POLITYKA OCHRONY DANYCH OSOBOWYCH PODMIOTU LECZNICZEGO PROKIDS AND FAMILY CARE SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ

Spis treści

1. Wstęp

1.1. Niniejsza polityka ochrony danych osobowych jest dokumentem opisującym sposób przetwarzania danych osobowych oraz obowiązki podmiotu leczniczego działającego w charakterze administratora danych osobowych, przetwarzanych w związku z prowadzoną działalnością leczniczą.

1.2. Niniejsza polityka poddawana jest bieżącej aktualizacji, nie rzadziej niż raz do roku.

1.3. Słownik:

* administrator - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem niniejszej polityki jest PROKIDS AND FAMILY CARE spółka z ograniczoną odpowiedzialnością, z siedzibą w Krakowie, przy ul. Ruczaj 43/U2A (kod pocztowy: 30-409), wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla Krakowa Śródmieścia w Krakowie, XI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0001081768, NIP: 6762660790, REGON: 527508101, z kapitałem zakładowym w wysokości 30 000 zł;

* dane dotyczące zdrowia - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej - w tym o korzystaniu z usług opieki zdrowotnej - ujawniające informacje o stanie jej zdrowia; do danych o stanie zdrowia należą także informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, takie jak w szczególności: numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych;

* dane osobowe (dane) - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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;

* Inspektor Ochrony Danych (IOD) - inspektor w rozumieniu art. 37 Rozporządzenia;

* naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

* odbiorca - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny

podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; nie są odbiorcami organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego;

* podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

* przetwarzanie - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taki jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

* Rozporządzenie (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;

* UODO (Urząd Ochrony Danych Osobowych) - organ publiczny powołany w celu ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych

2. Zasady przetwarzania danych osobowych

2.1. Administrator przetwarza dane osobowe z poszanowaniem poniższych zasad:

* legalność - posiada odpowiednią podstawę prawną przetwarzania danych i na niej opiera to przetwarzanie;

* rzetelność i prawidłowość - dba o aktualność danych oraz ich poprawność;

* przejrzystość - przetwarza dane w sposób przejrzysty dla osoby, której dane dotyczą (w szczególności poprzez informowanie o przetwarzaniu danych);

* celowość - przetwarza dane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza danych w sposób niezgodny z tymi celami;

* adekwatność - dane są stosowne do celu, w jakim zostały zebrane;

* minimalizacja - dane są przetwarzane w zakresie niezbędnym do celu, w jakim zostały pozyskane;

* ograniczenie przechowywania - dane przechowywane są przez okres nie dłuższy, niż jest to niezbędne do celów w jakim dane osobowe zostały pozyskane;

* integralność i poufność - dba o bezpieczeństwo danych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową

utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;

2.2. Administrator zapewnia rozliczalność - jest w stanie wykazać przestrzeganie wszystkich zasad, o których mowa w pkt 2.1, w szczególności poprzez stosowanie odpowiednich polityk oraz procedur.

3. Podstawy prawne przetwarzania danych osobowych

3.1. Działalność administratora jako podmiotu leczniczego regulują w szczególności:

* ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta;
* ustawa o działalności leczniczej;
* ustawa o służbie medycyny pracy;
* ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi;
* ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
* ustawa o zawodach lekarza i lekarza dentysty;
* rozporządzenie Ministra Zdrowia w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą;
* rozporządzenie Ministra Zdrowia w sprawie rodzajów dokumentacji medycznej służby medycyny pracy, sposobu jej prowadzenia i przechowywania oraz wzoru stosowanych dokumentów;
* rozporządzenie Ministra Zdrowia w sprawie rodzajów i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

3.2. Jako podmiot leczniczy, administrator przetwarza dane osobowe w celach zdrowotnych na podstawie art. 9 ust. 2 lit. h Rozporządzenia.

3.3. Przez cele zdrowotne rozumie się:

* profilaktykę zdrowotną - w szczególności poprzez informowanie pacjentów o możliwości pobierania świadczeń zdrowotnych, przekazywanie materiałów edukacyjnych,
* medycynę pracy oraz ocenę zdolności pracownika do pracy - w szczególności poprzez sprawowanie zadań jednostki służby medycyny pracy, w tym poprzez badania wstępne, okresowe oraz kontrolne na podstawie umowy zawartej pomiędzy administratorem a pracodawcą,
* diagnozę medyczną oraz leczenie - w szczególności poprzez udzielanie świadczeń zdrowotnych oraz prowadzenie dokumentacji medycznej,
* zapewnienie opieki zdrowotnej oraz zarządzanie systemami opieki zdrowotnej

- w szczególności poprzez: rejestrację pacjenta do usług administratora, odbieranie oraz archiwizację oświadczeń pacjentów wynikających z realizacji ich praw pacjenta, wykorzystywanie i utrzymywanie infrastruktury informatycznej służącej wspieraniu procesu leczenia, rozliczanie udzielonych świadczeń, wymianę danych osobowych pacjenta z innym podmiotem leczniczym w ramach zachowania ciągłości leczenia.

3.4. W zakresie wykraczającym poza cele zdrowotne administrator przetwarza dane na podstawie:

* zgody pacjenta (art. 6 ust. 1 lit. a Rozporządzenia) - w celach marketingowych

* prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia) - w celu dochodzenia roszczeń i obrony przed roszczeniami.

3.5. Zgoda, o której mowa w pkt 3.4.1. jest dobrowolna i jej wyrażenie jest świadomym działaniem pacjenta. Nieudzielenie zgody nie powoduje dla pacjenta żadnych negatywnych konsekwencji, w szczególności nie skutkuje odmową udzielenia świadczenia zdrowotnego ani nie warunkuje udzielenia tego świadczenia.

4. Obowiązki administratora

Środki organizacyjne i techniczne

4.1. Administrator stosuje środki techniczne oraz organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych, z uwzględnieniem stanu wiedzy technicznej, kosztu wdrożenia, charakteru, zakresu, kontekstu i celu przetwarzania, ryzyka naruszenia praw lub wolności o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. W szczególności administrator stosuje w tym celu:

* pseudonimizację oraz szyfrowanie danych;

* środki zapewniające poufność, integralność, dostępność danych oraz odporność systemów i usług przetwarzania;

* środki zapewniające szybkie przywrócenie dostępności danych osobowych i dostęp do nich w razie incydentu fizycznego lub technicznego;

* regularne testowanie, mierzenie i ocenę skuteczności tych środków.

4.2. Administrator prowadzi dokumentację opisującą sposób przetwarzania danych osobowych oraz sposób ich zabezpieczenia, w szczególności w postaci polityk, procedur, wytycznych oraz formularzy.

4.3. Administrator dopuszcza do przetwarzania danych osobowych jedynie osoby upoważnione przez administratora, które złożyły oświadczenie o zachowaniu danych oraz sposobu ich zabezpieczeń w poufności. Obowiązek złożenia oświadczenia nie dotyczy osób zobowiązanych do zachowania tajemnicy zawodowej, w szczególności personel medyczny (lekarze, pielęgniarki).

4.4. Administrator prowadzi rejestr osób upoważnionych oraz przechowuje treść oświadczeń, o których mowa w pkt 4.3.

4.5. Administrator opracował oraz wdrożył procedury gwarantujące ochronę prywatności na etapie powstawania nowych projektów, inwestycji oraz zmian w prowadzonych przez administratora procesach z udziałem danych osobowych.

4.6. Administrator regularnie szkoli personel posiadający dostęp do danych i podnosi jego wiedzę w zakresie bezpieczeństwa danych osobowych.

Rejestr czynności przetwarzania

4.7. Administrator prowadzi rejestr czynności przetwarzania. Rejestr ten prowadzony jest w formie elektronicznej.

4.8. Rejestr czynności przetwarzania administratora zawiera:

* imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także przedstawiciela administratora oraz inspektora ochrony danych;
* określenie celu przetwarzania;
* opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
* opis kategorii odbiorców, który dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach poza Unią Europejską lub w organizacjach międzynarodowych;
* jeżeli dane przekazywane są do państw poza Unię Europejską lub do organizacji międzynarodowych - nazwę tego państwa lub organizacji oraz dokumentację odpowiednich zabezpieczeń;
* planowane terminy usunięcia poszczególnych kategorii danych (jeżeli możliwe jest ich wskazanie);
* ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w pkt 4.1.1.

4.9. Rejestr czynności przetwarzania jest na bieżąco aktualizowany i udostępniany przez administratora na każde żądanie Urzędu Ochrony Danych Osobowych.

Ocena skutków dla ochrony danych

4.10. Administrator dokonuje oceny skutków dla ochrony danych i dokumentuje fakt dokonania tej oceny.

4.11. Wykonanie oceny skutków dla ochrony danych jest konieczne, 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 i wolności pacjentów. Dla podobnych operacji przetwarzania wiążących się z podobnym wysokim ryzykiem ocena skutków dla ochrony danych wykonywana jest pojedynczo.

4.12. Wykonanie oceny skutków dla ochrony danych osobowych wymaga w szczególności:

* systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie wykorzystującego elementy rozpoznawania cech lub właściwości obiektów znajdujących się w monitorowanej przestrzeni, z użyciem danych pacjentów, prowadzonego przez szpital, podmiot prowadzący badania kliniczne lub pobierający materiał genetyczny do badań;

* przetwarzania na dużą skalę informacji o stanie zdrowia, w szczególności dokonywane przez szpital lub placówkę medyczną.

4.13. Administrator monitoruje wykaz rodzajów przetwarzania, dla których wymagane jest przeprowadzenie oceny skutków dla ochrony danych opublikowany przez Urząd Ochrony Danych Osobowych i dokonuje oceny skutków czynności przetwarzania wskazanych w tym wykazie jako rekomendowanych do poddania tej ocenie.

4.14. Ocena skutków dla ochrony danych osobowych zawiera co najmniej:

* systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;

* ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celu, w jakim dane zostały pozyskane;

* ocenę ryzyka naruszenia praw i wolności pacjentów;

* środki planowane w celu mitygacji ryzyka, w tym zabezpieczenia, środki i mechanizmy bezpieczeństwa zapewniające ochronę danych oraz wykazanie przestrzegania przepisów Rozporządzenia.

4.15. Administrator dokonuje bieżącego przeglądu czynności przetwarzania, celem weryfikacji, czy przetwarzanie to odbywa się w sposób zgodny z dokonaną oceną skutków dla ochrony danych osobowych.

4.16. Administrator konsultuje się z Urzędem Ochrony Danych Osobowych, jeżeli dokonana ocena skutków dla ochrony danych będzie wskazywała na występowanie wysokiego ryzyka dla praw i wolności pacjentów, jeżeli nie zastosowane zostałyby środki mitygujące ryzyko. Konsultacje z UODO dokonywane są przed rozpoczęciem przetwarzania danych osobowych.

Inspektor ochrony danych

4.17. Administrator jako podmiot leczniczy zobowiązany jest do wyznaczenia inspektora ochrony danych osobowych, w szczególności jeżeli:

* jego główna działalność polega na przetwarzaniu na dużą skalę danych szczególnej kategorii (danych o stanie zdrowia);

* jest podmiotem publicznym (w szczególności samodzielnym publicznym

zakładem opieki zdrowotnej).

4.18. Administrator wyznaczył inspektora ochrony danych i dokonał zawiadomienia o wyznaczeniu inspektora do Urzędu Ochrony Danych Osobowych.

4.19. Inspektor ochrony danych został wyznaczony na podstawie jego kwalifikacji zawodowych, w tym wiedzy oraz zdobytego doświadczenia, które to kwalifikacje zostały udokumentowane.

4.20. Administrator stwarza inspektorowi ochrony danych odpowiednie warunki, aby mógł realizować swoje obowiązki, w szczególności poprzez:

* niezwłoczne oraz odpowiedne włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych,

* zapewnienie zasobów niezbędnych do wykonywania jego zadań oraz utrzymania jego fachowej wiedzy,

* zapewnienie mu niezależności w sprawowaniu jego funkcji, m.in. poprzez niewydawanie instrukcji dotyczących wykonywania przez niego jego zadań, nieponoszenie przez inspektora negatywnych konsekwencji za wypełnianie przez niego jego zadań, zapewnienie odpowiedniej struktury organizacyjnej aby podlegał jedynie najwyższemu kierownictwu.

4.21. Zadania inspektora ochrony danych obejmują w szczególności:

* podnoszenie świadomości wśród personelu przetwarzającego dane osobowe oraz podmiotów przetwarzających dane osobowe na zlecenie administratora, poprzez realizację szkoleń oraz informowanie o obowiązkach spoczywających na tych osobach i podmiotach;

* monitorowanie przestrzegania przez Administratora przepisów Rozporządzenia i innych przepisów prawa ochrony danych osobowych oraz regulacji wewnętrznych przyjętych u administratora regulujących kwestie związane z przetwarzaniem danych osobowych;

* wykonywanie audytów w kwestiach związanych z przetwarzaniem danych osobowych;

* uczestniczenie oraz wspieranie administratora w dokonywaniu oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny tych skutków;

* współpraca z Urzędem Ochrony Danych Osobowych;

* sprawowanie funkcji punktu kontaktowego dla pacjentów w kwestiach związanych z przetwarzaniem danych osobowych.

Powierzenie przetwarzania danych osobowych

4.22. Administrator może korzystać z usług podmiotów zewnętrznych w celu wspierania administratora w jego bieżącej działalności, w szczególności polegających na dostarczeniu oraz/lub utrzymaniu infrastruktury teleinformatycznej,

w tym narzędzi wspierających administratora w prowadzeniu dokumentacji medycznej w formie elektronicznej.

4.23. Administrator korzysta wyłącznie z usług takich dostawców usług, którzy zapewniają odpowiednie gwarancje bezpieczeństwa danych osobowych i zgodności przetwarzania danych z przepisami Rozporządzenia.

4.24. Administrator dokonuje weryfikacji podmiotu przetwarzającego przed dokonaniem wyboru takiego podmiotu, jak również dokonuje jego późniejszej, okresowej weryfikacji, zgodnie z przyjętą u administratora procedurą, weryfikacja jest dokumentowana.

4.25. Administrator zawiera z podmiotem przetwarzającym umowę powierzenia przetwarzania danych osobowych lub reguluje okoliczność powierzenia przetwarzania danych innym instrumentem prawnym, w której określone zostają obowiązki podmiotu przetwarzającego wynikające z faktu powierzenia.

4.27. Administrator nie przekazuje danych osobowych do państw poza terenem Unii Europejskiej.

5. Obowiązki personelu

5.1. Dostęp do danych osobowych pacjentów posiada personel medyczny (lekarze oraz pielęgniarki) oraz inne osoby podczas wykonywania czynności pomocniczych niezbędnych przy udzielaniu świadczeń zdrowotnych, adekwatnie do ich obowiązków służbowych.

5.2. Personel administratora zobowiązany jest do:

* zapoznania się oraz stosowania przepisów prawa w zakresie ochrony danych osobowych, w tym Rozporządzenia;

* ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem do tych danych, ich nieuzasadnioną modyfikacją lub zniszczeniem;

* niszczenia w bezpieczny sposób wszelkich nośników zawierających dane osobowe (w formie papierowej jak i elektronicznej);

* korzystania z zasobów informatycznych oraz sprzętu w sposób zgodny z ich przeznaczeniem i w sposób bezpieczny, m.in. poprzez okresową zmianę haseł, zachowanie poufności loginów i haseł oraz niepozostawianie sprzętu bez nadzoru;

* niezwłocznego informowania przełożonych o zaobserwowanych nieprawidłowościach, które mogą mieć wpływ na bezpieczeństwo przetwarzanych danych osobowych;

* przechowywania dokumentacji zawierającej dane osobowe w przeznaczonych do tego miejscach, z ograniczonym dostępem osób trzecich, zwłaszcza dokumentacji medycznej pacjentów;

* niepozostawiania stanowisk recepcyjnych/punktów rejestracji pacjenta bez nadzoru.

5.3. Personel ponosi odpowiedzialność za należyte wykonywanie swoich obowiązków i jest on pouczony przez administratora o sankcjach wynikających z nieprawidłowości w tym zakresie, w tym o odpowiedzialności karnej.

6. Prawa osób, których dane dotyczą

6.1. Administrator przetwarza dane osobowe z poszanowaniem praw pacjenta oraz praw osób, których dane dotyczą wynikających z Rozporządzenia.

6.2. Administrator prowadzi rejestr zgłoszonych żądań, przez osoby, których danych dotyczą.

6.3. Przed wykonaniem praw osoby, której dane dotyczą administrator dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia, czy żądanie pochodzi od osoby uprawnionej.

6.4. Administrator zapewnia odpowiednie zaplecze techniczne oraz kadrowe w celu terminowej oraz rzetelnej realizacji praw osoby, której dane dotyczą. Zgłoszone żądania realizowane są przez administratora niezwłocznie, nie później niż w terminie miesiąca od otrzymania żądania. W przypadku niemożności wykonania żądania w w/ w terminie, z uwagi na skomplikowany charakter sprawy, administrator kontaktuje się z pacjentem i informuje go o przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania pacjenta.

Prawo do informacji

6.5. Pacjenci są informowani przez administratora o sposobie przetwarzania ich danych osobowych oraz przysługującym ich uprawnieniach w formie noty informacyjnej, z którą mogą zapoznać się w każdej chwili w siedzibie administratora, jego jednostkach organizacyjnych oraz na stronie internetowej.

6.6. Nota informacyjna jest sporządzona prostym językiem, w sposób przejrzysty i wyczerpuje wszystkie informacje zgodnie z art. 13 oraz 14 Rozporządzenia.

Prawo dostępu do danych

6.7. Na żądanie pacjenta administrator udziela mu informacji o sposobie przetwarzania jego danych osobowych.

6.8. Na żądanie pacjenta administrator udostępnia mu nieodpłatnie pierwszą kopię jego danych osobowych, w tym zawierającą jego dokumentację medyczną; za każdą kolejną kopię administrator może pobrać opłatę w rozsądnej wysokości (w tym za wydanie kopii w formie papierowej pobierana jest opłata zgodnie z przepisami regulującymi stawki za każdą wydaną stronę dokumentacji medycznej).

6.9. Jeżeli żądanie wydania kopii danych zostało złożone administratorowi w formie elektronicznej a pacjent nie zaznacza inaczej - kopia wydawana jest w tej samej

formie.

6.10. Administrator może udostępnić kopię w inny sposób, niż wybrany przez pacjenta, jeżeli ze względów technicznych nie jest to możliwe (np. ze względu na wagę pliku w wersji elektronicznej); o niemożności dostarczenia kopii w wybrany przez pacjenta sposób oraz proponowanym alternatywnym rozwiązaniu administrator niezwłocznie powiadamia pacjenta.

Prawo do sprostowania danych

6.11. Administrator umożliwia pacjentowi niezwłoczne sprostowanie jego danych osobowych, jeżeli są one nieprawidłowe lub nieaktualne, lub ich uzupełnienie.

6.12. Administrator może żądać od pacjenta stosownych dokumentów w celu okazania, aby ustalić zasadność oraz zgodność z prawem dokonywanej zmiany danych osobowych.

Prawo do usunięcia danych (prawo do bycia zapomnianym)

6.13. Administrator usuwa bez zbędnej zwłoki dane osobowe pacjenta na żądanie pacjenta, jeżeli na administratorze nie spoczywają obowiązki nakazujące dalsze przetwarzanie danych osobowych.

6.14. Administrator odmawia realizacji prawa do bycia zapomnianym, jeżeli została wytworzona dokumentacja medyczna pacjenta i nie upłynął okres jej przechowywania wynikający z przepisów regulujących sposób oraz okres prowadzenia oraz przechowywania dokumentacji medycznej.

6.15. Odmowa realizacji prawa do usunięcia danych jest przekazywana przez administratora pacjentowi wraz z uzasadnieniem przyczyny odmowy zawierającym podstawy prawne odmowy.

Prawo do ograniczenia przetwarzania

6.16. Z uwagi na fakt, iż realizacja prawa do ograniczenia przetwarzania danych znacznie utrudniłaby realizację celów zdrowotnych, o których mowa w pkt 3.3., pomimo zgłoszonego żądania ograniczenia przetwarzania danych, administrator jest uprawniony do ich przetwarzania w dalszym zakresie (w szczególności zawartych w dokumentacji medycznej lub innych danych, przetwarzanych w oparciu o art. 9 ust. 2 lit. h Rozporządzenia).

Prawo do przenoszenia danych

6.17. Dla danych osobowych przetwarzanych w oparciu o podstawę prawną - art. 9 ust. 2 lit. h, wobec administratora będącego podmiotem leczniczym, prawo do przenoszenia danych nie znajduje zastosowania.

6.18. W sytuacji odmowy realizacji żądania prawa do przenoszenia danych, administrator informuje pacjenta o przyczynie odmowy i instruuje pacjenta jakie kroki może podjąć w celu przekazania dokumentacji medycznej do innego podmiotu leczniczego.

Prawo do sprzeciwu

6.19. Dla danych osobowych przetwarzanych przez administratora będącego

podmiotem leczniczym, w oparciu o podstawę prawną - art. 9 ust. 2 lit. h Rozporządzenia, prawo do sprzeciwu nie znajduje zastosowania.

7. Naruszenia ochrony danych osobowych

7.1. Administrator opracował i wdrożył procedury postępowania w przypadku naruszeń lub podejrzeń naruszeń ochrony danych osobowych.

7.2. Administrator prowadzi rejestr naruszeń ochrony danych osobowych oraz dokumentuje wszystkie okoliczności związane z naruszeniami.

7.3. W przypadku naruszeń ochrony danych osobowych mogących skutkować naruszeniem praw lub wolności pacjenta, administrator dokonuje zgłoszenia takiego naruszenia Urzędowi Ochrony Danych Osobowych w terminie 72 godzin od stwierdzenia naruszenia.

7.4. W celu dotrzymania terminu, o którym mowa w pkt 7.1.3. administrator wprowadza do umowy powierzenia przetwarzania danych lub innego instrumentu regulującego kwestię powierzenia przetwarzania danych, odpowiednie postanowienia zobowiązujące podmiot przetwarzający do niezwłocznego zgłaszania administratorowi wszelkich naruszeń ochrony danych osobowych oraz udzielania wszelkich okoliczności dotyczących tych naruszeń.

7.5. W przypadku, jeżeli naruszenie skutkowałoby wysokim ryzykiem naruszenia praw i wolności pacjenta, administrator bez zbędnej zwłoki zawiadamia również tego pacjenta i informuje go jasnym i prostym językiem o okolicznościach naruszenia oraz podjętych środkach mających na celu zapobieżenie jego negatywnym skutkom.

8. Udostępnianie danych osobowych

8.1. Administrator udostępnia dane osobowe podmiotom trzecim zgodnie z przepisami ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta.

8.2. W szczególności administrator udostępnia dane osobowe pacjenta (poprzez udostępnienie dokumentacji medycznej lub udzielenie informacji o stanie zdrowia pacjenta i udzielonych mu świadczeniach zdrowotnych) osobom upoważnionym przez pacjenta.

8.3. Przed udostępnieniem danych osobowych pacjenta administrator podejmuje niezbędne czynności mające na celu ustalenie tożsamości pacjenta, osoby upoważnionej oraz zakres upoważnienia.