ankiety anonimowe. Oznacza to, że przy tej okazji nie są zbierane żadne dane mogące posłużyć do identyfikacji konkretnego pacjenta, a pytania przygotowane są na takim poziomie ogólności, który uniemożliwia taką identyfikację. Niedopuszczalną praktyką będzie również wykorzystanie danych osobowych pacjenta do wysłania zaproszenia do udziału w ankiecie lub samej ankiety.

Przykładem badań satysfakcji pacjentów objętych opieką zdrowotną są badania przewidziane m.in. w przepisach w zakresie standardów organizacyjnych opieki okołoporodowej oraz zestawu standardów akredytacyjnych w POZ.

Wyniki badań ankietowych nie mogą wiązać się z negatywnymi konsekwencjami dla pacjenta, np. w formie nieprzyjemnego zachowania lekarza wobec pacjenta, który krytycznie ocenił go w ankiecie.

To samo dotyczy praw samych lekarzy – wynik badania ankietowego w żadnym stopniu nie może być wykorzystany do wyciągania konsekwencji służbowych wobec lekarzy, np. na podstawie przepisów kodeksu pracy. Takie badania służą bowiem realizacji celu zupełnie innego niż kontrola i ocena pracowników.

Anonimowa ankieta satysfakcji pacjenta powinna składać się z pytań zamkniętych, które będą dotyczyły obszarów najbardziej istotnych dla prawidłowego funkcjonowania placówki.

Przykłady pytań:

1. Co jest dla Pani/Pana najbardziej istotne podczas korzystania ze świadczeń zdrowotnych w naszej placówce?
    a. przyjazne podejście do pacjenta personelu rejestracji,
    b. uprzejmość personelu medycznego,
    c. wysokie kompetencje personelu medycznego,
    d. kompleksowa informacja dotycząca diagnozy,
    e. warunki lokalowe.
2. Jak długo czekał/a Pan/Pani na wizytę do specjalisty w naszej placówce?
    a. wizyta odbyła się tego samego dnia,
    b. wizyta odbyła się po (wpisać liczbę dni, miesięcy),
    c. nadal czekam na wizytę.
3. Czy w trakcie rejestracji do naszej placówki zapewniono Pani/Panu możliwość poufnego przekazania informacji, tj. w taki sposób by nie słyszały tego inne osoby czekające w kolejce?
    a. tak,
    b. nie.

2.5 W jakich celach MPM może zbierać zgody na przetwarzanie danych?

Jak już wspomniano wyżej, przetwarzanie danych pacjenta do celów niemedycznych jest możliwe na podstawie zgody. W praktyce funkcjonowania MPM zgoda będzie najczęściej podstawą przetwarzania danych w celu realizacji działań do celów marketingowych, w tym wysyłania newsletterów na wskazany przez pacjenta adres poczty elektronicznej czy innych form reklamy, informacji mających na celu budowanie pozytywnego wizerunku MPM i pozyskanie nowych pacjentów (np. informacja o nagrodzie zdobytej przez jednego z lekarzy zatrudnionych w MPM).

Jako działania marketingowe nie są traktowane kierowane do pacjentów MPM informacje nierozerwalnie związane z udzielanymi świadczeniami zdrowotnymi, zawierające ważny dla pacjentów przekaz związany z pracą placówki medycznej lub zakresem udzielanych świadczeń, np.:

- informacja o uruchomieniu serwisu internetowego, który umożliwia rejestrację wizyty online,
- informacja o zmianach godzin funkcjonowania MPM,

- informacja o wdrożonych w MPM udogodnieniach dla osób z niepełnosprawnością (np. zamontowanie windy czy podjazdu).

Wysyłanie powyższych informacji będzie możliwe bez zgody marketingowej pacjentów. MPM ma bowiem prawo podawać do wiadomości publicznej informacje o zakresie i rodzajach udzielanych świadczeń zdrowotnych, zgodnie z przepisami UoDL. Treść i forma tych informacji nie mogą mieć jednak cech reklamy.

Możliwa będzie również zgoda pacjenta na udostępnienie jego danych w celu prowadzenia badań naukowych. Należy wówczas pamiętać, że taka zgoda powinna być wyraźnym oświadczeniem pacjenta, które nie będzie pozostawiało wątpliwości, na co pacjent się zgadza.

MPM prosi o wyraźną zgodę pacjenta na przekazanie jego dokumentacji medycznej do eksperta z biobanku, do którego MPM zwraca się o dokonanie analizy naukowej. Z uwagi na szczególny charakter tych informacji MPM prosi o podpis osobę, której dane dotyczą, w celu uzyskania ważnej wyraźnej zgody oraz aby móc później wykazać, że taką wyraźną zgodę od tego pacjenta otrzymano.

2.6 Jak należy zbierać zgody na przetwarzanie danych?

Zgoda na przetwarzanie danych osobowych zawsze powinna mieć charakter dobrowolnego, konkretnego, świadomego oraz jednoznacznego wyrażenia swojej woli – w formie oświadczenia lub wyraźnego działania potwierdzającego. Pacjent może wyrazić zgodę na przetwarzanie danych osobowych poprzez złożenie ustnego lub pisemnego oświadczenia, ale także poprzez innego rodzaju działanie (którego wykonanie placówka może potwierdzić). Przed wyrażeniem zgody pacjent powinien mieć możliwość zapoznania się z klauzulą informacyjną (dostępną na stronie internetowej, pod formularzem, w treści kuponu konkursowego lub innego dokumentu, za pośrednictwem którego pozyskiwana jest zgoda). Wyrażenie zgody powinno nastąpić przed faktycznym rozpoczęciem przetwarzania danych przez MPM.

Działanie potwierdzające oznacza, że pacjent musiał podjąć celowe działanie w celu wyrażenia zgody. Może to polegać na:

- zaznaczeniu okienka wyboru podczas przeglądania strony internetowej,
- podaniu adresu poczty elektronicznej np. w celu otrzymania zaproszenia do udziału w wydarzeniach promocyjnych lub bezpłatnej próbki wyrobu medycznego,
- pozostawieniu swojej wizytówki podczas loterii z nagrodami.

Zgodnie z Wytycznymi EROD 5/2020[4], możliwe jest również uzyskanie zgody wyraźnej poprzez złożenie ustnego oświadczenia, „jednak administratorowi może być trudno udowodnić,

[4] Wytyczne EROD 5/2020 w sprawie zgody na podstawie rozporządzenia 2018/679. Są one, według EROD, lekko poprawioną wersją (*slightly updated version*) Wytycznych Grupy Roboczej art. 29 dotyczących zgody na mocy rozporządzenia 2016/679WP 259. W obu dokumentach uwagi dotyczące zgody wyraźnej znajdują się na stronach 20-21: https://uodo.gov.pl/pl/414/1607.

że spełniono wszystkie przesłanki ważnej wyraźnej zgody w chwili, gdy przyjmowano oświadczenie".

W sytuacji, kiedy zgoda obejmuje wykorzystanie danych o stanie zdrowia, standardem powinno być zatem złożenie stosownego oświadczenia przez pacjenta (w formie papierowej bądź elektronicznej) – tak by MPM mogła w łatwy sposób wykazać, że zgoda została udzielona w sposób wyraźny.

Niedopuszczalne będą natomiast wszelkie modele pozyskiwania zgody opierające się na milczeniu, bierności czy nieuwadze pacjenta. Ważną zgodą nie będzie zatem zignorowanie przez osobę domyślnie zaznaczonego okienka, jak również korzystanie przez MPM z opcji domyślnych, które osoba musi zmienić, aby odmówić MPM przetwarzania swoich danych.

Bardzo ważnym aspektem w kontekście zasady rozliczalności jest konieczność udowodnienia, że pacjent wyraził na coś swoją zgodę świadomie. Dobrą praktyką będzie zatem dokumentowanie czynności związanych z pozyskiwaniem zgód, np. rejestrowanie zgód udzielonych ustnie lub ewidencjonowanie oświadczeń o wyrażeniu zgody. W taki sposób możliwe będzie wykazanie sposobu i okoliczności pozyskania zgody pacjenta na przetwarzanie jego danych osobowych w określonym celu, a także potwierdzenie faktu realizacji obowiązku informacyjnego wobec osoby, której dane są przetwarzane.

2.7 Jakie warunki MPM musi spełnić, by zgoda była ważna?

Aby zgoda była ważna, oświadczenie lub działanie potwierdzające musi być dobrowolne, konkretne, świadome i jednoznaczne. Jak podkreśla Prezes Urzędu Ochrony Danych Osobowych[5] (do 25 maja 2018 r. Generalny Inspektor Ochrony Danych Osobowych, GIODO) kryteria te oznaczają[6]:

Dobrowolność – możliwość realnego, swobodnego wyboru, bez jakiegokolwiek przymusu; brak zgody nie może również powodować negatywnych konsekwencji dla osoby, której dane dotyczą; MPM dba, by pozyskiwane zgody nie były wymuszone, tj. nie mogą być przedkładane do podpisu jako konieczny element realizacji świadczenia medycznego (np. zgoda zawarta na formularzu do kontaktu marketingowego).

Konkretność – precyzyjne określenie celu przetwarzania danych oraz zakresu danych; niedopuszczalne jest zbieranie zgód blankietowych, ogólnych; należy również wyraźnie oddzielić informacje związane z uzyskiwaniem zgody od informacji dotyczących innych kwestii; MPM w klauzuli zgody wskazuje nazwę i adres administratora oraz cele przetwarzania.

Świadomość – przed uzyskaniem zgody należy osobom, których dane dotyczą, zapewnić niezbędne informacje do podjęcia świadomej decyzji i zrozumienia, na co wyrażają zgodę;

[5] Organ nadzorczy odpowiedzialny za kontrolę przestrzegania RODO na terytorium RP.

[6] Stanowisko dotyczące ważności zgód na przetwarzanie danych osobowych: https://giodo.gov.pl/pl/1520281/10303.

prosząc o zgodę, MPM powinna używać jasnego i prostego języka, zrozumiałego dla pacjenta;

Jednoznaczność – dana osoba musi podjąć celowe działanie w celu wyrażenia zgody na określone przetwarzanie; ważna zgoda może być np. jednoznacznie potwierdzona pisemnym lub ustnym oświadczeniem. MPM dba, by forma udzielenia zgody uwzględniała te wymogi.

2.8 Czy można wycofać swoją zgodę?

Pacjent powinien otrzymać informację, że jego zgoda na przetwarzanie danych osobowych jest ważna do momentu jej wycofania. Należy zatem również poinformować pacjenta, jak może łatwo i skutecznie wycofać udzieloną zgodę.
W praktyce oznacza to, że jeśli zgoda była pozyskana na przykład za pośrednictwem strony internetowej, jej odwołanie powinno być możliwe również za pomocą strony internetowej. Odwołanie zgody oznacza, że nie można tych danych dłużej przetwarzać w celu, w jakim zostały zebrane, nie wpływa to jednak na legalność operacji przetwarzania sprzed momentu wycofania zgody.

Podstawy prawne RODO:

Artykuł 6 - Zgodność przetwarzania z prawem

1. *Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:*

   a) *osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;*

   b) *przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;*

   c) *przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;*

   d) *przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;*

   e) *przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;*

   f) *przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, kiedy nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem, w myśl art. 6, 7 i 9 RODO.*

Artykuł 7 - Warunki wyrażenia zgody

1. *Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.*
2. *Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.*
3. *Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.*
4. *Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.*

Artykuł 9 - Przetwarzanie szczególnych kategorii danych osobowych

1. *Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.*
2. *Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:*
   a) *osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;*
   b) *przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującym odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;*
   c) *przetwarzanie 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;*

d) *przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;*

e) *przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;*

f) *przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;*

g) *przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;*

h) *przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;*

i) *przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw lub wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;*

j) *przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowychi interesów osoby, której dane dotyczą.*

3. *Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa*

państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. *Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.*

3. Dane osobowe w MPM

3.1 Jakie dane osobowe przetwarza MPM?

Mała placówka medyczna przetwarza przede wszystkim dane osobowe niezbędne do realizacji celów, jakimi są profilaktyka zdrowotna, medycyna pracy, rejestracja i świadczenie usług opieki zdrowotnej oraz ochrona żywotnych interesów[7] osoby, której dane dotyczą. W określonych wypadkach MPM przetwarza także dane osobowe w związku z działaniami marketingowymi oraz realizacją badań klinicznych i naukowych.

Przepisy branżowe wskazują jednoznacznie zakres danych zbieranych przez MPM:

- na potrzeby prowadzenia indywidualnej dokumentacji medycznej,
- w deklaracji wyboru oraz
- w oświadczeniu o przysługującym świadczeniobiorcy prawie do świadczeń opieki zdrowotnej.

Przepisy określają minimalny zakres informacji, jakie powinny znaleźć się w dokumentacji medycznej oraz wskazują na dane osobowe, które można zbierać w uzasadnionych przypadkach.

W trosce o prawa osoby fizycznej członkowie kodeksu przyjmują, że w ramach udzielania świadczeń zdrowotnych będą zbierać wyłącznie dane osobowe niezbędne do realizacji celów nałożonych na MPM przez przepisy obowiązującego prawa.

3.2 Jaki zakres danych może przetwarzać MPM dla celów medycznych?

Na potrzeby kodeksu przyjmuje się, że będą to przede wszystkim dane wymienione w UoPPiRPP i ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych oraz aktach wykonawczych do nich.

[7] Żywotne interesy osoby, której dane dotyczą, należy rozumieć jako interesy niezbędne dla życia tej osoby.

3.2.1 Dane, których przetwarzanie przez MPM jest obowiązkowe lub możliwe

D	dokumentacja medyczna indywidualna
W	deklaracja wyboru świadczeniodawcy udzielającego świadczeń z zakresu POZ
O	oświadczenie o przysługującym świadczeniobiorcy prawie do świadczeń opieki zdrowotnej
*	wyłącznie w sytuacji, gdy pacjent nie posiada numeru PESEL
**	jeżeli zawód pacjenta wiąże się z określonymi czynnikami ryzyka
***	tylko w przypadku matki noworodka nieposiadającego numeru PESEL
****	jeżeli pacjent poda z własnej inicjatywy (po wcześniejszym poinformowaniu przez MPM, że data urodzenia będzie używana wyłączenie do potwierdzenia tożsamości)

Tabela 1. Legenda tabeli danych, których przetwarzanie przez MPM jest obowiązkowe lub możliwe.

DANE PACJENTA			
Lp.	**Kategoria danych**	**Obowiązek przetwarzania**	**Możliwość przetwarzania**
1	imię (imiona)	D, W, O	
2	nazwisko	D, W, O	
3	PESEL	D, W, O	
4	data urodzenia	D*, W	
5	adres zamieszkania	D, W, O	
6	płeć	D*	
7	numer telefonu	W	
8	adres poczty elektronicznej	W	
9	numer dokumentu potwierdzającego tożsamość	D*, W*, O	
10	rodzaj dokumentu potwierdzającego tożsamość (w tym nazwa dokumentu i nazwa kraju, w którym został wystawiony)	D*, O	
11	numer i rodzaj dokumentu potwierdzającego szczególne prawo do świadczeń	D	
12	zawód		D**

DANE PRZEDSTAWICIELA USTAWOWEGO PACJENTA[8]			
Lp.	**Kategoria danych**	**Obowiązek przetwarzania**	**Możliwość przetwarzania**
1	imię (imiona)	D, W, O	
2	nazwisko	D, W, O	
3	PESEL	D***, O	
4	numer telefonu		W
5	adres zamieszkania	D, W, O	
DANE OSOBY UPOWAŻNIONEJ PRZEZ PACJENTA			
Lp.	**Kategoria danych**	**Obowiązek przetwarzania**	**Możliwość przetwarzania**
1	imię (imiona)	D	
2	nazwisko	D	
3	dane kontaktowe		D
4	data urodzenia		D****

Tabela 2. Tabela danych, których przetwarzanie przez MPM jest obowiązkowe lub możliwe.

3.2.2 Dane, których MPM nie może przetwarzać (na potrzeby prowadzenia dokumentacji medycznej)

DANE PACJENTA	
Lp.	**Kategoria danych**
1	miejsce urodzenia
2	obywatelstwo
3	stan cywilny
4	wykształcenie
DANE OSOBY UPOWAŻNIONEJ PRZEZ PACJENTA	
Lp.	**Kategoria danych**
1	stopień pokrewieństwa / relacje z pacjentem
2	numer i rodzaj dokumentu potwierdzającego tożsamość

Tabela 3. Tabela danych, których MPM nie może przetwarzać.

[8] W przypadku oświadczenia (O) mogą to być również dane opiekuna prawnego lub faktycznego pacjenta.

3.2.3 Szczególne kategorie danych

Podczas wizyty lekarskiej pacjent może podać lekarzowi informacje dotyczące chorób genetycznych, życia seksualnego, informacje o nałogach, może to być także informacja o przynależności wyznaniowej (pacjent może nie wyrazić zgody na wykonanie proponowanego zabiegu ze względu na swoje wyznanie). Powyższe dane są niezbędne do prawidłowego procesu leczenia pacjenta i mogą być zbierane przez MPM – ich podanie jednak zawsze jest dobrowolne.

3.3 Jaki zakres danych może przetwarzać MPM dla celów identyfikacji osób innych niż pacjenci?

W celu **minimalizacji** zbieranych danych członkowie kodeksu określają, że dla potrzeb identyfikacji osoby upoważnionej lub przedstawiciela ustawowego pacjenta przez pacjenta obowiązkowymi danymi podawanymi podczas składania oświadczenia będą: imię i nazwisko oraz – w przypadku dobrowolnego przekazania przez tę osobę – data urodzenia osoby upoważnionej. **Data urodzenia** może być używana wyłącznie do potwierdzenia tożsamości, stąd **nie powinna być pozyskiwana w każdym przypadku**, a jedynie wtedy, gdy istnieje potrzeba dodatkowej weryfikacji osoby upoważnionej (np. w zasobach placówki znajduje się już osoba posiadająca to samo imię i nazwisko lub też osoba posiada bardzo popularne imię i nazwisko).

MPM nie zbiera również w tym celu numerów PESEL czy też numerów dokumentów potwierdzających tożsamość.

4. Zbieranie danych osobowych

4.1 Od kogo MPM otrzymuje dane osobowe?

Od kogo MPM otrzymuje dane osobowe	W jaki sposób
Pacjent, jego przedstawiciel ustawowy lub osoba trzecia (w tym opiekun faktyczny)	Osobiście (np. podczas rejestracji, wizyty lekarskiej), pocztą (np. w przesyłanych wnioskach lub zapytaniach), elektronicznie (np. mailem lub poprzez platformę służącą do rejestracji on-line), telefonicznie.
Kontrahenci i inne placówki medyczne (np. laboratorium)	Osobiście, pocztą, elektronicznie (np. za pomocą systemu umożliwiającego dostęp do wyników badań pacjentów on-line), telefonicznie.

Tabela 4. Zestawienie źródeł danych osobowych i sposób ich uzyskiwania przez MPM.

4.2 Jakie procedury należy opracować na potrzeby zbierania danych?

Niezależnie od sposobu zbierania danych osobowych, MPM musi w razie konieczności wykazać, że **dane osobowe zostały pozyskane zgodnie z prawem**. W związku z tym opracowuje odpowiednie procedury dotyczące zbierania danych osobowych, instrukcje dotyczące przyjmowania i sprawdzania dokumentów, które wpływają do placówki (niezależnie od tego, czy jest to forma papierowa, czy elektroniczna) oraz identyfikacji osób, których dotyczą dane.

Na każdym etapie przetwarzania danych osobowych bardzo ważna jest weryfikacja zarówno osoby, której dane przetwarzamy, jak i osoby, której udostępniamy dane osobowe. W związku z powyższym ADO wyraźnie informuje personel odpowiedzialny za przetwarzanie danych osobowych, pacjentów oraz osoby trzecie, które chcą uzyskać dostęp do danych o tym, jakie dokumenty mogą być wymagane przez MPM w celu weryfikacji tożsamości. Taką informację zamieszcza w widocznym miejscu w strefach przebywania pacjentów (np. rejestracja, tablica informacyjna przed gabinetem lekarskim).

Pacjent może dostarczyć deklarację wyboru świadczeniodawcy do MPM na piśmie lub za pomocą SIM. Każda wspomniana forma wymaga podpisu pacjenta lub przedstawiciela ustawowego. W wypadku dokumentacji elektronicznej wymagany jest podpis kwalifikowany albo potwierdzony profilem zaufanym ePUAP. Obowiązkiem MPM jest sprawdzenie, czy ww. deklaracja złożona w wersji papierowej została wypełniona prawidłowo i czy zawiera wyłącznie dane wskazane w ustawie o podstawowej opiece zdrowotnej**.**

Dokumenty pomocne przy weryfikacji tożsamości pacjenta lub osoby chcącej uzyskać dostęp do danych osobowych (wyliczenie jest przykładowe i nie ma charakteru katalogu zamkniętego):

a) Dokument potwierdzający tożsamość, np. dowód osobisty, paszport, karta pobytu, polski dokument tożsamości cudzoziemca;

b) Inne dokumenty publiczne pozwalające na jednoznaczną identyfikację, np. prawo jazdy, legitymacja szkolna dla osoby do 18 roku życia;

c) akt urodzenia dziecka oraz dokument potwierdzający tożsamość (jeżeli personel medyczny ma wątpliwości, czy osoba zgłaszająca się na wizytę z dzieckiem lub wnioskująca o informację / dokumentację medyczną dotyczącą małoletniego pacjenta jest jego rodzicem i tym samym ma prawo wglądu do danych osobowych);

d) odpis orzeczenia sądowego, np. ustanawiającego opiekę nad niepełnosprawnym lub małoletnim oraz dokument potwierdzający tożsamość (jeśli personel medyczny ma wątpliwości, czy osoba zgłaszająca się na wizytę z pacjentem lub wnioskująca o informację / dokumentację medyczną jest jego opiekunem prawnym i tym samym ma prawo wglądu do danych osobowych).

W wypadku wszystkich powyższych dokumentów, MPM nie kopiuje ich ani nie skanuje do dokumentacji, prosi jedynie o ich okazanie (wyjątkiem są przypadki, w którychkiedy możliwość kopiowania dokumentu przewidują przepisy prawa, jak np. w przypadku karty EKUZ). Nie należy również spisywać danych z dokumentów innych niż niezbędne dla realizacji świadczenia.

4.3 Jak długo MPM może przechowywać dane osobowe?

Dane osobowe powinny być przechowywane nie dłużej, niż jest to niezbędne do realizacji celów, dla których dane te zostały zebrane (art. 5 ust. 1 pkt e RODO). Okres przechowywania jest zatem uzależniony od celu przetwarzania. Jeśli więc MPM zbiera dane w celu:

- zapewnienia opieki medycznej - dane przechowuje się 20 lat (termin liczony od końca roku kalendarzowego, kiedy dokonano ostatniego wpisu w dokumentacji) lub nawet 30 lat w wypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia – stosownie do przepisów UoPPiRPP lub innych przepisów (między innymi regulujących medycynę pracy);
- przesyłania pacjentom materiałów marketingowych - dane te można przetwarzać dopóki MPM posiada ważną zgodę pacjenta lub też do momentu wyrażenia sprzeciwu jeśli podstawą jest realizacja prawnie uzasadnionego interesu MPM.

4.3.1 Okres przechowywania dokumentacji medycznej

Domyślnie dokumentację medyczną przechowuje się przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu (zgodnie z art. 29 ust. 1 UoPPiRPP). Szczegółowe określenie, jak długo należy przechowywać określone rodzaje dokumentacji, wskazano w załączniku nr 1 do Kodeksu.

4.4 W jaki sposób MPM powinna przechowywać papierową dokumentację medyczną?

Papierowa dokumentacja medyczna powinna być przechowywana w taki sposób, aby:

- miały do niej dostęp jedynie osoby upoważnione oraz
- zabezpieczyć ją przed przypadkowym lub celowym uszkodzeniem, zniszczeniem, kradzieżą lub innym negatywnym zdarzeniem powodującym jej utratę.

Jeżeli MPM dysponuje oddzielnym pomieszczeniem, w którym przechowuje się niewykorzystywaną na co dzień dokumentację medyczną (pełniącym rolę archiwum), zalecane jest spełnianie następujących wymagań:

- fizyczny dostęp do pomieszczenia powinien być zabezpieczony minimum poprzez drzwi wyposażone w dodatkowy zamek (jako dodatkowe zabezpieczenie należy rozważać m.in. drzwi antywłamaniowe, czujkę ruchu obejmującą pomieszczenie, kamerę monitoringu obejmującą pomieszczenie);

- jeśli w pomieszczeniu są okna – powinny być one zabezpieczone kratami lub roletami antywłamaniowymi;
- dokumentacja powinna być przechowywana w szafach, szafkach lub na regałach; dokumenty nie mogą być przechowywane w pudłach lub kartonach stojących bezpośrednio na podłodze (jest to szczególnie istotne, gdy w pomieszczeniu pełniącym rolę archiwum biegnie rura wodociągowa lub kanalizacyjna);
- w pomieszczeniu należy utrzymywać odpowiednią temperaturę (14-20°C, ± 2°C wahania w ciągu 24 godzin) i wilgotność (wilgotność względna 45-60%, ± 5% wahania w ciągu 24 godzin)[9];
- dokumentacja powinna być regularnie sprawdzana pod kątem śladów obecności grzybów pleśniowych, owadów lub gryzoni, a także takich czynników jak wilgoć czy kurz;
- sprzątanie pomieszczenia pełniącego rolę archiwum powinno odbywać się w obecności przynajmniej jednej osoby z personelu MPM.

Gdyby na skutek zalania, pożaru lub innej przyczyny część dokumentacji uległa zniszczeniu, należy niezwłocznie sporządzić notatkę opisującą:

- datę wystąpienia zniszczenia lub stwierdzenia zniszczenia przez personel MPM;
- opis przyczyny zniszczenia (np. podtopienie, zalanie, pożar);
- opis podjętych czynności – np. osuszanie i sortowanie dokumentacji, odtwarzanie treści uszkodzonej dokumentacji (o ile jest taka możliwość, np. gdy dane będą jednocześnie utrwalone w programie komputerowym).

5. Formy przetwarzania danych

5.1 W jakiej formie MPM przetwarza dane osobowe?

MPM przetwarza dane osobowe pacjentów w formie papierowej lub elektronicznej. Każda z tych form wymaga odpowiedniej ochrony i dostosowania zabezpieczeń.

MPM musi zapewnić integralność danych i stały dostęp do dokumentacji osobom upoważnionym. W wypadku dokumentacji medycznej każdy wpis w niej dokonywany – niezależnie od formy jej prowadzenia – musi być opatrzony podpisem i danymi identyfikacyjnymi osoby go wprowadzającej, a każda zmiana musi być zarejestrowana.

W wypadku dołączania do dokumentacji prowadzonej w formie elektronicznej dokumentów utworzonych w postaci papierowej należy stworzyć procedurę, która krok po kroku opisuje, w jaki sposób z zachowaniem wiarygodności danych powinny one być digitalizowane.

[9] Wartości wywiedzione z załącznika do rozporządzenia Ministra Kultury z dnia 15 lutego 2005 r. w sprawie warunków przechowywania dokumentacji osobowej i płacowej pracodawców (Dz.U.2005.32.284).

Powyższa procedura powinna wskazywać osobę odpowiedzialną za wykonanie czytelnego odwzorowania cyfrowego dokumentacji papierowej i zdjęć radiologicznych oraz umieszczenie jej w systemie informatycznym. System powinien odnotowywać datę wprowadzenia dokumentu oraz dane osoby, która wprowadziła materiał do systemu. Administrator musi wybrać odpowiedni sposób digitalizacji dokumentacji medycznej, który zapewni dostęp i spójność dokumentacji.

Należy także opisać, co zrobić z oryginałem dokumentu po wprowadzeniu go do systemu informatycznego, uwzględniając przy tym wymogi aktualnego rozporządzenia ws. dokumentacji medycznej, które wyraźnie wskazuje, że dołączenie do dokumentacji elektronicznej dokumentów utworzonych w innej postaci powinno być dokonane przez osobę upoważnioną przez MPM w sposób zapewniający czytelność, dostęp i spójność dokumentacji. Po wykonaniu digitalizacji danych oryginał powinien być wydany pacjentowi lub trwale zniszczony, w sposób uniemożliwiający identyfikację pacjenta. Zdigitalizowany dokument jest ważnym nośnikiem informacji w rozumieniu kodeksu cywilnego, nie ma potrzeby zatem (z kilkoma wyjątkami[10]) przetrzymywania papierowej wersji dokumentu.

Dane osobowe pacjentów mogą być także przetwarzane za pośrednictwem systemów teleinformatycznych lub systemów łączności wykorzystywanych do udzielania świadczeń zdrowotnych bez konieczności osobistego stawiennictwa pacjenta w placówce.[11] MPM musi zadbać o bezpieczeństwo danych otrzymywanych i przekazywanych podczas udzielania powyższych świadczeń. Powinna opracować procedury, które pozwolą na ustalenie tożsamości pacjenta i szczegółowo opisać zakres usług, jakie mogą być udzielone bez fizycznej obecności pacjenta.

W razie korzystania z usług podmiotów zewnętrznych związanych z wykorzystywaniem, np. rejestracji online lub udzielania porad medycznych online należy pamiętać o podpisaniu z nimi stosownej umowy powierzenia.

Ponadto MPM powinna dopilnować, aby pacjenci korzystający z systemów teleinformatycznych lub systemów łączności udostępnionych przez placówkę w celu udzielania świadczeń, mieli możliwość zapoznania się z regulaminem usługi oraz informacją na temat przetwarzania danych osobowych (przy czym zapoznanie się ze wskazanymi dokumentami powinno nastąpić przed założeniem przez pacjenta konta w systemie i może zostać potwierdzone na etapie rejestracji, np. za pomocą zaznaczenia okienka: „Tak, potwierdzam zapoznanie się z regulaminem oraz zasadami dotyczącymi przetwarzania danych osobowych). Więcej informacji na temat realizacji obowiązków informacyjnych znajduje się w dalszej części niniejszego kodeksu.

[10] Rejestr udostępnianej dokumentacji medycznej i rejestr wydawanych badań nie powinny być niszczone po digitalizacji, ponieważ na podstawie art. 27 ust. 4 UoPPiRPP wymaga, aby były podpisywane przez osobę udostępniającą dokumentację medyczną. Rejestry można pozostawić jedynie w formie zdigitalizowanej jedynie jeśli mają one zostać załączone do elektronicznej dokumentacji medycznej.

[11] Art. 3 ust. 1 UoDL, Art. 2 ust. 4 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty oraz art. 11 ust. 1 ustawy z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej.

5.2 Jakie obowiązki spoczywają na MPM w odniesieniu do dokumentacji medycznej?

MPM jest zobowiązana do **prowadzenia**, **przechowywania** i **udostępniania** dokumentacji medycznej zgodnie z obowiązującymi przepisami prawa. Jednocześnie musi zapewnić **ochronę wszelkich danych** zawartych w tej dokumentacji, niezależnie od formy jej prowadzenia (papierowej lub elektronicznej).

W tym celu MPM zapewnia, że w dokumentacji medycznej są przechowywane wyłącznie dane niezbędne do udzielania świadczeń zdrowotnych (np. informacje zbierane podczas rozmowy/wywiadu istotne dla lekarza czy pielęgniarki w procesie leczenia) oraz dane dostarczone przez pacjenta.

Kartę informacyjną z leczenia szpitalnego lekarz POZ załącza w oryginale do dokumentacji medycznej. Należy wówczas poinformować pacjenta o tym, że dokument włączony do dokumentacji medycznej nie może być z niej usunięty. Inne dokumenty (np. wyniki badań wykonanych bez zlecenia lekarza) mogą zostać załączone w oryginale za zgodą pacjenta lub w postaci kopii (jeżeli jest to istotne dla przebiegu leczenia).

Ponadto MPM musi zadbać o to, żeby zapisy w dokumentacji medycznej (zarówno papierowej, jak i elektronicznej) były dokonywane wyłącznie przez osoby do tego upoważnione. Dokumentacja medyczna musi być prowadzona w sposób gwarantujący jej **prawidłowość**, **integralność** i **poufność**. To znaczy, że musi być prowadzona w sposób czytelny i zapewniający osobom upoważnionym dostęp do jej elementów bez zbędnej zwłoki[12].

MPM powinna zapewnić dostęp do dokumentacji medycznej wyłącznie osobom upoważnionym przez administratora, w zakresie niezbędnym do wykonywania zadań realizowanych w ramach obowiązków służbowych. Na podstawie obowiązujących przepisów[13] mogą to być osoby wykonujące zawód medyczny (np. lekarze, pielęgniarki/pielęgniarze, położne), a także inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych (np. rejestratorki/rejestratorzy, asystenci medyczni, informatycy/osoby odpowiedzialne za IT).

Ponadto MPM jest zobowiązana udostępniać dokumentację medyczną podmiotom upoważnionym, w sposób wskazany przez wnioskodawcę, o ile posiada techniczną możliwość udostępnienia dokumentacji medycznej we wskazanej przez wnioskodawcę formie. Nie ma obowiązku przekazywania skanów dokumentacji medycznej na nośniku informatycznym czy drogą mailową podmiot, który zastrzegł w regulaminie organizacyjnym, że nie wykonuje skanów dokumentacji medycznej.

---

[12] Rzecznik Praw Pacjenta zauważa w szczególności, że wprowadzanie ograniczeń czasowych (np. umieszczenie w treści regulaminu organizacyjnego MPM informacji, że udostępnienie dokumentacji medycznej pacjenta nastąpi „w terminie do 7 dni") nie jest uzasadnione (źródło: Rzecznik Praw Pacjenta, *Udostępnianie, prowadzenie i przechowywanie dokumentacji medycznej – zagadnienia praktyczne*, https://www.gov.pl/web/rpp/objasnienia-prawne).

[13] Art. 24 ust. 2 pkt 1 i 2 UoPPiRPP.

Przykłady zarządzania dokumentacją prowadzoną w formie papierowej i elektronicznej:

Przykłady	Dokumentacja medyczna w formie papierowej	Dokumentacja medyczna w formie elektronicznej
	Dokumentacja medyczna indywidualna i zbiorcza, deklaracje wyboru	
Dostęp do dokumentacji	Określenie, kto i na jakich zasadach może mieć dostęp do dokumentów (upoważnienia dla pracowników)	Nadanie dostępu upoważnionym pracownikom do pracy w systemie informatycznym i określenie zakresu czynności, jakie dane osoba może wykonywać na danych.
Przechowywanie	Przykład: wypełnione deklaracje wyboru przechowuje się w miejscu udzielania świadczeń, dokumenty zawierające dane osobowe przechowuje się w szafach zamykanych na klucz.	Własna infrastruktura informatyczna (serwery, infrastruktura sieciowa, oprogramowanie, odpowiednie pomieszczenie przystosowane do pracy serwera, zapewnienie opieki i serwisu sprzętu i oprogramowania). Outsourcing – na podstawie umowy powierzenia przetwarzana danych.
Udostępnianie	Przykład: MPM ma obowiązek zapewnienia dostępności deklaracji wyboru pacjentom, których one dotyczą. Dokumentacja medyczna może być udostępniona w sposób określony w UoPPiRPP. MPM tworzy odpowiednie instrukcje dotyczące udostępnienia dokumentacji medycznej w formie papierowej.	MPM udostępnia dokumentację medyczną za pośrednictwem środków komunikacji elektronicznej (e-mail, ePUAP) oraz na informatycznym nośniku danych (płyta CD, pendrive). MPM tworzy odpowiednie instrukcje dotyczące udostępnienia dokumentacji medycznej w formie elektronicznej.
Powierzenie	ADO może powierzyć przetwarzanie danych osobowych wyłącznie na podstawie umowy zawartej z procesorem.	ADO może powierzyć przetwarzanie danych osobowych wyłącznie na podstawie umowy zawartej z procesorem.

Archiwizowanie	ADO określa okresy przechowywania dokumentacji papierowej (uwzględniając przy tym ustawowo określone okresy przechowywania dokumentacji medycznej, o których mowa wyżej w pkt. 4.3 „Jak długo MPM może przechowywać dane osobowe?") oraz odpowiednie warunki jej przechowywania. Jeżeli ADO nie może zapewnić właściwego zabezpieczenia archiwalnej dokumentacji może na podstawie umowy powierzyć przechowywanie takich danych osobowych podmiotowi zewnętrznemu.	ADO określa okresy przechowywania danych w wersji elektronicznej (uwzględniając przy tym ustawowo określone okresy przechowywania dokumentacji medycznej, o których mowa powyżej w pkt. 4.3 „Jak długo MPM może przechowywać dane osobowe?") oraz sposoby jej archiwizowania i zasady bezpieczeństwa nośników danych.
Niszczenie	ADO określa procedury dotyczące niszczenia papierowej dokumentacji w sposób uniemożliwiający jej późniejsze odczytanie, np. przez niszczenie siłami własnymi – za pomocą niszczarki, podpisanie umowy z firmą zewnętrzną zajmującą się profesjonalnym niszczeniem nośników danych.	ADO określa procedury dotyczące niszczenia danych w formie elektronicznej uwzględniające trwałe usunięcie danych lub trwałe zniszczenie nośników danych.

Tabela 5. Przykłady zarządzania dokumentacją prowadzoną w formie papierowej i elektronicznej.

6. Zarządzanie ochroną danych osobowych

Zarządzając przetwarzaniem danych osobowych MPM powinna regularnie kontrolować i doskonalić funkcjonujący w przedsiębiorstwie system ochrony danych osobowych, który można podzielić na trzy podstawowe elementy:

1) bezpieczeństwo,
2) dokumentacja,
3) zasoby ludzkie.

6.1 W jaki sposób MPM powinna zarządzać bezpieczeństwem danych osobowych?

W celu sprawowania kontroli nad danymi osobowymi przetwarzanymi w MPM, należy wprowadzić procedury umożliwiające monitorowanie wszelkich czynności wykonywanych na danych.

Kontrola przetwarzania danych osobowych w MPM polega przede wszystkim na:

a) inwentaryzacji zasobów – MPM ustala jakie dane osobowe i w jaki sposób przetwarza, np. dane osobowe pacjentów zbierane w deklaracjach wyboru, dane utrwalane w dokumentacji medycznej – w wersji papierowej i elektronicznej; dane przechowywane w szafach kartotecznych, zamykanych na klucz; na serwerze, w chmurze, na zewnętrznych nośnikach danych;

b) określeniu, jakie obowiązki, w związku z przetwarzaniem powyższych danych, nakłada na administratora danych osobowych RODO;

c) analizie ryzyka;

d) prowadzeniu audytów ochrony danych osobowych, podczas których sprawdzany jest niezbędny zakres zbieranych informacji, adekwatność i stosowanie procedur, środki ochrony technicznej;

e) przeglądzie upoważnień dostępu do danych osobowych (w szczególności upoważnień do przetwarzania danych osobowych w formie papierowej lub elektronicznej, nadanych osobom zatrudnionym w MPM w związku z realizacją ich obowiązków służbowych);

f) przeglądzie uprawnień dostępu do danych osobowych (w szczególności zakresu uprawnień osób zatrudnionych w MPM do określonych baz danych lub modułów w wykorzystywanych przez MPM aplikacjach, programach bądź systemach informatycznych).

MPM musi pamiętać o cyklicznym przeprowadzaniu analizy ryzyka, audytów bezpieczeństwa oraz przeglądów upoważnień i uprawnień. Zalecane jest, aby terminy ponownych audytów/analiz zostały zaplanowane z góry.

Organizując zarządzanie bezpieczeństwem danych osobowych MPM powinna określić, jakie dane osobowe są niezbędne do realizacji konkretnego celu (np. dane osobowe pacjentów podawane w deklaracji wyboru, dane osobowe zbierane w celu udzielenia świadczenia zdrowotnego) oraz w jakiej formie je przetwarza (papierowo/elektronicznie). MPM określa również, kto i na jakich zasadach musi mieć dostęp do tych danych (lekarze, pielęgniarki, rejestratorski, pracownicy statystyki medycznej).

6.2 Jak należy przeprowadzić szacowanie ryzyka?

MPM cyklicznie przeprowadza **analizę ryzyka** oraz – jeżeli wynika to z analizy – **ocenę skutków. Analizując ryzyko**, MPM identyfikuje zagrożenia związane z przetwarzaniem danych osobowych oraz określa ich wartość.

Ryzyko wzrasta, gdy:

- przetwarzane są dane osobowe o stanie zdrowia;
- dane przechowywane są w sposób dostępny dla osób nieupoważnionych (np. wyniki badań leżące na kontuarze otwartej recepcji);
- dokumentacja medyczna przechowywana jest w sposób narażający ją na zniszczenie (np. w piwnicy pod rurami kanalizacyjnymi).

Ryzyko maleje, gdy:

- przetwarzane są dane osobowe zwykłe;
- dokumentacja przechowywana jest w zamkniętych szafach kartotecznych;
- archiwum z dokumentacją medyczną zapewnia odpowiednie warunki jej przechowywania (temperatura, wilgoć, kontrola dostępu personelu MPM).

MPM musi ocenić, jakie jest ryzyko naruszenia praw lub wolności osób, których dane przetwarza oraz jakie ryzyko dla placówki niesie za sobą przetwarzania tych danych.

O tym, czym jest ryzyko dla praw lub wolności, mówi motyw 85 RODO: *Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.*

6.2.1 Analiza ryzyka

Aby dokonać oceny, o której mowa powyżej, MPM powinna przeprowadzić szczegółową analizę czynności przetwarzania prowadzonych w placówce (np. rejestracja pacjentów) i na tej podstawie ocenić ryzyko, na jakie mogą być narażone dane osobowe. MPM musi określić, jakie są możliwe rodzaje ryzyka utraty, zniszczenia, nieuprawnionego udostępnienia danych osobowych, jakie skutki dane ryzyko niesie dla osoby fizycznej, której dane dotyczą.

Ponadto MPM musi określić prawdopodobieństwo wystąpienia poszczególnych rodzajów ryzyka i określić sposób postępowania w celu ich eliminacji lub minimalizacji.

Każdy proces (czynność przetwarzania danych) zachodzący w MPM należy podzielić na trzy obszary:

- **ludzie**, którzy przetwarzają dane osobowe;
- **środowisko informatyczne**, gdzie przetwarza się dane osobowe oraz fizyczne nośniki danych (jak komputery, dyski zewnętrzne);
- **przepływ danych** osobowych w danym procesie.

Zdefiniowanie osób biorących udział w danym procesie jest niezwykle ważne z punktu widzenia ochrony danych osobowych oraz ryzyka związanego z ich przetwarzaniem.
Chodzi oczywiście o wskazanie stanowisk służbowych biorących udział w procesie, a nie wskazywanie konkretnych osób z imienia i nazwiska. Precyzyjne określenie środowisk informatycznych oraz fizycznych nośników danych wykorzystywanych w procesie pozwala z kolei ocenić ryzyko z punktu widzenia zabezpieczeń, jakie stosuje MPM by chronić należycie dane osobowe. Kluczową kwestią w procesie oceny ryzyka jest natomiast dokładny opis przepływu danych osobowych w danym procesie. Chodzi o to, aby MPM miała pełną jasność co do tego, kto, kiedy i w jakim celu przetwarza dane osobowe oraz jaką drogą weszła w ich posiadanie. Analizujemy w tym kroku po kolei: jakie dane przetwarzamy (mapowanie), niezbędność i proporcjonalność przetwarzania (podstawy prawne) oraz procedury (np. sposób realizowania praw pacjentów).

Po takiej analizie MPM musi określić, jakie są możliwe zagrożenia związane z przetwarzaniem danych osobowych w poszczególnych procesach, które mogą powodować ryzyko **utraty, zniszczenia i nieuprawnionego udostępnienia** danych osobowych. Dla każdego z tych zagrożeń należy ocenić **prawdopodobieństwo** wystąpienia oraz jakie **konsekwencje** dla praw lub wolności osób może mieć naruszenie ochrony danych osobowych. Po ocenie prawdopodobieństwa zdarzenia oraz możliwych konsekwencji dla osoby, której dane dotyczą, należy ocenić ryzyko w skali: duże ryzyko dla praw lub wolności pacjenta (np. uniemożliwienie dalszego właściwego leczenia z powodu utraty dostępności do bazy danych – MPM może wtedy nie móc określić, jakie leki i w jakiej dawce należy podać pacjentowi, co zagraża jego zdrowiu i życiu), średnie ryzyko dla praw lub wolności pacjenta (przekazanie wyników badania krwi niewłaściwemu pacjentowi) lub małe ryzyko dla praw lub wolności pacjenta (zgubienie zaszyfrowanego pendrive'a z wynikami badań).

Ocena ryzyka dla praw lub wolności osób, których dane dotyczą, jest więc wypadkową dwóch czynników: prawdopodobieństwa wystąpienia zagrożenia (kradzież dokumentów, pożar w budynku, wyciek danych w postaci przekazania wyników badań niewłaściwemu pacjentowi) oraz możliwych konsekwencji dla osoby, której dane dotyczą. Takimi konsekwencjami mogą być np. wykonanie niewłaściwych świadczeń medycznych, utrata dobrej opinii w lokalnej społeczności, wyższa składka ubezpieczeniowa, rozpowszechnianie plotek na temat danej osoby. Jest to, co naturalne, proces ciągły i wymagający poprawy w zakresie mechanizmów kontrolnych w kontekście nowo odkrytych zagrożeń, których wcześniej nie zidentyfikowaliśmy.

Po przeprowadzeniu tej analizy, koniecznym jest zastosowanie mechanizmów kontrolnych. Mechanizmy kontrolne stanowią środki techniczne i organizacyjne, o których mowa w RODO. Do poszczególnych procesów należy stosować adekwatne mechanizmy kontrolne. I tak:

- w odniesieniu do osób mechanizmem kontrolnym może być nadanie upoważnień do dostępu do danych. Rolę środka organizacyjnego będzie też pełnił regulamin wewnętrzny dotyczący zasad zachowywania się w budynku podmiotu leczniczego oraz podział zadań służbowych;
- w odniesieniu do środowiska informatycznego oraz fizycznych nośników danych należy określić takie mechanizmy kontrolne jak: logiczne zabezpieczenia systemów, np. hasła do dysków, systemów, urządzeń typu pendrive, poszczególnych plików z danymi osobowymi pacjentów, oprogramowanie antywirusowe, zapory sieciowe itp. oraz zabezpieczenia fizyczne, np. kłódki do szafek, szyfry do sejfów, klucze do pomieszczeń i schowków, karty dostępu, systemy alarmowe, gaśnice, żaluzje antywłamaniowe;
- w odniesieniu do przepływu danych należy ocenić, czy w danym procesie nie występuje zbyt duża liczba osób bądź czy dane osobowe nie są przekazywane wewnątrz MPM bez uzasadnionej potrzeby. Każdorazowo należy wyznaczyć najniższą z możliwych liczbę osób uczestniczących w danym procesie przy jednoczesnej minimalizacji przetwarzanych danych osobowych.

Przykłady zagrożeń i zabezpieczeń:

Zapewnienie właściwej ochrony danych osobowych wymaga ustalenia, na jakie zagrożenia mogą być narażone dane osobowe pacjentów przetwarzane w MPM.

Ochrona przed...	**Przykłady zagrożeń w zależności od formy przetwarzania danych**		**Zabezpieczenie**	
	Dane osobowe w formie papierowej	**Dane osobowe w formie elektronicznej**	**Organizacyjne**	**Techniczne**
Zniszczeniem	Pożar, zalanie.	Wirus.	Zabezpieczenie systemu informatycznego poprzez zainstalowanie antywirusa oraz tworzenie kopii zapasowych. Stworzenie instrukcji dotyczącej postępowania na wypadek zagrożenia.	Fizyczne zabezpieczenie dokumentacji papierowej poprzez umieszczenie jej w metalowych szafach kartotecznych z dala od rur wodociągowych, umieszczenie dokumentacji na podwyższeniu – nie bezpośrednio na podłodze.

Utratą	Kradzież.	Kradzież nośnika danych, atak hackerski.	Kontrola dostępu pracowników.	Zamki, alarmy, rolety, drzwi antywłamaniowe, firewalle, antywirusy, back-upy.
Udostępnieniem osobie nieupoważnionej	Pomyłka przy wydawaniu dokumentacji medycznej.	Przesłanie danych na niewłaściwy adres e-mail.	Zasady udostępniania dokumentacji medycznej.	Odpowiednie poziomy dostępu w systemach IT dla personelu MPM.
Nieuprawnioną modyfikacją	Fałszowanie zapisów w dokumentacji medycznej.	Wprowadzanie zatwierdzonych zmian w dokumentacji elektronicznej bez odnotowania w systemie danej operacji.	Zasady postępowania dokumentacji medycznej.	Odpowiednie poziomy dostępu w systemach IT dla personelu MPM.
Nieuprawnionym dostępem	Personel sprzątający mający dostęp do dokumentacji medycznej.	Rejestratorki medyczne mające dostęp do wszelkich zapisów prowadzonych w elektronicznej dokumentacji medycznej.	Zasada czystego biurka, szafki zamykane na klusze, nadzór nad osobami sprzątającymi.	Wylogowywanie się z systemów i aplikacji, stosowanie wygaszaczy ekranów, folie prywatyzujące.

Tabela 6. Przykłady zagrożeń dla danych osobowych i sposób zapobiegania tym zagrożeniom.

6.2.2. Ocena skutków dla ochrony danych

Jeżeli przeprowadzona przez MPM analiza ryzyka uwzględniająca charakter, zakres, kontekst i cel przetwarzania) wykaże, że dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, konieczne będzie dokonanie oceny skutków dla ochrony danych osobowych.

Jest to proces bardzo podobny do szacowania ryzyka, musi jednak uwzględniać również propozycje, jakie środki organizacyjne i techniczne należy wdrożyć, aby poziom ryzyka dla danego procesu obniżyć z poziomu wysokiego do średniego lub małego[14].

[14] Więcej informacji na temat oceny skutków dla ochrony danych znajduje się w Wytycznych WP248 Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, dostępnych na stronie Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/pl/10/9.

Poniżej przedstawiono narzędzia i dokumenty, które MPM powinna wziąć pod uwagę przy dokonywaniu oceny skutków dla ochrony danych.

Organ	Nazwa / tytuł
Grupa Robocza Art. 29	Wytyczne dotyczące oceny skutków dla ochrony danych (*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*)[15]
Prezes UODO	Wykaz rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[16]
CNIL[17]	PIA software (narzędzie wspierające w dokonywaniu oceny skutków, dostępne m.in. w polskiej wersji językowej)[18]

Tabela 7. Zestawienie narzędzi i dokumentów, stosowanych przy dokonywaniu oceny skutków dla ochrony danych.

Jeśli MPM nie będzie jednak w stanie zminimalizować ryzyka, konieczna będzie konsultacja z Prezesem Urzędu Ochrony Danych Osobowych[19].

Podstawy prawne RODO:

Artykuł 24 - Obowiązki administratora

1. *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.*
2. *Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.*
3. *Stosowanie zatwierdzonych kodeksów postępowania, o których mowa wart. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa wart. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.*

[15] Polskie tłumaczenie: https://uodo.gov.pl/pl/10/9. Wersja angielskojęzyczna jest dostępna pod adresem https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

[16] Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M.P.2019.666): https://monitorpolski.gov.pl/MP/2019/666.

[17] Fr. *Commission nationale de l'informatique et des libertés* (Narodowa Komisja Ochrony Informacji i Wolności) – francuski organ nadzorczy.

[18] https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

[19] Więcej na temat uprzednich konsultacji na stronie: https://uodo.gov.pl/pl/127.

Artykuł 35 - Ocena skutków dla ochrony danych

1. *Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.*
2. *Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.*
3. *Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:*
   a) *systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;*
   b) *przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10; lub*
   c) *systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.*
4. *Organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych na mocy ust. 1. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych, o której mowa w art. 68.*
5. *Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy przekazuje te wykazy Europejskiej Radzie Ochrony Danych.*
6. *Jeżeli wykazy, o których mowa w ust. 4 i 5, obejmują czynności przetwarzania związane z oferowaniem towarów lub usług osobom, których dane dotyczą, lub z monitorowaniem ich zachowania w kilku państwach członkowskich lub mogące znacznie wpłynąć na swobodny przepływ danych osobowych w Unii, przed przyjęciem takich wykazów właściwy organ nadzorczy stosuje mechanizm spójności, o którym mowa w art. 63.*
7. *Ocena zawiera co najmniej:*
   a) *systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;*
   b) *ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;*

c) *ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz*

d) *środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.*

8. *Oceniając - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania, o których mowa w art. 40.*

9. *W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania.*

10. *Ust. 1-7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej - chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.*

11. *W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.*

6.3 Jakie środki techniczne i organizacyjne (mechanizmy kontrolne) MPM powinna wdrożyć?

Po przeprowadzeniu analizy administrator będzie mógł zadecydować o wprowadzeniu zabezpieczeń adekwatnych do poziomu ryzyka naruszenia ochrony danych osobowych. Zabezpieczenia możemy podzielić na:

- **zabezpieczenia techniczne dostępu do pomieszczeń i budynku oraz bezpiecznego przechowywania danych osobowych.** Do tych zabezpieczeń zaliczają się w szczególności**:** instalacja przeciwpożarowa, instalacja alarmowa, zabezpieczenie okien (zarówno przed dostępem osób niepowołanych, np. rolety antywłamaniowe, jak i przed zaglądaniem z zewnątrz, np. folie mleczne, żaluzje, rolety), drzwi zamykane na klucz (np. gałko-klamki) lub wyposażone w system kontroli dostępu (np. karty magnetyczne), szafki zamykane na klucz, odrębne kluczniki do przechowywania kluczy do szaf i pomieszczeń z dokumentami, odpowiednie ustawienie monitorów lub wykorzystanie folii prywatyzujących;

- **zabezpieczenia organizacyjne, które regulują zasady organizacji pracy oraz przetwarzania danych osobowych.** Do tych zabezpieczeń należą w szczególności: procedury i instrukcje, m.in. nadawania upoważnień i uprawnień, korzystania z poczty elektronicznej oraz sprzętu służbowego, potwierdzania tożsamości pacjentów i innych osób zgłaszających się do placówki medycznej, rejestrowania pacjentów, udostępniania dokumentacji medycznej, reagowania w sytuacji stwierdzenia wystąpienia incydentu bezpieczeństwa, udzielania odpowiedzi na wnioski podmiotów danych dotyczące realizacji ich praw wynikających z RODO, zarządzania kluczami do pomieszczeń – tzw. polityka kluczy, archiwizowania dokumentów, niszczenia dokumentów.

Odrębnym zagadnieniem niezmiernie istotnym w czasie informatyzacji placówek medycznych jest zapewnienie optymalnego poziomu bezpieczeństwa informatycznego. Każda MPM musi zadbać o to, by do przetwarzania danych osobowych używany był odpowiedni sprzęt oraz programy. Trzeba również wdrożyć odpowiednie procedury informatyczne, m.in. dotyczące:

- haseł, np. wymuszanie na użytkownikach, żeby hasło miało określoną długość oraz żeby było regularnie zmieniane;
- korzystania z poczty elektronicznej, np. zasada ograniczonego zaufania w odniesieniu do korespondencji i załączników od nieznanych nadawców, zasada zakazu wykorzystywania poczty służbowej do celów prywatnych;
- użytkowania sprzętu informatycznego, np. zakaz wykorzystywania sprzętu służbowego do celów prywatnych;
- wykorzystywania aplikacji służących do przetwarzania danych osobowych, np. pracy wyłącznie na swoim koncie, wylogowywania się z aplikacji w chwili czasowego opuszczenia stanowiska pracy;
- zabezpieczenia sprzętu przed dostępem osób nieupoważnionych oraz przed kradzieżą, np. wykorzystanie linki zabezpieczającej do laptopów, montaż kłódek na obudowie komputera stacjonarnego, przechowywanie komputerów stacjonarnych w specjalnych szafkach z otworami wentylacyjnymi.

MPM przetwarza dane osobowe w formie elektronicznej. Podczas analizy ryzyka stwierdzono, że największym zagrożeniem dla danych osobowych pacjentów może być kradzież dokumentacji papierowej oraz komputera, który pełni funkcję serwera. W związku z powyższym zdecydowano o wprowadzeniu następujących zabezpieczeń:

- montaż rolet antywłamaniowych w oknach archiwum;
- montaż instalacji alarmowej oraz rozpoczęcie współpracy z firmą ochroniarską;
- formalne uregulowanie, kto ma dostęp do kodu aktywującego i dezaktywującego alarm;
- ustalenie sposobu postępowania w chwili zakończenia współpracy z osobami znającymi kod do alarmu;

- wyposażenie placówki w gaśnice, w tym specjalną gaśnicę dedykowaną do gaszenia czułych urządzeń elektronicznych i elektrycznych, która nie zostawia zanieczyszczeń po środku gaśniczym;
- osobne przechowywanie komputera, który pełni rolę serwera i ograniczenie dostępu do pomieszczenia, gdzie się znajduje;
- montaż gałko-klamek w drzwiach do gabinetów oraz rejestracji;
- przechowywanie kluczy do szafek i pomieszczeń w odrębnych, szyfrowanych klucznikach oraz wdrożenie zabezpieczeń organizacyjnych uregulowanych w polityce kluczy (w tym określenie, kto zna kod do kluczników i jaki jest sposób postępowania w chwili zakończenia współpracy z daną osobą);
- nadawanie upoważnień wszystkim osobom zatrudnionym w MPM, które mają dostęp do danych osobowych;
- szkolenie personelu;
- prowadzenie dokumentacji określającej zasady ochrony danych osobowych (np. udostępnianie dokumentacji medycznej, korzystanie z poczty elektronicznej, niszczenie dokumentacji).

6.4 Co oznaczają zasady privacy by design i privacy by default?

W wypadku wprowadzania nowego systemu informatycznego lub aplikacji, już **na etapie projektowania** takiego rozwiązania, administrator musi **uwzględnić ochronę danych osobowych,** czyli ustalić, jakie środki techniczne i organizacyjne będzie musiał zapewnić w celu ochrony tych danych.

Przykład 1: Ochrona danych osobowych w fazie projektowania.

Podczas projektowania systemu internetowej rejestracji pacjentów należy pamiętać o dostosowaniu odpowiednich zabezpieczeń technicznych i organizacyjnych, tak żeby już na etapie planowania prac związanych z wdrożeniem nowego systemu uwzględniano koszt wdrożenia, zakres niezbędnych danych, cele przetwarzania oraz ryzyko naruszenia praw lub wolności osoby fizycznej.

Jeszcze przed rozpoczęciem wdrożenia nowego systemu należy wziąć pod uwagę, czy działanie będzie zgodne z przepisami prawa i uwzględnić środki niezbędne do zapewnienia tego bezpieczeństwa.

Przykład 2: Ochrona danych osobowych w fazie projektowania.

W sytuacji, kiedy MPM zdecyduje się na rozbudowę przychodni, powinna uwzględnić aspekt zapewnienia pacjentom prywatności i odpowiedzieć sobie na kilka kluczowych pytań: jak powinna wyglądać rejestracja, aby zachować poufność danych przekazywanych przez pacjentów, jak powinny wyglądać nowe gabinety (gdzie postawić kozetkę, jak będzie ustawiony komputer, czy i ile zmieści się tam szaf kartotekowych)?

Przykład 3: Ochrona danych osobowych w fazie projektowania.

Decydując się na dołączenie do zewnętrznej platformy pozwalającej na rejestrowanie pacjentów, administrator powinien zadbać o podpisanie odpowiedniej umowy z właścicielami systemu, gdzie zamieszczone zostaną zapisy dotyczące np. **pseudonimizacji** danych wprowadzanych podczas rejestracji, żeby dostęp do danych był możliwy wyłącznie dla pacjenta oraz osób upoważnionych w MPM.

Przykład 4: Domyślna ochrona danych osobowych.

System internetowej rejestracji pacjenta, wprowadzany w placówce, może domyślnie przetwarzać tylko te dane, które są niezbędne do osiągnięcia konkretnego celu.

Podstawy prawne RODO:

Artykuł 25 - Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania -wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.*
2. *Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.*
3. *Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.*

Artykuł 32 - Bezpieczeństwo przetwarzania

1. *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:*

   a) *pseudonimizację i szyfrowanie danych osobowych;*

b) *zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*

c) *zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*

d) *regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

2. *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*

3. *Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.*

4. *Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.*

6.5 Jaką dokumentację dotyczącą ochrony danych osobowych powinna prowadzić MPM?

MPM powinna stworzyć **odpowiednią dokumentację** ochrony danych osobowych, która będzie zawierała konkretne instrukcje dotyczące przetwarzania danych osobowych na każdym etapie ich obiegu. Na powyższą dokumentację powinny składać się przede wszystkim **rejestr czynności przetwarzania**, procedury związane z **naruszeniem ochrony danych osobowych**, które uwzględniają sposób dokumentowania naruszeń i zgłaszania ich do Prezesa UODO oraz powiadomienia osoby fizycznej.

Dokumentację dotyczącą ochrony danych osobowych w MPM należy prowadzić w sposób, który umożliwi administratorowi wykazanie przestrzegania przepisów RODO.

Obowiązkiem MPM, wynikającym z przepisów RODO, jest **prowadzenie rejestru czynności przetwarzania danych osobowych** oraz **dokumentowanie naruszeń ochrony danych osobowych**.

Prowadzenie rejestru czynności pozwala na systematyzację wykonywanych działań na danych oraz całościowe spojrzenie na wykonywane operacje przetwarzania danych osobowych. Dla Prezesa UODO rejestr jest z kolei potrzebny do monitorowania procesów przetwarzania danych – Prezes UODO prosząc o rejestr dostaje informacje o prowadzonym przez administratora przetwarzaniu – w sposób czytelny i uproszczony, umożliwiający dokonanie ich szybkiego przeglądu i wstępnej oceny.

RODO nie definiuje pojęcia „czynności przetwarzania". Zgodnie z interpretacją Prezesa UODO, czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane[20]. Przykładem tak rozumianej czynności jest np. udostępnianie dokumentacji medycznej – zestaw kilku operacji na danych osobowych (np. sprawdzanie upoważnienia wnioskodawcy do otrzymania dokumentacji, wydanie dokumentacji, etc.), których nie umieszczamy odrębnie w rejestrze, ale grupujemy w jedną czynność podejmowaną w celu udostępnienia dokumentacji.

Przykładowe opisanie czynności w rejestrze może mieć miejsce jak poniżej:

Kategorie przetwarzanych danych	**Zakładanie dokumentacji medycznej**	**Dokumentowanie świadczeń opieki zdrowotnej**	**Udostępnianie dokumentacji medycznej pacjentowi, przedstawicielowi ustawowemu pacjenta lub osobie upoważnionej przez pacjenta**
Cele przetwarzania	Identyfikacja pacjenta i jego ogólnego stanu zdrowia (art. 24 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta).	Pozyskanie kompleksowej informacji o stanie zdrowia pacjenta, udzielonych mu świadczeniach oraz ustalenie dalszego postępowania diagnostyczno-terapeutycznego (art. 25 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta).	Realizowanie uprawnień w zakresie udostępniania dokumentacji medycznej (art. 26 ust. 3 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta).
Opis kategorii osób, których dane dotyczą	Pacjenci Przedstawiciele ustawowi pacjentów Osoby upoważnione przez pacjentów do dostępu do dokumentacji medycznej oraz informacji o stanie zdrowia i udzielonych świadczeniach	Pacjenci Przedstawiciele ustawowi pacjentów Opiekunowie faktyczni pacjentów	Pacjenci Przedstawiciele ustawowi pacjentów Osoby upoważnione przez pacjentów do dostępu do dokumentacji medycznej oraz informacji o stanie zdrowia i udzielonych świadczeniach

[20] Więcej informacji na ten temat dostępnych jest we *Wskazówkach i wyjaśnieniach dotyczących obowiązku z art. 30 ust. 1 i 2 RODO*, dostępnych na stronie Prezesa UODO: https://uodo.gov.pl/pl/123/214

Opis kategorii danych osobowych	Oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości: 1) nazwisko i imię (imiona), 2) datę urodzenia, 3) oznaczenie płci, 4) adres miejsca zamieszkania, 5) 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 oraz kraj wydania; 6) jeżeli pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody - nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania; 7) informacja o posiadanych przez pacjenta uprawnieniach szczególnych.	Dane o stanie zdrowia i udzielonych świadczeniach.	Dane identyfikacyjne. Dane o stanie zdrowia i udzielonych świadczeniach.
Odbiorcy lub kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych (dla większej przejrzystości	NFZ oraz inne organy uprawnione na mocy przepisów prawa. Dostawca oprogramowania IT dla placówek medycznych.	NFZ oraz inne organy uprawnione na mocy przepisów prawa. Dostawca oprogramowania IT dla placówek medycznych. Dostawca usług telemedycznych.	Podmioty uprawnione na podstawie przepisów prawa. Dostawca oprogramowania IT dla placówek medycznych.

rekomendujemy wskazanie konkretnych odbiorców z nazwy)			
Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń	n/d	USA. Standardowe klauzule umowne.	n/d
Planowane terminy usunięcia poszczególnych kategorii danych	20 lat od końca roku kalendarzowego, w którym zostanie dokonany ostatni wpis.	20 lat od końca roku kalendarzowego, w którym zostanie dokonany ostatni wpis.	20 lat od końca roku kalendarzowego, w którym zostanie dokonany ostatni wpis.
Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenia, wskazane w treści Polityki bezpieczeństwa i załączników do niej.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenia, wskazane w treści Polityki bezpieczeństwa i załączników do niej.	Nadawanie upoważnień dla osób zatrudnionych, mających dostęp do danych osobowych. Zapoznanie osób zatrudnionych z zasadami ochrony danych osobowych. Podpisanie umów powierzenia z zewnętrznymi podmiotami, mającymi dostęp do danych osobowych. Zabezpieczenia, wskazane w treści Polityki bezpieczeństwa i załączników do niej.

Tabela 8. Przykładowy rejestr czynności przetwarzania.

Ponadto MPM zobowiązana jest do wykazania przestrzegania zasad określonych w RODO. Żeby to zrobić, MPM musi stworzyć dokumentację odpowiednią do potrzeb ochrony danych osobowych.

Dokumentacja prowadzona przez MPM, w zakresie ochrony danych osobowych, powinna uwzględniać:

- procedury związane z analizą ryzyka i ewentualną koniecznością przeprowadzenia oceny skutków;
- ewidencję naruszeń bezpieczeństwa danych;
- instrukcje dotyczące: nadawania upoważnień osobom zaangażowanym w przetwarzanie danych osobowych w placówce; zbierania danych osobowych (w deklaracjach, dokumentacji medycznej, zbieranych podczas osobistego kontaktu z pacjentem, od osób trzecich i droga elektroniczną); spełniania obowiązków informacyjnych; powierzenia danych osobowych (jakie warunki ma spełnić podmiot, z którym MPM podpisuje umowę powierzenia danych osobowych); udostępnienia danych osobowych (zasady udostępniania); niszczenia danych osobowych, zgłaszania naruszeń UODO i informowania osób fizycznych o naruszeniach; sposobu spełnienia obowiązku informacyjnego.

Podstawy prawne RODO:

Artykuł 30 - Rejestrowanie czynności przetwarzania

1. *Każdy administrator oraz - gdy ma to zastosowanie - przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje:*
   a) *imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;*
   b) *cele przetwarzania;*
   c) *opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;*
   d) *kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;*
   e) *gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;*
   f) *jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;*
   g) *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.*
2. *Każdy podmiot przetwarzający oraz - gdy ma to zastosowanie - przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności*

przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) *imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;*

b) *kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;*

c) *gdy ma to zastosowanie -przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;*

d) *jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.*

3. *Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.*

4. *Administrator lub podmiot przetwarzający oraz - gdy ma to zastosowanie - przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego.*

5. *Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.*

6.6 W jaki sposób MPM powinna zarządzać zasobami ludzkimi w procesie przetwarzania danych osobowych?

MPM powinna przeszkolić i upoważnić personel biorący udział w procesie przetwarzania danych osobowych (pisemne upoważnienia dla pracowników, które określają zakres ich dostępu do danych, szkolenia dostosowane do specyfiki danego stanowiska pracy) oraz – w razie konieczności – wyznaczyć **inspektora ochrony danych**.

MPM musi zadbać o to, żeby do przetwarzania danych osobowych miały dostęp wyłącznie osoby upoważnione przez ADO. Na podstawie obowiązujących przepisów mogą to być osoby wykonujące zawód medyczny (np. lekarze, pielęgniarki), jak również inne osoby wykonujące czynności pomocnicze przy udzielaniu świadczeń zdrowotnych (np. rejestratorki, informatycy).

Upoważnienie musi konkretnie określać, kto, do jakich danych i w jakim zakresie będzie miał dostęp. Ponadto do zadań MPM należy zapoznanie upoważnionych osób z zasadami dotyczącymi ochrony danych osobowych oraz regularne podnoszenie świadomości w tym zakresie osób zatrudnionych w placówce.

6.7 Czy MPM musi powołać inspektora ochrony danych (IOD)?

Zgodnie z art. 37 ust. 1 RODO powołanie IOD będzie **obowiązkowe między innymi** w przypadku, gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

Ta okoliczność jest dość ocenna. W tej sytuacji wyznaczenie inspektora ochrony danych będzie bowiem konieczne dla administratorów, których główna działalność polega na przetwarzaniu wrażliwych danych osobowych. Jak czytamy w Wytycznych WP 243 Grupy Roboczej Art. 29[21], główna działalność oznacza zasadnicze, a nie poboczne działanie. Dla przykładu: główną działalnością placówek medycznych będzie udzielanie świadczeń opieki zdrowotnej. *„Natomiast prowadzenie efektywnej opieki medycznej nie byłoby możliwe bez przetwarzania danych medycznych, jak np. historii choroby pacjenta. W związku z tym działalność polegająca na przetwarzaniu historii choroby pacjenta również powinna zostać zaklasyfikowana jako działalność główna*".

Pojęcie dużej skali przetwarzania jest z kolei jeszcze bardziej nieostre. Zaleca się uwzględnianie następujących czynników przy określaniu, czy przetwarzanie następuje na „dużą skalę":

- liczba osób, których dane dotyczą – konkretna liczba osób albo procent określonej grupy społeczeństwa, np. kiedy dana placówka medyczna przetwarza dane osobowe niemal wszystkich mieszkańców małej gminy;
- zakres przetwarzanych danych osobowych – ten w przypadku placówek medycznych będzie zawsze szeroki i będzie uwzględniał dane wrażliwe;
- okres, przez jaki dane są przetwarzane – istotną kwestią będzie zgodny z przepisami, maksymalny czas przechowywania dokumentacji medycznej;
- zakres geograficzny przetwarzania danych osobowych.

Biorąc pod uwagę powyższe uwarunkowania wydaje się, że MPM powinna wyznaczyć inspektora ochrony danych. Nie będzie to jednak dotyczyć sytuacji, kiedy przetwarzanie danych pacjentów – klientów, dokonywane będzie przez pojedynczego lekarza prowadzącego indywidualny gabinet lekarski i przetwarzającego dane osobowe niewielkiej grupy pacjentów.

Przykład przetwarzania na dużą skalę:
Dane osobowe pacjentów przetwarzane przez szpital.

Przykład przetwarzania niemieszczącego się w definicji „dużej skali":
Dane osobowe pacjentów przetwarzane przez pojedynczego lekarza, w ramach wykonywania działalności leczniczej.

[21] Wytyczne WP 243 Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych ('DPO'), s. 8: https://uodo.gov.pl/pl/10/7.

6.8 W jaki sposób należy powiadomić Prezesa UODO o wyznaczeniu IOD?

Zgodnie z RODO, po wyznaczeniu IOD, MPM musi powiadomić o tym Prezesa Urzędu Ochrony Danych Osobowych oraz podać dane kontaktowe IOD. U.o.d.o. przesądza również sposób zawiadamiania organu nadzorczego o danych kontaktowych inspektora wskazując, że „zawiadomienia sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP". W praktyce oznacza to, że jedyną dopuszczalną formą zgłoszenia IOD jest forma elektroniczna. Zawiadomienie należy przesłać, wykorzystując w tym celu jedną z dostępnych usług znajdujących się na stronie portalu biznes.gov.pl.

W zawiadomieniu należy podać imię, nazwisko oraz adres e-mail lub numer telefonu IOD. Formularz należy wysłać najpóźniej 14 dni od dnia wyznaczenia IOD (np. od dnia podjęcia uchwały/zarządzenia kierownictwa MPM wyznaczającego konkretną osobę fizyczną na funkcję IOD). Dodatkowo, jeśli MPM prowadzi swoją stronę internetową, niezwłocznie po wyznaczeniu IOD należy umieścić na niej imię, nazwisko oraz adres e-mail lub numer telefonu IOD. Najlepszą praktyką w tym zakresie jest umieszczenie tych informacji w zakładce „Kontakt", bądź też stworzenie dedykowanej zakładki poświęconej ochronie danych osobowych (np. o nazwie „RODO"). Jeśli natomiast MPM nie prowadzi własnej strony internetowej, powyższe informacje o IOD należy przekazać w sposób ogólnie dostępny w miejscu prowadzenia działalności (np. w gablotach lub na tablicy ogłoszeń znajdującej się w pobliżu rejestracji).

6.9 Kto może zostać IOD?

Inspektorem ochrony danych może być pracownik bądź współpracownik MPM, który zostanie wyznaczony do sprawowania tej funkcji. Nie ma jednak przeszkód, aby funkcję IOD pełniła osoba spoza placówki, zatrudniona na podstawie umowy o świadczenie usług, np. osoba wskazana przez zewnętrzny podmiot specjalizujący się w obsłudze MPM w zakresie ochrony danych osobowych. Jeśli MPM zdecyduje się na wyznaczenie IOD spośród swojego personelu musi pamiętać, żeby nie była to osoba, której dotychczasowe zadania i obowiązki będą powodować konflikt interesów z nowo pełnioną funkcją (np. kiedy IOD miałaby stać się osoba odpowiedzialna za IT w placówce, która z jednej strony decydowałaby o stosowanych zabezpieczeniach, a z drugiej – jako IOD – oceniałaby je pod kątem zgodności z RODO). Ponadto IOD powinien podlegać jedynie kierownictwu MPM.

Osoba pełniąca funkcję IOD powinna cechować się odpowiednią wiedzą i umiejętnościami – najlepiej, by miała wiedzę nie tylko z zakresu ochrony danych osobowych, ale przede wszystkim z obszaru przepisów sektorowych, regulujących funkcjonowanie MPM.

Wśród wielu zadań IOD, RODO wylicza m.in. monitorowanie przestrzegania przez MPM przepisów o ochronie danych osobowych (w szczególności RODO) i wewnętrznych regulacji MPM dotyczących bezpieczeństwa informacji, współpracę z Prezesem UODO oraz pełnienie funkcji punktu kontaktowego dla pacjentów w sprawach związanych z ochroną danych. Aby należycie realizować te zadania, IOD powinien być niezwłocznie angażowany we wszystkie sprawy związane z działalnością MPM, które mogą mieć wpływ na ochronę danych

osobowych pacjentów i pracowników placówki.[22] Wszystko to ma na celu zapewnienie niezależności IOD w wykonywaniu jego zadań. Niezależność, która oznacza zobowiązanie kierownictwa MPM do nieprzekazywania IOD instrukcji, odnoszących się do sposobu jego działania, jak również wiążących poleceń, nakazujących zajęcie określonego stanowiska w danej sprawie bądź przyjęcie określonego stanowiska.

Podstawy prawne RODO:

Artykuł 37 - Wyznaczenie inspektora ochrony danych

1. *Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:*
   a) *przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;*
   b) *główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub*
   c) *główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.*
2. *Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.*
3. *Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych.*
4. *W przypadkach innych niż te, o których mowa w ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych. Inspektor ochrony danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących administratorów lub podmioty przetwarzające.*
5. *Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39.*
6. *Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.*

[22] Więcej informacji na temat zadań oraz statusu IOD dostępnych jest na stronie Urzędu Ochrony Danych Osobowych: www.uodo.gov.pl.

7. *Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.*

Podstawy prawne u.o.d.o.:

Artykuł 10. [Zawiadomienie Prezesa Urzędu o wyznaczeniu inspektora ochrony danych]

1. *Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.*
2. *Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, o którym mowa w ust. 1. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej.*
3. *W zawiadomieniu oprócz danych, o których mowa w ust. 1, wskazuje się:*
   1) *imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;*
   2) *firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;*
   3) *pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2;*
   4) *numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.*
4. *Podmiot, który wyznaczył inspektora, zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 1 i 3, oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania.*
5. *W przypadku wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez grupę przedsiębiorców, każdy z tych podmiotów dokonuje zawiadomienia, o którym mowa w ust. 1 i 4.*
6. *Zawiadomienia, o których mowa w ust. 1 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.*

Artykuł 11. [Udostępnianie danych inspektora ochrony danych]

Podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

7. Komu i na jakich warunkach MPM może powierzyć przetwarzanie danych osobowych

7.1 Kiedy dochodzi do powierzenia przetwarzania danych osobowych?

W sytuacji, w której:

- MPM przekazuje dane osobowe (pacjentów, pracowników lub innych osób) zewnętrznemu podmiotowi, aby je przetwarzał w imieniu i na rzecz MPM lub
- zewnętrzny podmiot przekazuje MPM dane osobowe, aby je przetwarzał w imieniu i na rzecz tego podmiotu.

dochodzi do powierzenia przetwarzania danych osobowych i konieczne jest zawarcie **umowy powierzenia przetwarzania danych osobowych**.

Przykłady powierzenia danych osobowych:

- placówka medyczna -> firma informatyczna
- placówka medyczna -> biuro rachunkowe
- placówka medyczna -> kancelaria prawna

7.2 Kto jest administratorem, a kto podmiotem przetwarzającym?

Administrator danych osobowych:

- ustala cele i sposoby przetwarzania danych osobowych;
- przekazuje dane osobowe na zewnątrz.

Podmiot przetwarzający (procesor):

- przetwarza dane osobowe w imieniu i na rzecz administratora;
- to jemu przekazywane są dane osobowe

Przykład:

Wykres 1. Przykład powierzenia przetwarzania danych osobowych

Jeżeli placówka medyczna korzysta z systemu informatycznego, gdzie gromadzi się informacje o pacjentach, dochodzi do powierzenia danych osobowych. **Administratorem** jest placówka medyczna (od niej wyszły dane dotyczące pacjenta), a procesorem – **firma, która dostarcza system informatyczny**, np. służący do prowadzenia elektronicznej dokumentacji, rejestracji wizyt online, udzielania świadczeń zdrowotnych za pośrednictwem systemów teleinformatycznych.

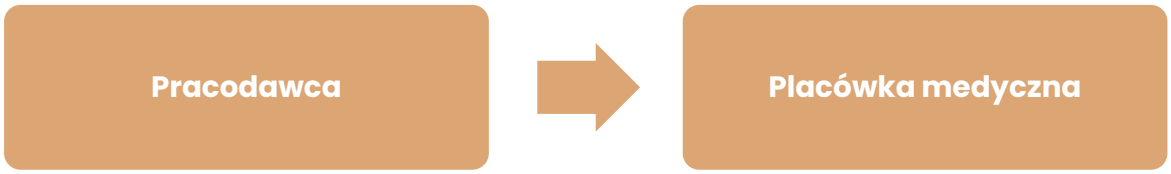
7.3 Kiedy NIE ZAWIERAMY umowy powierzenia?

Przykład 1:

Wykres 2. Przykład udostępnienia danych osobowych

Jeżeli jedna placówka medyczna udostępnia dane osobowe pacjentów drugiej placówce medycznej **w celu zachowania ciągłości usług medycznych**, nie ma podstaw dla zawarcia umowy powierzenia. Przykładem takiej sytuacji jest przekazywanie kart szczepień małoletniego pacjenta do nowej placówki medycznej, którą wybrali rodzice dziecka.

Przykład 2:



Wykres 3. Przykład udostępnienia danych osobowych

W przypadku świadczenia usług z zakresu medycyny pracy odrębnymi administratorami są:

- pracodawca kierujący pracowników na badania medycyny pracy oraz
- placówka medyczna świadcząca usługi z zakresu medycyny pracy.

Nie jest to sytuacja współadministrowania w rozumieniu art. 26 RODO, placówki świadczące usługi z zakresu medycyny pracy mają bowiem odrębną podstawę prawną, którą możemy znaleźć w przepisach o służbie medycyny pracy.

Zgodnie z przepisami o służbie medycyny pracy, placówka medyczna:

- musi prowadzić dokumentację medyczną pacjentów oraz
- nie może udostępniać pracodawcy dokumentacji medycznej jego pracowników.

Powyższe oznacza, że nie istnieje podległość placówki medycznej wobec pracodawcy – oba podmioty są administratorami danych osobowych. **Przy medycynie pracy nie dochodzi do powierzenia przetwarzania danych osobowych, ale do ich udostępniania**[23].

Przykład 3:

Wykres 4. Przykład udostępnienia danych osobowych

Udostępnieniem danych osobowych (a nie ich powierzeniem) jest także sytuacja, w której dane osobowe pacjentów są przekazywane przez placówkę medyczną do zewnętrznego laboratorium diagnostycznego, wystawiając pacjentowi skierowanie do wykonania badań diagnostycznych – w celu zachowania ciągłości leczenia (działalność laboratorium obejmuje udzielanie świadczeń zdrowotnych w celu rozpoznania stanu zdrowia i ustalenia dalszego postępowania leczniczego)[24].

Przykład 4:

Z powierzeniem nie mamy również do czynienia w sytuacji, w której osoba wykonująca zawód medyczny i prowadząca działalność gospodarczą wykonuje swoje zadania w ramach działalność leczniczej MPM. Jeżeli dana osoba (lekarz czy pielęgniarka):

- nie działa na własny rachunek;
- wykorzystuje bazy danych pacjentów MPM i system informatyczny MPM;
- nie prowadzi też własnej dokumentacji medycznej

to występuje w tej relacji jako **osoba upoważniona przez MPM do przetwarzania danych**, a nie jej podmiot przetwarzający.

7.4 Z kim można zawrzeć umowę powierzenia?

Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO).

[23] Urząd Ochrony Danych Osobowych, „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców" s. 29. (https://uodo.gov.pl/pl/138/545)
[24] Czy z laboratorium należy zawrzeć umowę powierzenia? https://uodo.gov.pl/pl/225/1552

7.5 Co powinna zawierać umowa powierzenia?

Przepisy dotyczące powierzenia mogą być zawarte:

- w oddzielnej umowie powierzenia;
- w umowie będącej podstawą współpracy stron (placówki medycznej i np. biura księgowego);
- w aneksie do umowy będącej podstawą współpracy stron.

Umowa może mieć formę pisemną, w tym formę elektroniczną.

Elementy umowy powierzenia:

1. Przedmiot umowy – *powierzenie danych osobowych pacjentów MPM do firmy IT w celu administrowania, konserwacji i naprawy systemu informatycznego w placówce medycznej.*
2. Czas trwania przetwarzania – *czas trwania umowy powierzenia jest równy okresowi umowy z firmą IT.*
3. Charakter przetwarzania – *z wykorzystaniem systemu IT.*
4. Cel przetwarzania – *administrowanie systemem IT na rzecz MPM.*
5. Rodzaj danych osobowych – *dane obecne w systemie IT (imiona, nazwiska, adresy zamieszkania, informacje o stanie zdrowia itp.)*.
6. Kategorie osób, których dane dotyczą – *pacjenci MPM.*
7. Prawa i obowiązki administratora.
8. Obowiązki procesora:
    a) zapewnienie, że pracownicy procesora zachowują dane w tajemnicy,
    b) zabezpieczenie danych osobowych,
    c) korzystanie z usług innego podmiotu przetwarzającego (podpowierzenie) na warunkach określonych przez administratora zgodnie z RODO,
    d) pomoc administratorowi w realizacji praw osób, których dane dotyczą,
    e) pomoc administratorowi w realizacji obowiązków wskazanych w art. 32-36 RODO,
    f) w zależności od decyzji administratora – usunięcie lub zwrot danych osobowych po zakończeniu współpracy (o ile nic innego nie wynika z przepisów prawa),
    g) udostępnienie administratorowi wszelkich informacji niezbędnych do wykazania przestrzegania przepisów RODO w zakresie umów powierzenia.

Podstawy prawne RODO:

Artykuł 28 - Podmiot przetwarzający

1. *Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.*
2. *Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.*
3. *Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:*
   a) *przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora - co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej - chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;*
   b) *zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;*
   c) *podejmuje wszelkie środki wymagane na mocy art. 32;*
   d) *przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;*
   e) *biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;*
   f) *uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36;*
   g) *po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz*

usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

W związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

4. *Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają - na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego - te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.*

5. *Wystarczające gwarancje, o których mowa w ust. 1 i 4 niniejszego artykułu, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.*

6. *Bez uszczerbku dla indywidualnych umów między administratorem a podmiotem przetwarzającym, umowa lub inny akt prawny, o których mowa w ust. 3 i 4 niniejszego artykułu, mogą się opierać w całości lub w części na standardowych klauzulach umownych, o których mowa w ust. 7 i 8 niniejszego artykułu, także gdy są one elementem certyfikacji udzielonej administratorowi lub podmiotowi przetwarzającemu zgodnie z art. 42 i 43.*

7. *Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.*

8. *Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.*

9. *Umowa lub inny akt prawny, o których mowa w ust. 3 i 4, mają formę pisemną, w tym formę elektroniczną.*

10. *Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.*

8. Postępowanie w przypadku naruszenia ochrony danych osobowych

8.1 Czym jest naruszenie ochrony danych osobowych?

Naruszenie ochrony danych osobowych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem:

- zniszczenia;
- utracenia;
- zmodyfikowania;
- nieuprawnionego ujawnienia;
- nieuprawnionego dostępu do danych

wobec danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez Administratora.

8.2 Jak dzielimy naruszenia ochrony danych osobowych?

NARUSZENIE POUFNOŚCI – niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych; przykład:

- wydanie dokumentacji medycznej osobie nieupoważnionej przez pacjenta;
- wyciek bazy danych pacjentów MPM do internetu.

NARUSZENIE DOSTĘPNOŚCI – niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich; przykład:

- zgubienie pendrive'a ze zdjęciami medycznymi pacjenta;
- zablokowanie dostępu lekarza do bazy danych pacjentów w wyniku ataku ransmoware na komputer tego lekarza.

NARUSZENIE INTEGRALNOŚCI – niedozwolona lub przypadkowa zmiana danych osobowych; przykład:

- zmiana nazwiska osoby fizycznej w systemie elektronicznej dokumentacji medycznej;
- zmiana danych w systemie rezerwacji na wizytę i wykonanie pacjentowi niewłaściwych badań czy zabiegów.

8.3 Jakie zdarzenia są naruszeniem ochrony danych osobowych lub mogą do niego prowadzić?

O naruszeniu bezpieczeństwa danych osobowych mogą świadczyć w szczególności następujące symptomy:

1. w obrębie pomieszczeń:
   a) ślady włamania lub prób włamania do pomieszczeń;
   b) ślady włamania lub prób włamania do szuflad, szafek lub szaf, w których przechowywane są dokumenty papierowe lub elektroniczne nośniki informacji zawierające dane osobowe,
2. w obrębie sprzętu komputerowego:
   a) kradzież lub zgubienie komputera lub innego sprzętu komputerowego, na którym przechowywane są dane osobowe;
   b) rozkręcona obudowa komputera;
   c) fizyczne zniszczenie komputera lub sprzętu komputerowego (na skutek działania przypadkowego lub celowego, bądź na skutek działania siły wyższej),
3. w obrębie systemu informatycznego:
   a) brak możliwości uruchomienia systemu operacyjnego komputera lub oprogramowania komputerowego;
   b) brak możliwości zalogowania się do systemu operacyjnego komputera lub oprogramowania komputerowego;
   c) zmiana zakresu upoważnień użytkownika w systemie informatycznym (np. brak możliwości wykonywania operacji, których realizacja była wcześniej możliwa lub dostęp do wcześniej zablokowanego programu);
   d) inny niż zwykle wygląd systemu operacyjnego lub oprogramowania komputerowego;
   e) niestandardowe komunikaty lub komunikaty błędu wyświetlane przez system operacyjny lub oprogramowanie komputerowe;
   f) znaczne spowolnienie działania systemu operacyjnego lub oprogramowania komputerowego;
   g) zmiana zakresu danych wykorzystywanych w ramach oprogramowania komputerowego.
4. inne:
   a) kradzież lub zgubienie dokumentacji papierowej zawierającej dane osobowe;
   b) kradzież lub zgubienie elektronicznego nośnika informacji zawierającego dane osobowe.

8.4 Kto w MPM odpowiada za bezpieczeństwo danych osobowych?

Każda osoba zatrudniona w placówce medycznej jest odpowiedzialna za bezpieczeństwo danych osobowych. Pracownik placówki medycznej, który podejrzewa lub stwierdza zdarzenie mogące doprowadzić do naruszenia bezpieczeństwa danych osobowych, zobowiązany jest do natychmiastowego poinformowania o tym **osoby odpowiedzialnej.**

Osoba odpowiedzialna przy realizacji swoich obowiązków w tym zakresie współpracuje z kierownictwem MPM, IOD (jeśli nie jest osobą odpowiedzialną) oraz informatykiem lub inną osobą, właściwą ze względu na naturę incydentu bezpieczeństwa.

Taką osobą, w pierwszej kolejności, jest **inspektor ochrony danych**. Jeżeli IOD nie został powołany, jego obowiązki w zakresie obsługi incydentów bezpieczeństwa realizuje osoba wyznaczona przez kierownictwo.

8.5 Jak postępować w razie otrzymania informacji o możliwym naruszeniu ochrony danych?

W przypadku otrzymania informacji o możliwym naruszeniu ochrony danych osoba odpowiedzialna współpracuje z kierownictwem placówki, informatykiem lub inną osobą, właściwą ze względu na naturę incydentu bezpieczeństwa i dokonuje sprawdzenia otrzymanej informacji.

Celem sprawdzenia jest przede wszystkim ustalenie, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych. Zgodnie z Wytycznymi WP 250 Grupy Roboczej art. 29[25], MPM powinna przy ocenie incydentu wziąć pod uwagę następujące kryteria: rodzaj naruszenia (poufność, dostępność, integralność), charakter, wrażliwość i zakres danych, łatwość identyfikacji osób fizycznych, skala konsekwencji dla osób fizycznych, liczba osób poszkodowanych oraz liczba osób, które uzyskały dostęp do danych. Wszystkie te informacje pozwolą właściwie określić poziom ryzyka danego incydentu dla praw lub wolności osób, których dane dotyczą (czyli prawdopodobieństwo i skutek wystąpienia negatywnych konsekwencji dla tych osób, np. kradzież tożsamości, brak możliwości wykonywania uprawnień, itp.). Jeżeli takie ryzyko się pojawia, MPM zgłasza tę sytuację do Prezesa UODO, zgodnie z art. 33 RODO. Incydent może również powodować wysokie ryzyko, czyli nieść ze sobą poważne konsekwencje dla osoby, której dane dotyczą – wtedy należy niezwłocznie zawiadomić o sytuacji tę osobę (zgodnie z art. 34 RODO). Przykłady takich sytuacji zawiera tabela poniżej.

O tym, czym jest ryzyko dla praw lub wolności piszemy w rozdziale 6 niniejszego kodeksu.

[25] Wytyczne WP250 Grupy Roboczej art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679: https://www.uodo.gov.pl/pl/10/12.

Właściwy sposób postępowania w zależności od poziomu ryzyka, jakie wiąże się z incydentem przedstawia poniższa tabela:

	Wewnętrzny rejestr naruszeń ADO	Zawiadomienie Prezesa UODO	Zawiadomienie osób, których dane dotyczą
Naruszenia ochrony danych, które nie powodują ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.	**TAK**	**NIE**	**NIE**
Naruszenia, które mogą skutkować ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą.	**TAK**	**TAK**	**NIE**
Naruszenia, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą.	**TAK**	**TAK**	**TAK**

Tabela 9. Sposób realizacji obowiązków MPM w przypadku określonych rodzajów naruszeń ochrony danych.

Jak widać, wszystkie opisane powyżej przypadki naruszeń, niezależnie od tego czy są zgłaszane do PUODO czy nie, MPM ewidencjonuje wewnętrznie. Może to robić w formie rejestru naruszeń na piśmie lub elektronicznie.

Przykłady:

Zdarzenie	Czy należy zawiadamiać Prezesa UODO?	Czy należy zawiadamiać osobę, której dotyczą dane?	Uwagi
Administrator przechowywał kopię zapasową archiwum danych osobowych, zaszyfrowaną na płycie CD. Płytę skradziono podczas włamania.	Nie	Nie	Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem techniki, istnieją kopie zapasowe danych, a unikalny klucz jest bezpieczny, może to być naruszenie niepodlegające obowiązkowi zgłoszenia.

			Jeżeli jednak w późniejszym terminie coś zagrozi temu bezpieczeństwu, powiadomienie Prezesa UODO będzie wymagane.
Z powodu krótkotrwałej przerwy w dostawie prądu w MPM, pacjenci nie mogli się dodzwonić do rejestracji.	Nie	Nie.	To nie jest naruszenie danych osobowych podlegające obowiązkowi zgłoszenia; niemniej, zdarzenie należy zarejestrować zgodnie z art. 33 ust. 5. RODO.
Na administratora przeprowadzono atak za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie istnieją kopie zapasowe i nie można odzyskać danych. W toku dochodzenia staje się jasne, że oprogramowanie jedynie szyfruje dane, a w systemie nie wykryto żadnego innego złośliwego oprogramowania.	Tak, ponieważ doszło do utraty dostępności należy powiadomić właściwy organ nadzorczy, jeżeli istnieje możliwość konsekwencji dla osób fizycznych.	Tak, należy powiadomić osoby fizyczne w zależności od charakteru naruszonych danych sobowych i możliwych skutków braku dostępu do danych oraz innych prawdopodobnych konsekwencji.	Jeżeli istniały kopie zapasowe i możliwe jest szybkie odzyskanie danych, o zdarzeniu nie trzeba powiadamiać organu nadzorczego ani osób fizycznych, ponieważ nie doszło do trwałej utraty dostępności lub poufności. Niemniej, w przypadku zgłoszenia do organu nadzorczego, organ może rozważyć przeprowadzenie dochodzenia w celu oceny zgodności z szerszymi wymogami bezpieczeństwa wynikającymi z art. 32. RODO.
Z powodu cyberataku dane medyczne placówki medycznej są niedostępne przez 30 godzin.	Tak, placówka jest zobowiązana zgłosić naruszenie, ponieważ może pojawić się wysokie ryzyko zagrożenia dobrostanu i prywatności pacjentów.	Tak, należy powiadomić osoby fizyczne, których dane naruszono	-
Pracownik MPM w drodze na wizytę patronażową przewozi dokumentację	Tak, dokumentacja medyczna zwiera szczególne kategorie danych matki i dziecka.	Tak, należy powiadomić osoby fizyczne, których dane naruszono	Przewożonej dokumentacji medycznej nie należy zostawiać w samochodzie (nawet w bagażniku). Zawsze należy zabierać ją ze sobą.

medyczną samochodem. Samochód zostaje skradziony wraz z dokumentacją.	Zakres informacji może powodować poważne konsekwencje dla tych osób, jeśli będą bezprawnie wykorzystane.		

Tabela 10. Sugerowane postępowanie MPM w przypadku stwierdzenia określonych rodzajów naruszeń ochrony danych.

8.6 W jaki sposób zawiadamiać o naruszeniach ochrony danych?

Jeśli sprawdzenie, o którym mowa wyżej potwierdzi, że MPM ma do czynienia z naruszeniem ochrony danych, które wiąże się z ryzykiem naruszenia praw lub wolności osób, MPM zgłasza takie naruszenie do Prezesa UODO niezwłocznie, nie później niż 72 godziny od momentu stwierdzenia naruszenia (czyli jego wykrycia, nie zaś kiedy naruszenie miało miejsce).

Zgłoszenia można dokonać na kilka sposobów:

- elektronicznie: poprzez platformę biznes.gov.pl (wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie lub za pomocą pisma ogólnego dostępnego na platformie) lub też poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP;
- tradycyjną pocztą wysyłając wypełniony formularz na adres Prezesa UODO.

Ważne, aby już na już etapie analizy incydentu, MPM zbierała wszelkie informacje niezbędne do wypełnienia formularza naruszenia ochrony danych, w tym m.in.: data stwierdzenia naruszenia, sposób stwierdzenia naruszenia, czas i data zaistnienia/zakończenia, na czym polegało naruszenie (np.: kradzież komputera, nieuprawnione uzyskanie dostępu do informacji itp.), przyczyna naruszenia, liczba osób, których dane dotyczą, kategorie danych (imię, nazwisko, dane o stanie zdrowia itp.), kategorie osób, których dane dotyczą (np.: pacjenci, pracownicy), czy też środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia.
W ten sposób MPM, w razie konieczności zawiadomienia Prezesa UODO o naruszeniu, będzie gotowy sprawnie i kompletnie wypełnić formularz i skutecznie zawiadomić organ nadzorczy o incydencie.

Jeśli w wyniku analizy zdarzenia, MPM nie będzie w stanie ustalić wszystkich okoliczności, o których mowa powyżej, w terminie 72 godzin, istnieje możliwość dokonania zgłoszenia wstępnego i przekazania informacji uzupełniających w późniejszym terminie.

W sytuacji, w której naruszenie wystąpiło u podmiotu przetwarzającego (np. w firmie kadrowej, obsługującej MPM, doszło do kradzieży dokumentacji pracowników MPM), **72 godziny również liczy się od momentu stwierdzenia naruszenia przez administratora,** czyli w momencie, w którym **podmiot przetwarzający poinformował go o wystąpieniu zdarzenia**[26].

W firmie kadrowej, obsługującej MPM, doszło do kradzieży dokumentacji pracowników. Naruszenie stwierdzono 24 lutego (poniedziałek) o godzinie 09:00. Firma poinformowała o tym placówkę medyczną 25 lutego (wtorek) o godzinie 09:00.
72 godziny na ewentualne zgłoszenie naruszenia do Prezesa UODO przez MPM upływają 28 lutego (piątek) o godzinie 09:00, a nie 27 lutego (czwartek) o godzinie 09:00.

Jeżeli naruszenie wiązać się będzie z wysokim ryzykiem naruszenia praw lub wolności osób, których to dotyczy, MPM będzie zobowiązane poinformować je o zdarzeniu, przekazując jasnym i prostym językiem takie informacje jak: opis charakteru naruszenia, imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, opis prawdopodobnych skutków naruszenia oraz opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Incydenty w zakresie ochrony danych mogą różnić się m.in.: charakterem naruszenia (poufność, dostępność, integralność), zakresem danych (dane zwykłe, dane wrażliwe) czy liczbą osób, które uzyskały dostęp do danych. W zależności od naruszenia, wśród prawdopodobnych skutków naruszenia MPM może wskazać w szczególności:

- wykorzystanie danych do naruszenia dobrego imienia (np. naruszenia dóbr osobistych podmiotu danych np. w postaci dyskryminacji), pozbawienia lub ograniczenia praw (np. możliwość korzystania z praw obywatelskich osoby, której dane dotyczą i głosowanie w imieniu poszkodowanego);
- składanie w imieniu poszkodowanego dyspozycji dotyczących wydawania dokumentacji medycznej lub wyrażania sprzeciwu co do udostępniania informacji medycznych czy uzyskiwania kopii dokumentacji medycznej z innych placówek medycznych;
- zarejestrowania na dane osobowe przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych;
- zawarcia w imieniu osoby, której dotyczy naruszenie umowy o świadczenie usług (np. telewizji kablowej, telefonu, energii elektrycznej, usług dostępu do materiałów audio lub wideo poprzez media strumieniowane, np. Spotify, Netflix, HBO itp.), która to umowa nie będzie opłacana i może spowodować znaczne zadłużenie.

Wśród działań, jakie MPM może rekomendować poszkodowanej osobie, można natomiast wskazać w szczególności:

[26] Zgodnie ze stanowiskiem EROD wyrażonym w zaktualizowanej wersji Wytycznych WP250 Grupy Roboczej art. 29, s.15.

- założenie konta w systemie informacji gospodarczej (np. bik.pl, bezpiecznypesel.pl, czy też chronpesel.pl) w celu upewnienia się, że na dane osobowe poszkodowanego nie została wzięta pożyczka lub kredyt (dotyczy sytuacji, kiedy incydent dotyczy numeru PESEL);
- poinformowanie właściwych organów (np. policji) w sytuacji, gdy poszkodowany dowie się o szkodzie majątkowej, związanej z kradzieżą tożsamości (np. w sytuacji, gdy ktoś wziął kredyt na jego dane osobowe);
- skontaktowanie się z innymi placówkami medycznymi, gdzie znajduje się dokumentacja medyczna poszkodowanego, w celu upewnienia się, że w jego imieniu nie były składane żadne dyspozycje (np. sprzeciw wobec wydania dokumentacji medycznej konkretnej osobie).

Wszystkie te informacje powinny być przekazywane osobom fizycznym indywidualnie, np. poprzez wysłanie wiadomości e-mail. **W wyjątkowych sytuacjach,** jeżeli zawiadomienie osób fizycznych, których dotyczy ryzyko, wymagałoby niewspółmiernie dużego wysiłku (np. kiedy niemożliwe jest ustalenie konkretnej liczby osób, których naruszenie dotyczy lub też MPM nie ma bezpośrednich danych kontaktowych, które mógłby użyć do szybkiego i skutecznego powiadomienia osoby) MPM może zrealizować obowiązek zawiadomienia poprzez publiczny komunikat:

- na tablicy ogłoszeń w MPM;
- na stronie internetowej MPM;
- przez ogłoszenie w prasie lokalnej.

Podstawy prawne RODO:

Artykuł 33 - Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. *W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chybaże jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.*
2. *Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.*
3. *Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:*
   a) *opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;*
   b) *zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;*

c) *opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;*

d) *opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.*

4. *Jeżeli - i w zakresie, w jakim - informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki*

5. *Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.*

Artykuł 34 - Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. *Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.*

2. *Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).*

3. *Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach*:

a) *administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*

b) *administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;*

c) *wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.*

4. *Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy - biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko - może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.*

9. Prawa osób, których dane dotyczą

9.1 Jakie prawa przysługują pacjentom zgodnie z RODO?

RODO przyznaje szereg uprawnień wszystkim osobom, których dane są przetwarzane. Dzięki tym uprawnieniom każda z osób będzie w stanie sprawować kontrolę nad informacjami, które jej dotyczą. Równocześnie nadanie tych uprawnień oznacza dla administratora danych obowiązki. MPM będzie zatem zobowiązany do realizacji następujących praw pacjentów:

- prawo do informacji (obowiązek informacyjny);
- prawo dostępu do danych;
- prawo do sprostowania danych;
- prawo do usunięcia danych (prawo do bycia zapomnianym);
- prawo do ograniczenia przetwarzania;
- prawo do przenoszenia danych;
- prawo do sprzeciwu,
- prawo do wycofania zgody w dowolnym momencie.

9.2 Jakie są podstawowe zasady, które MPM powinna stosować realizując uprawnienia osób?

Realizując prawa pacjentów, MPM dba w szczególności o potwierdzenie tożsamości osoby, która kieruje do MPM określone żądanie. W razie wątpliwości, MPM ma prawo poprosić pacjenta o potwierdzenie tożsamość (MPM prosi o okazanie dokumentów, ale ich nie kopiuje ani nie skanuje), tak by mieć pewność, że realizacja uprawnienia (np. prawa dostępu do danych) nastąpi wobec właściwej osoby i tym samym żadne informacje nie zostaną ujawnione osobom nieupoważnionym. W przypadku braku możliwości potwierdzenia tożsamości wnioskodawcy, MPM może nawet odmówić realizacji uprawnienia pacjenta, należy jednak podjąć wszelkie możliwe starania, żeby tę tożsamość ustalić (informując przy tym pacjenta, jakiego rodzaju informacje musi dostarczyć, by potwierdzić swoją tożsamość).

MPM dba, by wszelkie informacje dotyczące przetwarzania danych osobowych były przekazywane pacjentowi w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Należy więc dbać o to, by wszelka komunikacja z pacjentem była prowadzona w sposób dający nie tylko szansę na zapoznanie się z informacjami, ale przede wszystkim taki, który pozwoli pacjentowi na pełne zrozumienie przekazywanej treści.

MPM powinna również dokumentować wpływające wnioski i prowadzoną w związku z nimi korespondencję, choćby dla celów dowodowych, w związku z ewentualnymi sporami prowadzonymi z pacjentami.

9.3 W jakiej formie i jak szybko należy odpowiedzieć na żądanie osoby?

RODO dopuszcza różne formy udzielania informacji – pisemną, elektroniczną (np. poprzez bezpieczną stronę internetową) i nawet ustną (na żądanie pacjenta, po uprzednim potwierdzeniu jego tożsamości). Należy jednak pamiętać, że odpowiedzi na żądanie pacjenta należy udzielić niezwłocznie, najpóźniej w terminie miesiąca od wpłynięcia jego prośby. W tym terminie MPM powinna:

- zrealizować uprawnienie

lub

- poinformować pacjenta o działaniach podjętych w sprawie i konieczności przedłużenia terminu do maksymalnie 3 miesięcy z uwagi na skomplikowany charakter sprawy (MPM musi wskazać przyczyny takiego przedłużenia)

lub też

- poinformować o braku możliwości realizacji uprawnienia, wskazując na przyczyny niepodjęcia działań, prawie pacjenta do złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych oraz skargi do sądu.

MPM może także odmówić realizacji wniosków pacjenta w sytuacji, kiedy są one nieuzasadnione lub nadmierne, np.: nie udało się zweryfikować tożsamości pacjenta, realizacja uprawnienia naruszałaby prawa osób trzecich, mogłaby spowodować ujawnienie tajemnicy lekarskiej. Jeśli zatem odpowiedź na żądanie pacjenta (np. kiedy pacjent kilka razy w miesiącu prosi o nową kopię dokumentacji medycznej) wymagałoby zaangażowania personelu medycznego w taki sposób, że inni pacjenci nie mogliby skorzystać ze świadczeń medycznych lub znacznie wydłużyłby się czas realizacji takich świadczeń dla osób trzecich, MPM ma prawo odmówić realizacji takiego żądania.

9.4 Czy MPM może pobrać opłatę za zrealizowanie uprawnienia osoby?

Co do zasady, komunikacja z pacjentem w sprawach związanych z realizowaniem jego uprawnień wynikających z RODO powinna być prowadzona nieodpłatnie. Gdy jednak żądania pacjenta są ewidentnie nieuzasadnione lub nadmierne, MPM może pobierać rozsądną opłatę, uwzględniającą faktycznie poniesione koszty, np. wydatki związane ze sporządzaniem wydruków czy kserokopii.

Jeśli MPM otrzymuje zapytania od jednego pacjenta w sposób ustawiczny, udzielanie odpowiedzi angażuje wielu pracowników MPM lub też prawo ma zostać zrealizowane poprzez wysyłkę informacji do pacjenta kurierem, MPM może pobrać od pacjenta rozsądną opłatę za realizację uprawnienia pacjenta wynikającego z RODO.

9.5 Jak i kiedy należy realizować obowiązek informacyjny?

Prawo pacjenta do bycia poinformowanym jest jednym z najważniejszych elementów przetwarzania danych, gwarantuje bowiem należytą przejrzystość prowadzonych przez MPM działań.

Obowiązek informacyjny należy spełnić przed rozpoczęciem przetwarzania danych, tj. zanim dane będą zbierane. Zgodnie z RODO należy przekazać przede wszystkim takie informacje jak: oznaczenie MPM oraz dane kontaktowe MPM i wyznaczonego inspektora ochrony danych, cel przetwarzania danych oraz podstawę prawną takiego przetwarzania, jak również informacje o odbiorcach danych (np. informacja o przekazaniu danych do laboratoriów). Pełny zakres informacji, które należy przekazać, zawiera art. 13 i 14 RODO.

Obowiązek informacyjny powinien – w miarę możliwości – zostać spełniony bezpośrednio w komunikacji z pacjentem. Można go spełnić przede wszystkim poprzez umieszczenie informacji o przetwarzaniu danych osobowych w dokumentach przekazywanych pacjentowi do podpisu (np. deklaracji POZ czy też umowie o świadczenie usług medycznych). Niezależnie od powyższego MPM powinna zdecydować się na umieszczenie klauzul informacyjnych na tablicach informacyjnych w recepcji lub też umieszczenie klauzul informacyjnych na stronach internetowych MPM. Możliwe jest także ustne przekazanie informacji podczas rozmowy telefonicznej czy też informacja przekazana drogą elektroniczną.

Na potrzeby rozliczalności MPM przechowuje dokumentację dot. spełnienia obowiązku informacyjnego, np. poprzez zbieranie podpisanych formularzy, na których znajduje się taki obowiązek, zdjęcia tablic informacyjnych w rejestracji, zapewnienie możliwości odsłuchania nagrania podczas rozpoczęcia rozmowy telefonicznej lub też kopię strony internetowej, na której widnieje klauzula informacyjna. Działania te mają na celu udowodnienie, że właściwie spełniono obowiązki informacyjne wobec pacjenta.

RODO przewiduje sytuacje, w których przekazanie informacji dotyczących przetwarzania danych nie będzie konieczne. MPM nie musi przekazywać wszystkich powyższych informacji jeśli pacjent już te informacje posiada. Jeśli MPM zbiera dane osobowe, ale nie bezpośrednio od osoby, której dane dotyczą (np. kiedy otrzymuje udostępnioną przez inną placówkę dokumentację pacjenta lub zbiera dane osobowe osób upoważnionych przez pacjenta), spełnienie obowiązku również nie będzie konieczne, bowiem zgodnie z art. 14 ust. 5 lit. c) RODO zbieranie takich danych uregulowane jest przepisami UoPPiRPP.

9.5.1 Co w sytuacji ratowania życia i zdrowia pacjenta?

W sytuacji ratowania życia i zdrowia najważniejsza jest pomoc pacjentowi. W takiej sytuacji MPM również nie ma obowiązku spełniania obowiązków informacyjnych w momencie pozyskania danych. Obowiązki informacyjne MPM powinien jednak wypełnić kiedy będzie na to pozwalał stan pacjenta.

9.6 Co to jest prawo dostępu do danych i jak należy je realizować?

Każdy pacjent oraz osoby, których dane osobowe przetwarza MPM, mają prawo uzyskać od MPM potwierdzenie przetwarzania ich danych osobowych. Jeśli MPM rzeczywiście przetwarza ich dane, osoby te mają prawo dostępu do swoich danych i uzyskania wielu innych informacji, m.in.: o celu przetwarzania, kategorii danych (np. imię, nazwisko, dane kontaktowe, informacje o stanie zdrowia), przysługujących uprawnieniach, odbiorcach danych czy planowanym okresie przetwarzania. Pełną listę informacji, o które może prosić pacjent, określa art. 15 RODO.

Prawo pacjenta dostępu do danych na podstawie RODO jest uprawnieniem odrębnym od tego, który przysługuje mu na podstawie przepisów regulujących działalność medyczną MPM. Placówki medyczne udostępniają zatem dane osobowe dotyczące pacjentów na podstawie:

- art. 15 RODO (realizując prawo dostępu przysługujące osobie, której dane dotyczą); na podstawie tego artykułu pacjent ma prawo do otrzymania informacji na temat danych osobowych przetwarzanych na jego temat w MPM oraz do kopii tych danych;
- art. 9 UoPPiRPP (realizując prawo pacjenta do informacji);
- art. 26 UOPPIRPP (realizując prawo pacjenta do dokumentacji medycznej).

W celu prawidłowego zabezpieczenia danych osobowych przed udostępnieniem osobie nieuprawnionej, MPM musi ustalić, kto i na jakiej podstawie może otrzymać dane osobowe przetwarzane w jego placówce, na jakich zasadach będzie się odbywało udostępnienie oraz w jakiej formie. W tym celu dobrą praktyką jest opracowanie i wprowadzenie dwóch instrukcji:

1) dotyczącą udzielania informacji na temat stanu zdrowia pacjenta (jak również udzielanych mu świadczeń) oraz udostępniania dokumentacji medycznej pacjenta;
2) dotyczącą dostępu do danych osobowych, przysługującemu osobie, której dane dotyczą, w tym dostarczenia osobie, której dane dotyczą kopii danych osobowych podlegających przetwarzaniu.

	RODO	UoPPiRPP
Komu	Osobie, której dane dotyczą, przedstawicielowi ustawowemu, pełnomocnikowi.	Pacjentowi, przedstawicielowi ustawowemu, osobie upoważnionej przez pacjenta, podmiotom upoważnionym na podstawie przepisów prawa. Uwaga: w przypadku wydania recept wystawianych bez dokonania osobistego badania pacjenta należy pamiętać o tym, że taka recepta może zostać wydana pacjentowi, osobom upoważnionym przez

		pacjenta (wskazanym z imienia i nazwiska) oraz dowolnej osobie trzeciej – jeżeli pacjent w upoważnieniu wskaże, że ww. receptę można wydać dowolnej osobie, która się po nią zgłosi.
Zakres danych	Wszelkie informacje dotyczące konkretnego pacjenta wraz z informacjami o celu przetwarzania, czasie przechowywania, przysługujących uprawnieniach, a także fakcie przekazania danych odbiorcom (np. na podstawie umowy powierzenia).	Dokumentacja medyczna, informacja o stanie zdrowia i udzielonych świadczeniach
Sposób udostępnienia	Wgląd, kopia.	Wgląd, wyciąg, odpis, kopia, wydruk z systemu informatycznego, oryginał (na zasadach art. 27 ust. 1 pkt. 3 UoPPiRPP), np. za pośrednictwem środków komunikacji elektronicznej, na informatycznym nośniku danych, w formie skanu (na zasadach art. 27 ust. 3 UoPPiRPP).
Sposób przekazania	Odbiór osobisty, przesłanie pocztą, kurierem, przekazanie drogą elektroniczną (zapewniającą bezpieczną komunikację), umożliwienie wglądu poprzez własny kanał do pobrania danych.	Odbiór osobisty, przesłanie pocztą, kurierem, przekazanie drogą elektroniczną (zapewniającą bezpieczną komunikację), np. na nośniku danych.
Koszt udostępnienia	Pierwsza kopia nieodpłatnie, możliwość pobierania opłaty wynikająca z kosztów administracyjnych za kolejne kopie.	UoPPiRPP określa konkretne kwoty za udostępnienie dokumentacji medycznej, zastrzega jednak, że pierwszy dostęp do danych zawartych w dokumentacji medycznej w danym zakresie jest dla pacjenta lub jego przedstawiciela ustawowego nieodpłatny Forma udostępnienia nie ogranicza się jedynie do kopii -uprawnienie może zostać zrealizowane poprzez uzyskanie odpisu, wyciągu, wydruku, skanu (jeżeli taka forma udostępnienia została przewidziana w regulaminie organizacyjnym podmiotu leczniczego), a także udostępnienie danych na nośniku informatycznym.

Udokumentowanie udostępnienia	Każde udostępnienie danych osobowych powinno być udokumentowane w sposób pozwalający na ustalenie komu kiedy, przez kogo i jakie dane zostały przekazane.	Udostępnienie dokumentacji medycznej powinno być udokumentowane przez ADO. Przepisy sektorowe określają w jaki sposób ADO powinien dokumentować udostępnienie danych osobowych w zależności od rodzaju dokumentacji medycznej. Na podstawie art. 27, ust. 4 UoPPiRPP ADO zobowiązany jest do prowadzenia wykazu dotyczącego udostępnionej dokumentacji medycznej, w którym zawarte będą następujące informacje: 1) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna; 2) sposób udostępnienia dokumentacji medycznej; 3) zakres udostępnionej dokumentacji medycznej; 4) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna oraz ew. nazwę uprawnionego organu lub podmiotu; 5) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną; 6) datę udostępnienia dokumentacji medycznej. Art. 42 ust. 5 Ustawy o zawodach lekarza i lekarza dentysty z kolei, reguluje kwestię udokumentowania wydawania recepty bez dokonania osobistego badania pacjenta i wskazuje, że w takim przypadku informacja o osobie, której przekazano taką receptę lub zlecenie, odnotowuje się w dokumentacji medycznej pacjenta albo dołącza do niej. Przekazanie osobie upoważnionej (lub przedstawicielowi ustawowemu) informacji o stanie zdrowia pacjenta i udzielonych mu świadczeniach musi zostać odpowiednio opisane w dokumentacji medycznej.

Tabela 11. Omówienie zasad dostępu do danych na gruncie RODO i UoPPiRPP.

Przekazanie pacjentowi kopii danych nie stanowi podstawy do ich usunięcia czy skrócenia ustawowych okresów ich archiwizowania.

Ponadto należy pamiętać, że każde udostępnienie danych osobowych, niezależnie od formy i sposobu ich przekazania, powinno zostać udokumentowane w rejestrze.

Przykład 1: Upoważnienie do dokumentacji medycznej zawiera:

Imię i nazwisko osoby upoważnionej przez pacjenta, zakres dokumentacji, której dotyczy upoważnienie, np. dokumentacja poradni neurologicznej, wyniki badań laboratoryjnych albo opis RTG kolana.

UWAGA: Należy pamiętać, że obowiązkiem MPM jest przechowywanie oświadczenia o upoważnieniu do dokumentacji medycznej lub informacji o braku takiego upoważnienia. Kiedy pacjent nie jest w stanie przygotować pisemnego upoważnienia (np. pacjent niewidomy lub z niedowładem), może przekazać informację o upoważnieniu ustnie, natomiast pracownik MPM, któremu powyższa informacja jest przekazywana, powinien zapisać ten fakt i dołączyć do dokumentacji medycznej z adnotacją „podpis niemożliwy".

Przykład 2: Instrukcja udostępniania dokumentacji medycznej pacjenta zawiera:

1. Informacje o tym, komu można ją udostępnić;
2. Na jakiej podstawie MPM ją udostępnia[27];
3. W jakiej formie MPM ją udostępnia;
4. Zasady udostępniania oryginału;
5. Określenie zasad udostępniania za pośrednictwem środków komunikacji elektronicznej lub na informatycznym nośniku danych (sposoby weryfikacji wnioskodawcy, bezpieczny sposób przekazania danych);
6. Określenie zasad fizycznego przekazania dokumentacji medycznej (m.in. dopuszczalność przesyłania dokumentacji za pomocą poczty lub kuriera i związana z tym procedura weryfikacji odbiorcy);
7. Sposób weryfikacji wnioskodawcy i jego uprawnień;
8. Sposób prowadzenia wykazu każdej udostępnionej dokumentacji medycznej;

Powyższa instrukcja musi być zgodna z obowiązującymi przepisami prawa i uwzględniać rozdział 7 UoPPiRPP.

[27] Zgodnie z orzeczeniem Naczelnego Sądu Administracyjnego z 16 grudnia 2015 r. (sygn. akt II OSK 3019/15) wniosek o udostępnienie dokumentacji medycznej może być składany w dowolnej formie (w tym ustnie). Ustalenie w regulaminie organizacyjnym placówki ograniczeń w tym zakresie może być uznawane za naruszenie praw pacjentów.

Przykład 3: Przekazanie informacji na temat pacjenta drogą telefoniczną:

Ze względów bezpieczeństwa należy zachować szczególną ostrożność podczas przekazywania informacji medycznych telefonicznie. Nigdy nie mamy pewności, kto jest po drugiej stronie słuchawki, i czy nie podszywa się pod pacjenta MPM.

Mogą mieć jednak miejsce sytuacje, kiedy ze względu na dobro pacjenta konieczne będzie przekazywanie informacji za pośrednictwem telefonu, np. przy przekazywaniu wyników badań, gdzie od znajomości rezultatu zależy życie/zdrowie pacjenta (np. wyniki badań INR). W takich sytuacjach MPM powinna podjąć należyte środki ostrożności, np.:

- wcześniejsze uzgodnienie z pacjentem numeru telefonu, który należy do niego, i na który można przekazywać informacje o wynikach badań,
- ustalenie sposobu weryfikacji tożsamości pacjenta (przez zobowiązanie do podania informacji, którą zna tylko pacjent – data urodzenia, nazwisko lekarza prowadzącego, ustalone wcześniej słowo-klucz); zasadniczo uznaje się, że udzielenie odpowiedzi na trzy różne pytania pozwala na zdalną weryfikację tożsamości pacjenta,

w miarę możliwości unikanie przekazywania informacji medycznej - np. zamiast podawania wyników badań przez telefon poinstruowanie pacjenta co do sposobu uzyskania informacji (*Wyniki może Pan odebrać w recepcji placówki…* lub *Powinna się pani skontaktować z doktor X*).

9.6.1 Weryfikacja tożsamości przy kontakcie zdalnym

Przy realizowaniu świadczeń w ramach tzw. teleporad, wniosków o dostęp do dokumentacji medycznej, składanych elektronicznie lub telefonicznym przekazywaniu (w drodze wyjątku) kodu e-recepty również należy zachować odpowiednie środki ostrożności.

Przy kontakcie telefonicznym lub e-mailowym weryfikacja tożsamości tylko na podstawie danych identyfikacyjnych (imię, nazwisko, data urodzenia, PESEL) nie będzie wystarczająca. Należy dokonać dodatkowej weryfikacji przez zadanie minimum trzech pytań, spełniających następujące kryteria:

- wnioskodawca zna na nie odpowiedź,
- MPM zna na nie odpowiedź,
- odpowiedzi zna osoba postronna.

W związku z powyższym można prosić o podanie np.: nazwiska lekarza, do którego pacjent (wnioskodawca) złożył deklarację wyboru bądź u którego był na ostatniej wizycie lub wskazania daty ostatniej wizyty. Brak odpowiedzi na przynajmniej jedno z pytań oznacza, że weryfikacja tożsamości nie powiodła się i konieczny jest osobisty kontakt wnioskodawcy z MPM.

Weryfikacji uprawnień wnioskodawcy (przedstawiciela ustawowego, osoby upoważnionej) dokonuje się przede wszystkim na podstawie treści dokumentacji medycznej konkretnego pacjenta.

9.7 Czy prawo do uzyskania kopii danych jest tym samym co prawo dostępu do dokumentacji medycznej?

W związku z wejściem w życie nowych przepisów dotyczących udostępniania dokumentacji medycznej po wprowadzeniu RODO, doprecyzowano kwestię dostępu do pierwszej kopii danych osobowych, jeżeli dane te są zawarte w dokumentacji medycznej. Należy jednak pamiętać, że prawo pacjenta dotyczące dostępu do dokumentacji medycznej nie jest tym samym co przysługujące każdemu z nas na mocy RODO prawo otrzymania kopii danych osobowych. Są to dwa różne prawa i służą różnym celom.

Według opinii Moniki Krasińskiej, Dyrektor Departamentu Orzecznictwa i Legislacji w UODO, opublikowanej w „Ochrona danych osobowych medycznych. 2. Wydanie" *„Pacjent wnioskując o dostęp do dokumentacji medycznej, ma możliwość pozyskania informacji i elementów, których co do zasady nie jest uprawniony żądać na podstawie RODO (np. podpis osoby udzielającej świadczeń medycznych, kod jednostki z systemu resortowych kodów identyfikacyjnych."*

Oznacza to, że jeżeli pacjent wskaże, że wnioskuje o realizację prawa na gruncie przepisów RODO, to ma prawo bezpłatnie otrzymać kopię danych osobowych zawartych w dokumentacji medycznej. W praktyce trudno jednak wyobrazić sobie inny sposób realizacji tego uprawnienia niż przekazanie kopii dokumentacji medycznej.

Pacjent lub jego przedstawiciel ustawowy lub osoba upoważniona może (zgodnie z obowiązującymi od 4 maja 2019 r. przepisami) uzyskać za darmo pierwszy dostęp do dokumentacji medycznej w danym zakresie. Pacjent może w ramach tego uprawnienia zwrócić się zarówno o kopię, jak i o odpis, wyciąg lub wydruk, a także o przekazanie danych na informatycznym nośniku danych (nie pobiera się wówczas opłat za płytę CD czy pendrive'a). Jeżeli w regulaminie organizacyjnym przewidziano możliwość wykonywania skanów, również o taką formę udostępnienia może zwrócić się pacjent. Zapewnienie wglądu do dokumentacji medycznej nie jest natomiast wystarczające – pacjent musi uzyskać fizyczne potwierdzenie informacji, jakie znajdują się w zasobie określonego podmiotu.

Z nowego uprawnienia można skorzystać tylko raz, niezależnie od wybranej formy udostępnienia. Co istotne, bezpłatny dostęp należy zapewnić wyłącznie pacjentowi lub jego przedstawicielowi ustawowemu (np. rodzic dziecka), ale nowe uprawnienie nie dotyczy osób upoważnionych przez pacjenta czy instytucji. Udostępnienie, chociaż bezpłatne, musi zostać odnotowane w wykazie udostępnionej dokumentacji medycznej, do prowadzenia którego zobowiązany jest każdy podmiot prowadzący dokumentację medyczną.

Wdrożenie rozwiązań dotyczących dostępu do pierwszej kopii danych wymaga zweryfikowania dotychczasowych procedur udostępniania. W wykazie udostępnianej dokumentacji medycznej należy zadbać o prawidłowe wskazywanie zakresów udostępnionej dokumentacji medycznej przyjmując jednolite oznaczenia zakresów.
Mówiąc o zakresie możemy posługiwać się konkretnymi datami np. leczenie w Poradni Lekarza POZ od 01.01.2019 r. do 04.05.2019 r. (to dobre rozwiązanie przy dokumentacji prowadzonej w formie elektronicznej) albo numerami stron np. historia zdrowia i choroby

Poradni Laryngologicznej od str. 15 do 68 (optymalne rozwiązanie dla dokumentacji papierowej). Jeżeli we wzorze wykazu nie przewidziano miejsca na dodatkowe informacje należy dodać miejsce na adnotację, że udostępniono w danym zakresie po raz pierwszy, bez opłat, tak żeby ułatwić odnalezienie tej informacji w przyszłości. Można również wprowadzić rozwiązania sprzyjające łatwiejszemu wyszukiwaniu danych pacjenta w wykazie np. prowadząc wykaz w układzie alfabetycznym.

Personel, który odpowiada za udostępnianie dokumentacji medycznej musi mieć zapewniony stały dostęp do wykazu udostępnionej dokumentacji medycznej, aby mieć możliwość zweryfikowania, czy pacjent uzyskał już dostęp do swoich danych osobowych i w jakim zakresie.

W zakresie realizacji obowiązków informacyjnych, niezbędna jest zmiana informacji dotyczących opłat na tablicy informacyjnej podmiotu leczniczego. Do dotychczas przekazywanych pacjentom informacji o wysokości pobieranych opłat należy dodać informację o możliwości uzyskania przez pacjenta lub jego przedstawiciela ustawowego bezpłatnie pierwszej kopii, odpisu, wyciągu, skanu (jeżeli przewidziano w regulaminie organizacyjnym) lub dokumentacji na elektronicznym nośniku danych.

9.8 Inne przykłady wniosków o kopię danych w MPM

Zgodnie z tym co zostało wskazane we wcześniejszej części tekstu, najczęstszymi wnioskami o dostęp do danych na podstawie art. 15 RODO są wnioski o dostęp do dokumentacji medycznej. Mogą mieć jednak miejsce sytuacje, w których przywołany przepis nie będzie dotyczył dokumentacji medycznej.

Przykładem takiej sytuacji jest wniosek o dostęp do nagrania z monitoringu, którego administratorem jest MPM. Przy okazji takich wniosków należy pamiętać, że zgodnie z art. 15 ust. 4 RODO prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych osób. Oznacza to w szczególności, że jeżeli na nagraniu, które interesuje wnioskodawcę, znajdują się inne osoby, to udostępnienie nagrania wideo może mieć miejsce jedynie po spełnieniu warunków opisanych w p. 11.4 niniejszego kodeksu (ze względu na ryzyko naruszenia dóbr osobistych tych ludzi).

Dodatkowo jeżeli podstawą wniosku o wydanie nagrania z monitoringu jest negatywne zdarzenie, jakie dotknęło wnioskodawcę (np. kradzież portfela z płaszcza powieszonego w poczekalni lub zarysowanie auta na parkingu MPM przez innego kierowcę), należy postępować zgodnie z wytycznymi zawartymi w rozdziale 11 Kodeksu.

9.9 Czy pacjent ma prawo sprostować swoje dane?

Zgodnie z RODO każdy pacjent ma prawo żądać sprostowania danych, które są nieprawidłowe. Może również prosić o uzupełnienie danych, które są niekompletne.

> Pacjent o imieniu Jan Kowalski prosi o zmianę jego imienia i nazwiska na fikcyjne Onufry Zagłoba. MPM może odmówić sprostowania takiej informacji bez potwierdzenia tak znaczącej zmiany danych, upewniając się uprzednio, czy nowo podane dane są prawdziwe.

Kiedy MPM dokona korekty informacji dotyczącej pacjenta (np. zmiany nazwiska, zmiany numeru telefonu lub adresu zamieszkania), powinna poinformować o tym fakcie wszystkich odbiorców danych, w tym podmioty, którym powierzono dane osobowe. Ma to szczególne znaczenie dla prawidłowego leczenia tego pacjenta (np. nieprzekazanie informacji może nieść zagrożenie dla życia lub zdrowia pacjenta).

MPM nie musi jednak informować odbiorców o zmianach, o których mowa powyżej, jeśli okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku, np. gdy powierzenie danych obejmuje znaczącą liczbę podmiotów lub też dane zostały ujawnione odbiorcom wiele lat wcześniej (co najmniej rok) i MPM nie jest w stanie nawiązać z nimi kontaktu (pomimo podjętych prób).

9.10 Prawo do bycia zapomnianym – czy można zapomnieć o pacjencie?

Każda osoba, której dane są przetwarzane, ma prawo do żądania usunięcia swoich danych. RODO wskazuje jednak, że prawo to nie będzie miało zastosowania, jeśli przetwarzanie tych danych jest niezbędne do realizacji obowiązku prawnego. Wobec faktu, że dane medyczne pacjentów przetwarzane są na podstawie stosownych przepisów prawa, dane pacjenta oraz jego dokumentacja medyczna nie będą mogły zostać usunięte na wniosek pacjenta.

Jeśli podstawą przetwarzania jest zgoda pacjenta (np. kiedy pozyskujemy jego zgodę na przesyłanie informacji marketingowych), pacjent może wycofać zgodę i zawnioskować o usunięcie jego danych. Wtedy MPM usuwa te dane i nie wykorzystuje ich już do dalszego przetwarzania w celu, dla którego zostały zebrane.

Dane mogą jednak zostać zachowane w MPM, jeśli będzie to niezbędne dla celów archiwalnych (przechowywanie dokumentacji medycznej przez okres określony w przepisach prawa). Dobrą praktyką po usunięciu danych zgodnie z żądaniem pacjenta jest zachowanie informacji o tym, kto złożył wniosek i w sposób MPM spełniła żądanie. Będzie to konieczne do zachowania zasady rozliczalności. Wyznaczony przez MPM inspektor ochrony danych, uwzględniając formy przetwarzania danych, ustala sposób rozpatrywania oraz okres przechowywania takich wniosków.

9.11 Czy pacjent może ograniczyć przetwarzanie danych?

Pacjent ma prawo oczekiwać, że MPM ograniczy przetwarzanie jego danych osobowych na przykład w sytuacji, kiedy pacjent kwestionuje prawidłowość danych przetwarzanych przez MPM. Ograniczenie oznacza w praktyce, że nie można dokonywać na danych innych operacji niż przechowywanie.

W praktyce funkcjonowania MPM do takiej sytuacji jednak nie powinno dochodzić. RODO upoważnia do dalszego przetwarzania danych mimo zgłoszonego wniosku o ograniczenie, jeśli uzasadnia to interes publiczny, nadrzędny wobec uprawnienia osoby. Ograniczenie przetwarzania danych zawartych w dokumentacji medycznej mogłoby nieść duże ryzyko dla zdrowia i życia pacjenta, z tego powodu, wobec danych medycznych, prawo do ograniczenia przetwarzania co do zasady nie będzie miało zastosowania.

9.12 Sprzeciw i przeniesienie danych – czy MPM to dotyczy?

Prawa pacjenta do sprzeciwu i do przeniesienia danych nie stosuje się do operacji przetwarzania, których podstawą jest obowiązek wynikający z przepisu prawa. Pacjent nie będzie miał zatem prawa do sprzeciwu wobec przetwarzania danych medycznych. Nie będzie mógł również skorzystać z prawa do przeniesienia tych danych wobec tych danych.

Prawo do przeniesienia danych będzie oczywiście przysługiwało w sytuacji, kiedy podstawą przetwarzania będzie zgoda (np. kiedy wykorzystywane są dane kontaktowe pacjenta w celach marketingowych) oraz kiedy dane będą przetwarzane w sposób zautomatyzowany (prawo nie będzie więc miało zastosowania wobec dokumentów papierowych). W takiej sytuacji MPM zobowiązana będzie do przetwarzania danych zebranych na podstawie zgody w powszechnie używanym formacie umożliwiającym maszynowy odczyt i przeniesienie (np. otwarte formaty takie jak XML, JSON, CSV). Dane mogą zostać dostarczone do pacjenta lub do innego administratora – zgodnie z decyzją pacjenta. Więcej informacji na temat tego uprawnienia zawierają Wytyczne WP242 Grupy Roboczej Art. 29[28].

Natomiast sprzeciw będzie mógł zostać wykorzystany przez pacjenta w sytuacji, kiedy MPM prowadzi działania marketingowe tradycyjnymi kanałami komunikacji wobec pacjentów (np. wysyłka pocztą), od których nie ma zgód na kontakt marketingowy, o czym wyżej. W takiej sytuacji MPM w momencie otrzymania takie sprzeciwu powinna zaprzestać dalszej wysyłki informacji marketingowych takiemu pacjentowi.

[28] Wytyczne WP242 Grupy Roboczej art. 29 dotyczące prawa do przenoszenia danych: https://uodo.gov.pl/pl/10/6.

Podstawy prawne RODO:

Artykuł 12 - Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

1. *Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem - w szczególności gdy informacje są kierowane do dziecka - udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15-22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.*

2. *Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15-22. W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15-22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.*

3. *Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.*

4. *Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.*

5. *Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:*

   a) *pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo*

   b) *odmówić podjęcia działań w związku z żądaniem.*

   Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

6. *Bez uszczerbku dla art. 11, jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15-21, może*

zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

7. *Informacje, których udziela się osobom, których dane dotyczą, na mocy art. 13 i 14, można opatrzyć standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, muszą się nadawać do odczytu maszynowego.*
8. *Komisji przysługuje prawo przyjmowania aktów delegowanych zgodnie z art. 92 w celu określenia informacji przedstawianych za pomocą znaków graficznych i procedur ustanowienia standardowych znaków graficznych.*

Artykuł 13 - Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą

1. *Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:*
   a) *swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;*
   b) *gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;*
   c) *cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;*
   d) *jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;*
   e) *informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;*
   f) *gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.*
2. *Poza informacjami, o których mowa w ust. 1, podczas pozyskiwania danych osobowych administrator podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:*
   a) *okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;*
   b) *informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;*

c) *jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;*

d) *informacje o prawie wniesienia skargi do organu nadzorczego;*

e) *informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;*

f) *informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.*

3. *Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.*

4. *Ust. 1, 2 i 3 nie mają zastosowania, gdy - i w zakresie, w jakim - osoba, której dane dotyczą, dysponuje już tymi informacjami.*

Artykuł 14 - Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

1. *Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą, następujące informacje:*

a) *swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;*

b) *gdy ma to zastosowanie - dane kontaktowe inspektora ochrony danych;*

c) *cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;*

d) *kategorie odnośnych danych osobowych;*

e) *informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;*

f) *gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz informację o sposobach uzyskania kopii tych zabezpieczeń lub o miejscu ich udostępnienia.*

2. *Poza informacjami, o których mowa w ust. 1, administrator podaje osobie, której dane dotyczą, następujące informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania wobec osoby, której dane dotyczą*:

   a) *okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;*

   b) *jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) - prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;*

   c) *informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;*

   d) *jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;*

   e) *informacje o prawie wniesienia skargi do organu nadzorczego;*

   f) *źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;*

   g) *informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.*

3. *Informacje, o których mowa w ust. 1 i 2, administrator podaje*:

   a) *w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;*

   b) *jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub*

   c) *jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.*

4. *Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.*

5. *Ust. 1- 4 nie mają zastosowania, gdy - i w zakresie, w jakim*:

   a) *osoba, której dane dotyczą, dysponuje już tymi informacjami;*

   b) *udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do*

celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

c) *pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub*

d) *dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.*

Artykuł 15 - Prawo dostępu przysługujące osobie, której dane dotyczą

1. *Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:*

   a) *cele przetwarzania;*

   b) *kategorie odnośnych danych osobowych;*

   c) *informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;*

   d) *w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;*

   e) *informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;*

   f) *informacje o prawie wniesienia skargi do organu nadzorczego;*

   g) *jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle;*

   h) *informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.*

2. *Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana*

o odpowiednich zabezpieczeniach, o których mowa w art. 46, związanych z przekazaniem.

3. *Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.*

4. *Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.*

Artykuł 16 - Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

Artykuł 17 - Prawo do usunięcia danych ("prawo do bycia zapomnianym")

1. *Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:*

   a) *dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;*

   b) *osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;*

   c) *osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;*

   d) *dane osobowe były przetwarzane niezgodnie z prawem;*

   e) *dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;*

   f) *dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.*

2. *Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to - biorąc pod uwagę dostępną technologię i koszt realizacji - podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.*

3. *Ust. 1 i 2 nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:*

   a) *do korzystania z prawa do wolności wypowiedzi i informacji;*

   b) *do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;*

   c) *z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;*

   d) *do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub*

   e) *do ustalenia, dochodzenia lub obrony roszczeń.*

Artykuł 18 - Prawo do ograniczenia przetwarzania

1. *Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:*

   a) *osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;*

   b) *przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;*

   c) *administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;*

   d) *osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.*

2. *Jeżeli na mocy ust. 1 przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony*

praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

3. *Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą, która żądała ograniczenia na mocy ust. 1.*

Artykuł 19 - Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

Artykuł 20 - Prawo do przenoszenia danych

1. *Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, jeżeli:*
   a) *przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) lub na podstawie umowy w myśl art. 6 ust. 1 lit. b); oraz*
   b) *przetwarzanie odbywa się w sposób zautomatyzowany.*
2. *Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.*
3. *Wykonanie prawa, o którym mowa w ust. 1 niniejszego artykułu, pozostaje bez uszczerbku dla art. 17. Prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.*
4. *Prawo, o którym mowa w ust. 1, nie może niekorzystnie wpływać na prawa i wolności innych.*

Artykuł 21 - Prawo do sprzeciwu

1. *Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f), w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw*

do przetwarzania, nadrzędnych wobec interesów, praw lub wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

2. *Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.*
3. *Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.*
5. *Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.*
6. *W związku z korzystaniem z usług społeczeństwa informacyjnego i bez uszczerbku dla dyrektywy 2002/58/WE osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.*
7. *Jeżeli dane osobowe są przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, osoba, której dane dotyczą, ma prawo wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych, chyba że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.*

10. Prawa pacjenta

Jakie prawa posiada pacjent na mocy przepisów regulujących świadczenie usług medycznych?

10.1 Prawo pacjenta do tajemnicy informacji z nim związanych

Prawo to zobowiązuje wszystkie osoby zatrudnione w MPM, które wykonują zawód medyczny i udzielają świadczenia zdrowotnego pacjentowi, do zachowania w tajemnicy informacji związanych z pacjentem. Ponadto do zachowania w tajemnicy obowiązane są także osoby pracujące w rejestracji, osoby zajmujące się statystyką medyczną/rozliczeniami z NFZ, informatycy oraz wszelkie osoby, które z upoważnienia administratora mają dostęp do informacji na temat pacjenta. Wszystkie powyższe osoby związane są tajemnicą także po śmierci pacjenta, z wyjątkiem sytuacji, o których mowa w przepisach prawa (częściowo omówionych poniżej).

10.2 Prawo do poszanowania intymności i godności pacjenta

Pacjent może zażyczyć sobie, żeby przy udzielaniu świadczeń zdrowotnych była obecna wskazana przez niego osoba bliska (np. żona, mąż, rodzice, dziadkowie). Prawo to wiąże się z możliwością przekazywania informacji jednocześnie pacjentowi jak i osobie trzeciej. W celu uniknięcia sytuacji, kiedy pacjent oskarżyłby lekarza lub pielęgniarkę o udzielenie informacji na temat swojego stanu zdrowia osobie bliskiej, lekarz lub pielęgniarka MPM odnotowują, jeszcze przed wprowadzeniem innych zapisów w dokumentacji medycznej, że na życzenie pacjenta towarzyszy mu osoba bliska, która tym samym będzie świadkiem przekazywania pacjentowi wszelkich informacji związanych z procesem jego leczenia.

Ponadto, w przypadku odmowy obecności osoby bliskiej przy udzielaniu świadczeń zdrowotnych (w przypadkach określonych w art. 21 ust. 2 UoPPiRPP), osoba wykonująca zawód medyczny odnotowuje ten fakt w dokumentacji medycznej.

10.3 Prawo pacjenta do dokumentacji medycznej

Pacjent, jego przedstawiciel ustawowy lub osoba upoważniona przez pacjenta, mają prawo uzyskać dostęp do dokumentacji medycznej w wybrany przez siebie sposób – na zasadach określonych w UoPPiRPP.

Za udostępnienie dokumentacji medycznej MPM może pobrać opłatę (z wyjątkami, o których mowa w p. 9.7 kodeksu). Wysokość tej opłaty:

- musi być określona bezpośrednio w regulaminie organizacyjnym (z uwzględnieniem kryteriów wskazanych w art. 28 ust. 4 UoPPiRPP);
- musi być podana do wiadomości pacjentów w miejscu udzielania świadczeń (wywieszenie informacji o opłatach w widocznym miejscu) i na stronie internetowej (jeżeli MPM taką posiada) oraz w Biuletynie Informacji Publicznej (jeżeli MPM obowiązana jest do jego prowadzenia).

10.4 Upoważnienie do dostępu do informacji lub dokumentacji medycznej

Pacjent ma prawo upoważnić wybraną przez siebie osobę lub osoby do:

- dostępu do dokumentacji medycznej pacjenta;
- uzyskiwania informacji medycznej o pacjencie.

Pacjent może także wskazać, że nie upoważnia nikogo – ani do dostępu do dokumentacji medycznej, ani do informacji medycznej.

Osoby upoważnione przez pacjenta do dokumentacji medycznej mogą także sięgać po nią po śmierci pacjenta (jeżeli pacjent przed śmiercią nie odwoła upoważnienia).

Zgodnie z art. 42 ust. 4 ustawy o zawodach lekarza i lekarza dentysty pacjent może ponadto upoważnić dowolną osobę trzecią (bez bliższego określania jej tożsamości) do odbioru tzw. recept zaocznych lub zleceń na zaopatrzenie w wyroby medyczne.

10.5 Sprzeciw wobec dostępu do informacji lub dokumentacji medycznej po śmierci pacjenta

Pacjent może sprzeciwić się, by po jego śmierci osoby bliskie pacjenta (wszystkie lub tylko niektóre) sięgały po jego dokumentację medyczną lub uzyskiwały od osób wykonujących zawód medyczny informacje medyczne. Pacjent może wyrazić sprzeciw w dowolny sposób, natomiast dla celów dowodowych taka informacja powinna być utrwalona na piśmie (przez samego pacjenta lub w postaci notatki służbowej sporządzonej przez pracownika MPM) i dołączona do dokumentacji medycznej pacjenta.

10.6 W jaki sposób może dochodzić do ograniczenia praw pacjenta?

10.6.1 Uchylenie tajemnicy informacji o pacjencie

Osoby wykonujące zawód medyczny, posiadające informacje o pacjencie, nie są zobowiązane do zachowania tajemnicy, jeżeli zachodzą sytuacje określone w przepisach prawa dotyczących poszczególnych zawodów medycznych (np. art. 40 ustawy o zawodach lekarza i lekarza dentysty), tzn. gdy:

- tak stanowią przepisy odrębnych ustaw;
- zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób;
- pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy, po uprzednim poinformowaniu o niekorzystnych dla pacjenta skutkach jej ujawnienia;
- zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innemu lekarzowi lub uprawionym osobom uczestniczącym w udzielaniu tych świadczeń lub innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu tych świadczeń;
- badanie lekarskie zostało przeprowadzone na żądanie uprawnionych, na podstawie odrębnych ustaw, organów i instytucji; wówczas lekarz jest obowiązany poinformować o stanie zdrowia pacjenta wyłącznie te organy i instytucje;
- ma miejsce postępowanie przed wojewódzką komisją do spraw orzekania zdarzeniach medycznych;
- zachodzi potrzeba przekazania przez lekarza niezbędnych informacji o pacjencie lekarzowi sądowemu.

10.6.2 Kiedy można odmówić obecności osoby bliskiej przy badaniu

Osoba wykonująca zawód medyczny udzielająca świadczeń zdrowotnych pacjentowi może odmówić obecności osoby bliskiej przy udzielaniu świadczeń zdrowotnych, w przypadku istnienia prawdopodobieństwa wystąpienia zagrożenia epidemicznego lub ze względu na bezpieczeństwo zdrowotne pacjenta. Odmowę odnotowuje się w dokumentacji medycznej.

10.6.3 Kiedy można przekazać pacjentowi oryginał jego dokumentacji medycznej

Oryginał dokumentacji medycznej może być przekazany pacjentowi jedynie w sytuacji, gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta (zgodnie z art. 27 ust. 1 p. 3 UoPPiRPP). Wskazać jednak należy, że stwierdzenie istnienia takiej przesłanki występuje nie po stronie wnioskodawcy, ale podmiotu wykonującego działalność leczniczą, będącego właścicielem tej dokumentacji. **W związku z tym tego rodzaju wnioski pacjentów powinny być załatwiane odmownie.**

Pacjent może natomiast otrzymać oryginał swojej dokumentacji medycznej na warunkach opisanych w:

- art. 29 ust. 2 UoPPiRPP, tj. w sytuacji, gdy MPM planuje zniszczenie jego dokumentacji medycznej w związku z upływem okresu jej przechowywania,
- art. 13b ust. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, tj. w sytuacji, w której MPM dokonała digitalizacji papierowej dokumentacji medycznej i planuje jej zniszczenie.

10.6.4 Kiedy sprzeciw pacjenta wobec ujawniania informacji lub dokumentacji medycznej nie będzie wiążący

Sprzeciw pacjenta, dotyczący dostępu osób bliskich do informacji lub dokumentacji medycznej po śmierci, nie będzie wiążący, jeżeli tak zadecyduje sąd (w postępowaniu toczącym się na wniosek osoby bliskiej zmarłego pacjenta).

Sąd może wyrazić zgodę na udostępnienie dokumentacji lub informacji medycznej i określić zakres jej udostępnienia, jeżeli jest to niezbędne:

- w celu dochodzenia odszkodowania lub zadośćuczynienia, z tytułu śmierci pacjenta;
- dla ochrony życia lub zdrowia osoby bliskiej.

Sąd, podejmując decyzję o tym, czy udostępnić dokumentację lub informację medyczną, bierze pod uwagę:

- interes uczestników postępowania (najczęściej uczestnikiem będzie osoba, która chce otrzymać dokumentację i osoba, która sobie tego nie życzy – np. skonfliktowane po śmierci ojca rodzeństwo);
- rzeczywistą więź osoby bliskiej ze zmarłym pacjentem (np. czy i jak córka opiekowała się matką przed śmiercią);
- wolę zmarłego pacjenta (np. czy mimo braku formalnego sprzeciwu nie było życzeniem pacjenta, by określona osoba nie miała dostępu do jego dokumentacji);
- okoliczności wyrażenia sprzeciwu (np. czy pacjent nie znajdował się pod wpływem leków mogących wpływać na jego świadomość).

11. Monitoring w MPM

Decyzję MPM o instalacji systemu monitoringu wizyjnego powinna zawsze poprzedzać analiza zasadności stosowania takiego rozwiązania. Taka analiza powinna obejmować w szczególności:

- obowiązujące przepisy prawa;
- analizę ryzyka związanego ze stosowaniem monitoringu;
- test równowagi z motywu 47 RODO.

11.1 Analiza zasadności stosowania monitoringu wizyjnego w MPM

11.1.1 Podstawy prawne monitoringu wizyjnego w MPM

W obecnym stanie prawnym dopuszczalny jest:

- monitoring zakładu pracy – na warunkach opisanych w Kodeksie pracy;
- monitoring pomieszczeń ogólnodostępnych MPM (korytarzy, poczekalni, wejść itp.) – na warunkach opisanych w UoDL;
- monitoring pomieszczeń, w których są udzielane świadczenia zdrowotne oraz pobytu pacjentów – jeśli wynika to z odrębnych przepisów prawa.

Ponieważ pomieszczenia, w których udziela się świadczeń zdrowotnych, lub w których przebywają pacjenci MPM, nie są aktualnie objęte przepisami prawa, w treści kodeksu opisane zostaną jedyne regulacje dotyczące monitoringu zakładu pracy i pomieszczeń ogólnodostępnych MPM.

Podstawą prawną z RODO dla monitorowania:

- zakładu pracy – jest zapewnienie bezpieczeństwa pracowników lub ochrony mienia (prawnie uzasadniony interes ADO - art. 6 ust. 1 lit. f w związku z art. 22[2] Kodeksu pracy),
- pomieszczeń ogólnodostępnych MPM (korytarzy, przestrzeni przed rejestracją, wejść do placówki itp.) – jest zapewnienie bezpieczeństwa pracowników, pacjentów lub ochrony mienia (prawnie uzasadniony interes ADO - art. 6 ust. 1 lit. f w związku z art. 23a ust. 1 pkt. 1 UoDL).

Powyższe oznacza, że MPM ma wolną wolę co do decyzji, czy używać monitoringu, czy nie (po przeprowadzeniu analizy ryzyka i testu równowagi). Jeżeli jednak zdecyduje się to robić, musi wypełniać obowiązki przewidziane przepisami prawa.

Mając na względzie wspomniany powyżej brak odrębnych przepisów prawa, monitoring w MPM nie może obejmować gabinetów lekarskich lub zabiegowych, toalet, szatni lub przebieralni.

11.1.2 Analiza ryzyka stosowania monitoringu wizyjnego w MPM

Przy analizie ryzyka, dokonywanej przed podjęciem decyzji o stosowaniu systemu monitoringu wizyjnego, należy w szczególności wziąć pod uwagę następujące zagadnienia:

- Obszar objęty monitoringiem (Czy zakres odpowiada wskazanemu w UoDL? Czy kamery nie obejmą zasięgiem sąsiednich ulic lub posesji?);
- Liczba wykorzystywanych kamer (Czy obejmą wszystkie kluczowe z punktu widzenia bezpieczeństwa obszary?);
- Istniejące zagrożenia, uzasadniające stosowanie monitoringu (Czy występują częste kradzieże, dewastacje, próby ataków fizycznych itp.?);
- Czy dla osiągnięcia tego samego celu można byłoby zastosować mniej inwazyjne środki bezpieczeństwa (np. współpracę z firmą ochroniarską). Jeśli nie – dlaczego;
- Gdzie będzie umieszczony rejestrator monitoringu (czy będzie to miejsce, do którego nie będą miały dostępu osoby nieupoważnione?);
- Kto z personelu MPM będzie miał dostęp do bieżącego obrazu z kamer;
- Kto z personelu MPM będzie miał dostęp do nagrań obrazu z kamer;
- Jak długo będą przechowywane nagrania z kamer;
- Jak będzie odbywał się dostęp do bieżącego obrazu lub nagrań (monitory w rejestracji? strona internetowa? aplikacja mobilna?);
- Czy w obsługę lub konserwację systemu będzie zaangażowana firma zewnętrzna?

11.1.3 Test równowagi przy stosowaniu monitoringu wizyjnego w MPM

Jak wskazano w p. 11.1.1 powyżej, podstawą z RODO dla prowadzenia monitoringu wizyjnego przez MPM jest prawnie uzasadniony interes MPM jako administratora. Oznacza to konieczność przeprowadzenia testu równowagi między dwiema kategoriami wartości:

- istniejącymi po stronie MPM i uzasadniającymi stosowanie monitoringu wizyjnego (zapewnienia bezpieczeństwa pacjentów i innych osób przebywających na terenie MPM) oraz
- istniejącymi po stronie osób przebywających na terenie MPM i uzasadniającymi rezygnację ze stosowana monitoringu wizyjnego (poczucie inwigilacji, naruszenie prywatności).

Przy realizacji testu bierze się pod uwagę w szczególności:

- istniejące powiązania między administratorem a osobami, których dane dotyczą (MPM oraz osobami przebywającymi na terenie MPM, które znalazłyby się w zasięgu kamer monitoringu);
- istnienie po stronie osób, których dane dotyczą, rozsądnych przesłanek, by spodziewać się, że może dochodzić do przekazania danych (osoby poddawane monitoringowi mają wiedzieć, że taka sytuacja ma miejsce; konieczne jest realizowanie obowiązków, o których mowa w p. 11.2 poniżej).

Jeżeli w wyniku przeprowadzonego testu okaże się, że:

- system monitoringu wizyjnego, który miałaby stosować MPM, nie będzie powodował naruszenia podstawowych praw lub wolności osób, których dane dotyczą oraz
- MPM jest w stanie to udowodnić (zgodnie z zasadą adekwatności).

Podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą.

Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz.

Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są

przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania.

Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego (motyw 47 RODO).

11.2 Informowanie o stosowaniu monitoringu wizyjnego w MPM

Przed rozpoczęciem stosowania monitoringu wizyjnego MPM musi poinformować o tym osoby, które mogą się znaleźć w zasięgu kamer. Sposób informowania określają:

- przepisy RODO (w szczególności art. 13 RODO);
- przepisy UoDL (w szczególności art. 24 ust. 2 UoDL);

Ponadto warto **uwzględnić wytyczne**, wskazane w treści:

- *Wytycznych 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo*, przygotowanych przez EROD[29];
- *Wskazówek Prezesa Urzędu Ochrony Danych Osobowych dotyczących wykorzystywana monitoringu wizyjnego*, przygotowanych przez Prezesa UODO[30].

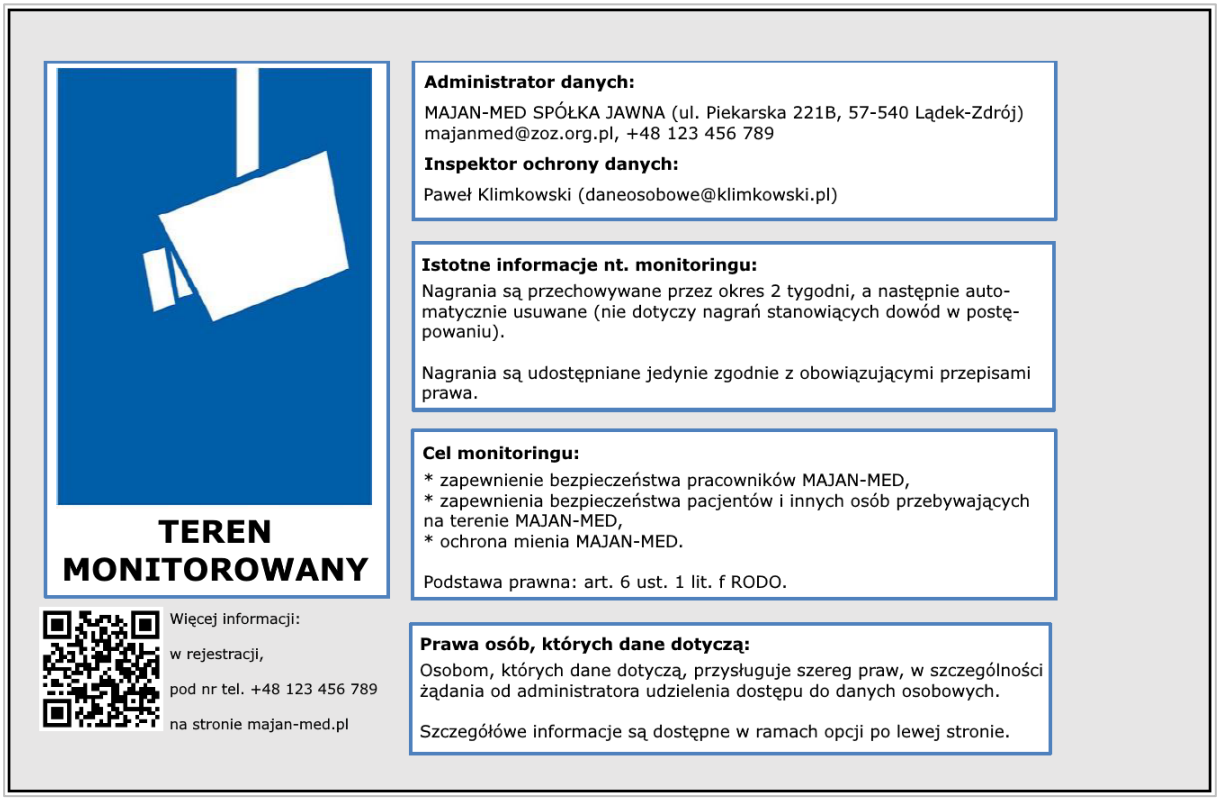
Realizacja obowiązku informacyjnego, związanego z monitoringiem wizyjnym, może odbywać się w sposób warstwowy:

1) warstwa pierwsza: podstawowe informacje o monitoringu, przekazane na piktogramach (tabliczkach, kartkach) umieszczonych przed wejściem na obszar monitoringu (np. na bramach lub drzwiach wejściowych);
2) warstwa druga: komplet informacji o monitoringu, dostępny w MPM
    a) w widoczny sposób w miejscu udzielania świadczeń (np. na tablicy ogłoszeń lub w rejestracji);
    b) na stronie internetowej MPM (jeżeli MPM ma taką stronę);
    c) w Biuletynie Informacji Publicznej MPM (jeżeli MPM jest zobowiązana do prowadzenia BIP-u).

[29] Guidelines 3/2019 on processing of personal data through video devices (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201903_video_devices_pl_0.pdf)

[30] https://uodo.gov.pl/pl/138/354

Poniżej zamieszczono przykład piktogramu monitoringu dla fikcyjnej MPM.



Rys. 1 Wzór piktogramu monitoringu na podstawie niewiążącego wzoru EROD.

11.3 Okres przechowywania nagrań z monitoringu wizyjnego w MPM

Przy określaniu czasu przechowywania nagrań przez placówki medyczne należy uwzględniać przede wszystkim cel, dla które one powstają.

Zgodnie z UoDL monitorowanie pomieszczeń ogólnodostępnych winno mieć miejsce, gdy jest niezbędne do zapewnienia bezpieczeństwa pacjentów lub pracowników pomieszczeń. Jako maksymalny okres przechowywania nagrania wskazano 3 miesiące od daty jego sporządzenia[31]. W praktyce MPM powinna jednak przechowywać nagrania przez krótszy okres – liczony raczej w tygodniach niż miesiącach – w celu zachowania zasady adekwatności. Efekt ten można osiągnąć w szczególności poprzez ustawienie pętli w rejestratorze, co spowoduje automatycznie nadpisywanie starszych nagrań. Należy pamiętać, że krótki okres przechowywania nagrań oznacza także mniej materiału wideo, wymagającego zabezpieczenia.

Nagrania można przechowywać dłużej niż 3 miesiące w szczególności w przypadku, kiedy są one dowodem w postępowaniu (np. kiedy policja poprosiła o zabezpieczenie nagrania).

[31] Art. 23a ust. 2 UoDL.

Z kolei maksymalny okres przechowywania nagrań z pomieszczeń medycznych określa przepis szczególny (taka sytuacja ma miejsce np. w przypadku nagrań z monitoringu izolatek, gdzie *zapis z monitoringu przechowuje się przez okres co najmniej 12 miesięcy od dnia jego zarejestrowania, nie dłużej jednak niż przez 13 miesięcy od dnia jego zarejestrowania, o ile nie zostanie on zabezpieczony jako dowód w sprawie w przypadku toczącego się postępowania*[32]).

11.4 Udostępnianie nagrań z monitoringu wizyjnego w MPM

Każda osoba, której dane dotyczą, ma prawo dostępu do swoich danych (oraz uzyskania kopii danych). W praktyce często zdarza się, że pacjent zwraca się do placówki o udostępnienie kopii nagrań, na których widać np. moment kradzieży roweru pacjenta czy też sprawcę zarysowań na aucie pacjenta. MPM, nie negując praw pacjentów w tym zakresie, powinien bardzo ostrożnie podchodzić do tego typu żądań. Należy bowiem pamiętać, że udostępnienie nagrań nie może naruszać praw innych osób, a z taką sytuacją będziemy mieli do czynienia kiedy na nagraniu utrwalony został również wizerunek innych osób[33].

W takiej sytuacji, kiedy na nagraniu można zidentyfikować również inne osoby, MPM może odmówić przekazania nagrania pacjentowi, wskazując na przykład na możliwość powiadomienia organów ścigania w sytuacji kiedy nagranie potrzebne jest pacjentowi do dochodzenia swoich praw – wtedy to te organy będą wnioskować o udostępnienie nagrań jako dowodu w sprawie.

Odmowa udostępnienia nagrania z powołaniem się na ochronę praw osób trzecich powinna mieć jednak miejsce jedynie w wyjątkowych sytuacjach. MPM powinien bowiem najpierw rozważyć – uwzględniając możliwości techniczne i organizacyjne stosowanego systemu monitoringu – wdrożenie odpowiednich środków technicznych umożliwiających przekazanie nagrania, z jednoczesną ochroną praw osób trzecich uwidocznionych na nagraniu. W ocenie unijnych organów ochrony danych, przykładem takich rozwiązań jest automatyczne lub manualne stosowanie technik maskowania (pikselizacji, zasłaniania, etc.) określonych obszarów na nagraniu[34], dzięki czemu możliwe jest zasłonięcie wizerunku osób trzecich uwidocznionych na nagraniu. Przykładem systemu umożliwiającego dokonanie takiej obróbki nagrania jest oprogramowanie *DaVinci Resolve* (dostępne zarówno w wersji odpłatnej, jak i darmowej).

Zanonimizowane w ten sposób nagranie może zostać bez przeszkód udostępnione wnioskodawcy – bez naruszania praw osób trzecich.

---

[32] Art. 18e ust. 6 ustawy z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego (Dz.U.2020.685 t.j.).

[33] Zgodnie z art. 15 ust. RODO, prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych.

[34] Wytyczne 3/2019 Europejskiej Rady Ochrony Danych w sprawie przetwarzania danych osobowych przez urządzenia wideo, s.24: https://uodo.gov.pl/pl/414/1332.

11.5 Inne kwestie związane z monitoringiem w MPM

11.5.1 Monitoring wizyjny na podstawie zgody pacjenta

Stosowanie monitoringu możliwe jest nie tylko w sytuacjach opisanych w 11.1.1 powyżej. Możliwa jest również sytuacja, kiedy pacjent wyrazi **zgodę** na nagrywanie (zgodnie z np. art. 6 ust. 1 lit a oraz np. art. 9 ust. 2 lit. a RODO w przypadku szczególnych kategorii danych), np. w sytuacji kiedy monitoringiem objęty jest (na czas wizyty pacjenta) gabinet zabiegowy, a wspomniany pacjent miał możliwość wyrażenia zgody na takie nagrywanie przed zabiegiem.

Ta wyjątkowa sytuacja przetwarzania danych w praktyce najczęściej występuje, gdy MPM potrzebuje nagrań do celów naukowych lub dydaktycznych. Ważne, by ten cel został szczegółowo określony w treści zgody pacjenta. MPM zbiera w takim przypadku pisemne oświadczenia, które zapewniają w największym wymóg zachowania wyraźnej formy zgody na przetwarzania danych o stanie zdrowia.

Dobrą praktyką w tym aspekcie jest również nagrywanie jak najmniejszego obszaru (np. jeżeli pacjent otrzymuje zastrzyk w udo, nie ma konieczności nagrywania jego twarzy).

Nagranie, dokonane na podstawie zgody pacjenta, jest przechowywane do momentu ewentualnego wycofania zgody przez tego pacjenta.

11.5.2 Atrapy kamer monitoringu wizyjnego

MPM nie może stosować atrap kamer monitoringu wizyjnego.

Najwyższa Izba Kontroli, w informacji o wynikach kontroli dotyczącej ochrony intymności i godności pacjentów w szpitalach, uznała za nieprawidłowość umieszczanie atrap kamer, stwierdzając jednocześnie, że takie działanie może wzbudzać u pacjentów poczucie ingerencji w sferę ich prywatności, a także powodować błędne poczucie bezpieczeństwa[35].

Takie stanowisko wyraził również Prezes Urzędu Ochrony Danych Osobowych:

> *Stanowisko organu do spraw ochrony danych osobowych jest w tej kwestii niezmienne – stosowanie atrap powinno być zakazane. Atrapy kamer z jednej strony wprowadzają u potencjalnie monitorowanych poczucie ingerencji w sferę prywatności, a z drugiej mylne poczucie zwiększonego bezpieczeństwa.*
> *Niepożądane skutki związane z wykorzystaniem monitoringu, także z atrapami kamer, czy to w otwartej przestrzeni (...) czy też w zamkniętej (...) mogą przeważać nad ewentualnymi korzyściami wynikającymi z ich stosowania i tym samym podawać w wątpliwość skuteczność i adekwatność tego narzędzia w realizacji zamierzonego celu w danych okolicznościach* (*Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego*[36]).

[35] Informacje o wynikach kontroli „Ochrona intymności i godności pacjentów w szpitalach" (https://www.nik.gov.pl/plik/id,16805,vp,19361.pdf), s. 12.
[36] https://uodo.gov.pl/pl/file/1200, s. 19.

11.5.3 Monitoring dźwiękowy w MPM

MPM nie może stosować monitoringu dźwiękowego.

UoDL nie przewiduje takiej formy obserwacji pomieszczeń, ponadto Prezes UODO uznał ją za nadmiarową formę przetwarzania danych[37].

Stosowanie rejestracji dźwięku może wiązać się w związku z tym z odpowiedzialnością administracyjną i cywilną, a nawet karną.

12. Teleporady

Szczególną formą działalności MPM jest realizacja świadczeń, udzielanych na odległość przy użyciu systemów teleinformatycznych lub systemów łączności, czyli tzw. **teleporad**.

W zakresie ochrony danych osobowych przy realizacji teleporad istotne jest, aby MPM zadbała o:

- identyfikację pacjentów korzystających z teleporad;
- bezpieczne warunki udzielania teleporad;
- odpowiednie zabezpieczenia techniczne przy realizacji teleporad[38].

12.1 Identyfikacja pacjentów korzystających z teleporad

12.1.1 Pacjenci znani MPM

Zakres danych dla weryfikacji tożsamości

Potwierdzenia tożsamości pacjenta należy dokonać na podstawie danych osobowych, wskazanych w art. 25 ust. 1 p. 1 UoPPiRPP:

- nazwisko i imię (imiona);
- data urodzenia;
- oznaczenie płci;
- adres miejsca zamieszkania;
- numer PESEL, jeżeli został nadany:

[37] https://uodo.gov.pl/pl/file/1200, s. 26.

[38] Rekomendowane rozwiązania w tym względzie zawierają również „Wytyczne dotyczące realizacji prawa do informacji przez osoby uprawnione na odległość" przygotowane przez Rzecznika Praw Pacjenta oraz Prezesa Urzędu Ochrony Danych Osobowych: https://uodo.gov.pl/pl/138/1787.

- w przypadku noworodka – numer PESEL matki;
- w przypadku osób, które nie mają nadanego numeru PESEL – rodzaj i numer dokumentu potwierdzającego tożsamość;

– nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania (w przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody).

Źródła danych do weryfikacji tożsamości

Po stronie MPM

Źródłem danych do weryfikacji tożsamości pacjenta po stronie MPM jest, w zależności od sytuacji:

– dokumentacja medyczna;

– deklaracja wyboru lekarza, pielęgniarki lub położnej POZ;

– Internetowe Konto Pacjenta.

Po stronie pacjenta

Źródłem danych do weryfikacji tożsamości po stronie pacjenta jest:

– jego dokument potwierdzający tożsamość, okazany w trakcie teleporady (jeśli teleporada odbywa się z wykorzystaniem połączenia wideo);

– sam pacjent, który przekazuje informacje na swój temat osobie udzielającej teleporady (w razie wątpliwości co do tożsamości należy zadać dodatkowe pytania, wskazane poniżej).

Weryfikacja tożsamości pacjenta na podstawie okazania – w trakcie realizacji wideoporady – dokumentu potwierdzającego tożsamość nie jest dopuszczalna w sytuacji, gdy wideoporada jest nagrywana. MPM nie ma podstaw prawnych do utrwalania i przechowywania obrazu takiego dokumentu. Jeżeli warunki techniczne na to pozwalają, nagrywanie wideoporady należy przerwać na czas okazywania dokumentu potwierdzającego tożsamość.

Dodatkowe pytania w razie wątpliwości co do tożsamości pacjenta

W razie wątpliwości co do tożsamości pacjenta kontaktującego się z MPM, należy zadać trzy pytania, spełniające poniższe kryteria:

– pacjent zna odpowiedzi na te pytania;

– MPM zna odpowiedzi na te pytania;

– odpowiedzi na te pytania nie są znane osobom nieupoważnionym.

W związku z powyższym można prosić pacjenta np. o:

- podanie nazwiska lekarza, do którego złożył deklarację wyboru lub był na ostatniej wizycie;
- wskazanie daty ostatniej wizyty;
- informację o lekach lub badaniach z ostatniej wizyty lekarskiej.

12.1.2 Pacjenci nieznani MPM

W sytuacji, w której z MPM kontaktuje się osoba, która nie była jej pacjentem i nie korzystała wcześniej z jej usług, nie występuje ryzyko, że osoba nieupoważniona uzyska dostęp do informacji nt. stanu zdrowia pacjenta, ponieważ MPM nie posiada takich informacji.

Z tego względu dopuszczalne jest postępowanie, zgodnie z którym:

- dane osobowe pacjenta są dokumentowane na podstawie jego oświadczenia;
- formalna weryfikacja tożsamości następuje przy okazji najbliższej osobistej wizyty pacjenta w MPM.

Wstępna weryfikacja tożsamości pacjenta nieznanego MPM następuje na podstawie informacji przekazanych przez pacjenta osobie udzielającej teleporady w celu dokonania sprawdzenia w systemie eWUŚ[39] (imię, nazwisko i PESEL pacjenta).

Jeżeli pacjent jest osobą ubezpieczoną – osoba udzielająca teleporady prosi pacjenta o podanie pozostałych informacji, niezbędnych dla założenia dokumentacji medycznej, tj. płci, daty urodzenia i adresu zamieszkania.

Jeżeli pacjent nie jest osobą ubezpieczoną lub jego weryfikacja w systemie eWUŚ nie jest możliwa – osoba udzielająca teleporady prosi pacjenta o złożenia oświadczenia, że:

- jest osobą ubezpieczoną – w przypadku świadczeń finansowanych przez NFZ;
- podane przez niego dane są prawidłowe.

Oświadczenie takie należy zanotować, opatrzyć podpisem osoby udzielającej teleporady i dołączyć do dokumentacji medycznej pacjenta (w przypadku dokumentacji elektronicznej należy zeskanować oświadczenie, a papierowy dokument przechowywać w odrębnym segregatorze).

[39] eWUŚ (Elektroniczna Weryfikacja Uprawnień Świadczeniobiorców) to system umożliwiający natychmiastowe potwierdzenie prawa pacjenta do świadczeń opieki zdrowotnej finansowanych ze środków publicznych.

12.2 Warunki udzielania teleporad

Przy udzielaniu teleporad MPM powinien pamiętać o realizacji następujących warunków

- świadczenia udzielane zdalnie odbywają się w miejscu, gdzie nie będzie możliwe podsłuchanie rozmowy telefonicznej / podsłuchanie wideorozmowy / podejrzenie ekranu przez osoby nieupoważnione; zdalne udzielanie świadczeń powinno mieć miejsce w oddzielnym, zamykanym pomieszczeniu, do którego nie mają dostępu pacjenci lub inne osoby postronne;
- jeżeli teleporada jest nagrywana, pacjent musi być o tym poinformowany przed jej rozpoczęciem;
- przekazywanie informacji pocztą elektroniczną ma odbywać się za pośrednictwem skrzynki poczty elektronicznej, do której nie mają dostępu osoby nieupoważnione i której zabezpieczenia zostały uprzednio skonsultowane z informatykiem oraz inspektorem ochrony danych (IOD).

12.3 Zabezpieczenia techniczne przy realizacji teleporad

W celu zapewnienia, by przekazywanie informacji w ramach teleporad odbywało się w sposób zapewniający ich integralność oraz ochronę przed nieuprawnionym wykorzystaniem, przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem, MPM powinna wykorzystywać rozwiązania techniczno-organizacyjne uprzednio konsultowane z:

- informatykiem lub firmą IT (pod kątem zabezpieczeń technicznych) oraz
- IOD (pod kątem spełnienia wymagań związanych z ochroną danych osobowych i bezpieczeństwem informacji).

13. Spisy

13.1 Spis załączników

13.2 Spis tabel

13.3 Spis wykresów

13.4 Spis ilustracji

Okres przechowywania dokumentacji medycznej

(stan na dzień 31.10.2022 r.).

Dokumentacja medyczna	Okres (w latach)	Sposób liczenia terminu	Podstawa prawna
Deklaracja wyboru lekarza / pielęgniarki / położnej POZ (wycofana przed 09.07.2014 r.)	10	od dnia, w którym deklaracja przestała być podstawą rozliczeń (np. wycofania deklaracji)	ustawa z dnia 13 kwietnia 2018 r. o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw
Deklaracja wyboru lekarza / pielęgniarki / położnej POZ (wycofana między 09.07.2014 r. a 08.07.2018 r.)	6	od dnia 9 lipca 2018 r.	ustawa z dnia 13 kwietnia 2018 r. o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw
Deklaracja wyboru lekarza / pielęgniarki / położnej POZ (wycofane od 09.07.2018 r.)	6	od dnia, w którym deklaracja przestała być podstawą rozliczeń (np. wycofania deklaracji)	art. 118 Kodeksu cywilnego
Dokumentacja medyczna (np. historia choroby lub księgi gabinetu zabiegowego)	20	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 ustawy o prawach pacjenta[40]
Dokumentacja dotycząca dzieci do ukończenia 2. roku życia	22	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 pkt. 4 ustawy o prawach pacjenta
Dokumentacja medyczna (w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia)	30	od końca roku kalendarzowego, w którym nastąpił zgon	art. 29 ust. 1 pkt. 1 ustawy o prawach pacjenta

[40] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

Dokumentacja medyczna zawierająca dane niezbędne do monitorowania losów krwi i jej składników	30	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 pkt. 1a ustawy o prawach pacjenta
Kupony RUM (jeśli informacja o świadczeniach zdrowotnych została wprowadzona do indywidualnej lub zbiorowej dokumentacji medycznej)	6	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 118 Kodeksu cywilnego
Kupony RUM (jeśli są jedynym zapisem dotyczącym wykonanych świadczeń zdrowotnych, a tym samym stanowią część dokumentacji medycznej)	20	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 ustawy o prawach pacjenta
Księga przyjęć	20	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 ustawy o prawach pacjenta
Skierowanie zrealizowane	5	od końca roku kalendarzowego, w którym realizowano skierowanie	art. 29 ust. 1 pkt. 3 lit. a ustawy o prawach pacjenta
Skierowania niezrealizowane	2	od końca roku kalendarzowego, w którym wystawiono skierowanie, jeśli pacjent nie odebrał skierowania	art. 29 ust.1 pkt. 3 lit. b ustawy o prawach pacjenta
Zdjęcia rentgenowskie przechowywane poza dokumentacją medyczną pacjenta	10	od końca roku kalendarzowego, w którym wykonano zdjęcie	art. 29 ust. 1 pkt. 2 ustawy o prawach pacjenta
Zlecenia lekarza	5	od końca roku kalendarzowego, w którym realizowano zlecenie	art. 29 ust. 1 pkt. 3 lit. a ustawy o prawach pacjenta
ZUS ZLA (L4)	3	od końca roku kalendarzowego, w którym wystawiono dokument	art. 58 ust. 1 pkt 3 ustawy o świadczeniach z ubezpieczenia społecznego[41]

[41] Ustawa z dnia 25 czerwca 1999 r. o świadczeniach pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa (w brzmieniu sprzed dnia 1 stycznia 2016 r.)

MEDYCYNA PRACY			
Dokumentacja pracowników narażonych na działanie substancji chemicznych, ich mieszanin, czynników lub procesów technologicznych o działaniu rakotwórczym lub mutagennym, o których mowa w rozporządzeniu ws. szkodliwych czynników rakotwórczych lub mutagennych[42]	40	od ustania narażenia na działanie substancji chemicznych, ich mieszanin, czynników lub procesów technologicznych o działaniu rakotwórczym lub mutagennym	§ 5 ust. 1 rozporządzenia ws. szkodliwych czynników rakotwórczych lub mutagennych
Dokumentacja badań i orzeczeń psychologicznych (służba medycyny pracy)	20	od dnia 31 grudnia roku kalendarzowego, w którym dokonano ostatniego wpisu	§ 5 ust. 2 rozporządzenia w sprawie rodzajów dokumentacji badań i orzeczeń psychologicznych[43]
Pozostała dokumentacja medyczna służby medycyny pracy	20	od końca roku kalendarzowego, w którym dokonano ostatniego wpisu	art. 29 ust. 1 ustawy o prawach pacjenta w związku z art. 11 ustawy o służbie medycyny pracy[44]

Po upływie okresu przechowywania, wynikającego z powyższej tabeli, obowiązkiem placówki medycznej jest zniszczenie dokumentacji medycznej w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła (art. 29 ust. 2 zd. 1 ustawy o prawach pacjenta).

Dokumentacja medyczna przeznaczona do zniszczenia może być także wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta (art. 29 ust. 2 zd. 2 ustawy o prawach pacjenta).

[42] Rozporządzenie Ministra Zdrowia z dnia 24 lipca 2012 r. w sprawie substancji chemicznych, ich mieszanin, czynników lub procesów technologicznych o działaniu rakotwórczym lub mutagennym w środowisku pracy.

[43] Rozporządzenie Ministra Zdrowia z dnia 14 lipca 2010 r. w sprawie rodzajów dokumentacji badań i orzeczeń psychologicznych, sposobu jej prowadzenia, przechowywania i udostępniania oraz wzorów stosowanych dokumentów.

[44] Ustawa z dnia 27 czerwca 1997 r. o służbie medycyny pracy.