Polityka Bezpieczeństwa Ochrony Danych Osobowych

z dnia 04.06.2021 r

EZRA UKSW Spółka z o.o. w Warszawie

ul. Daniłowskiego 31, 01-833 Warszawa, REGON: 380016423, NIP: 7010819366.

Wersja 2		**Pieczęć firmowa:**	
		EZRA UKSW Sp. z o.o. ul. G. Daniłowskiego 31 01-833 Warszawa NIP 7010819366, REGON 380016423	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Jolanta Kagelly	14.06.2021	Tomasz Rowiński Prezes Zarządu EZRA UKSW Sp. z o.o.	

Polityka Bezpieczeństwa

I. Wstęp

1. Informacje ogólne

Celem Polityki Bezpieczeństwa danych osobowych, zwanej dalej Polityką Bezpieczeństwa, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych, sposobu przetwarzania w EZRA UKSW Spółka z o.o., grupy informacji zawierającej dane osobowe.

Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1) **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2) **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3) **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4) **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

2. Cel przygotowania Polityki Bezpieczeństwa

Podstawowym celem przygotowania i wdrożenia dokumentu jest zapewnienie zgodności działania Placówki z Rozporządzeniem 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) oraz Polskim regulacją prawnym:

1) Ustawa z 10 maja 2018 o ochronie danych osobowych;
2) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.;
3) Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO;

3. Zakres informacji objętych polityką bezpieczeństwa oraz zakres stosowania

Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem. Jest to zbiór działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, tj. zapewnienie poufności, spójności i dostępności na każdym etapie tworzenia, przetwarzania, przechowywania i przesyłania danych osobowych.

Polityka Bezpieczeństwa, odnosi się całościowo do problemu zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie, jak i w systemach informatycznych

(w odniesieniu, do których w przypadku szczegółowych regulacji występuje odesłanie do procedur).

Jako załącznik do niniejszej polityki opracowano i wdrożono procedury. Określają one sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, oraz danych osobowych poza systemem informatycznym ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

II. Definicje

1. **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych.
2. **Administrator Danych Osobowych (ADO)** – EZRA UKSW Spółka z ograniczoną odpowiedzialnością w Warszawie, ul. ul. Daniłowskiego 31, 01-833 Warszawa, REGON: 380016423, NIP: 7010819366.
3. **RODO** – rozumie się przez to 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).
4. **RCPD –** Rejestr Czynności Przetwarzania Danych.
5. **Dane osobowe (dane)** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
6. **Szczególna kategoria danych -** Są to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane dotyczące zdrowia, seksualności lub orientacji seksualnej danej osoby oraz dane genetyczne i dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej.
7. **Informacja medyczna i dokumentacja medyczna** - są to informacje dotyczące stanu zdrowia pacjentów, przetwarzane zgodnie z wymaganiami ustawy z dnia 6 listopada2008 r. o Prawach Pacjenta i Rzeczniku Praw Pacjenta i rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów i wzorów zakresu dokumentacji medycznej oraz sposobu jej przetwarzania.
8. **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.

9. **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.
10. **Powierzenie danych osobowych -** operacji na danych osobowych na zlecenie Administratora.
11. **Pseudominizacja -** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
12. **Anonimizacja -** uniemożliwia wszystkim stronom wyodrębnienie konkretnej osoby fizycznej ze zbioru danych. Uniemożliwia też, tworzenie powiązań między dwoma zapisami w zbiorze danych (lub między dwoma oddzielnymi zbiorami) i wnioskowanie jakichkolwiek informacji z tych danych.
13. **Zbiór danych** – zestaw danych osobowych posiadający określoną strukturę, dostępnych wg. określonych kryteriów.
14. **Zgoda osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
15. **Baza danych osobowych** - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych na dysku twardym lub nośnikach zewnętrznych (np. zewnętrzny dysk twardy, płyta CD, DVD, pendrive). Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe.
16. **Przetwarzanie danych** - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
17. **System informatyczny (system)** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
18. **Administrator systemu Informatycznego (ASI- Informatyk)** - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień.
19. **Użytkownik** – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych lub zleceniem.

20. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów informacyjnych przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą.
21. **Nośnik danych** – nośnik służący do zapisu i przechowywania informacji, np. płyta CD, płyta DVD, pendrive, dysk twardy.
22. **Teleporada** - konsultacja z lekarzem znajdującym się w innym miejscu niż pacjent. Rozmowa jest prowadzona telefonicznie lub przy wykorzystaniu aplikacji do połączeń wideo.
23. **Praca zdalna** – wykonywanie zadań powierzonych przez pracodawcę poza siedzibą firmy.

III. Odpowiedzialność w zakresie zarządzania bezpieczeństwem.

1. Deklaracja

Administrator Danych(Zarząd) mając świadomość, że przetwarza dane osobowe, w tym dane osobowe **Pacjentów/Pracowników/Kontrahentów** deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa. Administrator danych deklaruje stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

2. Działalność administratora jako podmiotu leczniczego regulują w szczególności:

1) Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego;
2) Ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta;
3) Ustawa o działalności leczniczej;
4) Ustawa o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
5) Ustawa o zawodach lekarza i lekarza dentysty;
6) Ustawa z dnia 25 września 2015r o zawodzie fizjoterapeuty;
7) Ustawa z dnia 15 lipca 2011r o zawodach pielęgniarki i położnej;
8) Ustawa z dnia 8 czerwca 2001 r. o zawodzie psychologa i samorządzie zawodowym psychologów;
9) Ustawa z dnia 6 września 2001r Prawo farmaceutyczne;
10) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia
11) Ustawa z dnia 2 marca 2020r o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniemCOVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych;

12) Rozporządzenie Ministra Zdrowia z dnia 8 września 2015r w sprawie ogólnych warunków umów o udzielanie świadczeń opieki zdrowotnej;
13) Rozporządzenie Ministra Zdrowia z dnia 6 listopada 2013 r. w sprawie świadczeń gwarantowanych z zakresu ambulatoryjnej opieki specjalistycznej;
14) Rozporządzenie Ministra Zdrowia w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą;
15) Rozporządzenie Ministra Zdrowia z dnia 23 grudnia 2020r w sprawie recept;
16) Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018r w sprawie rodzajów elektronicznej dokumentacji medycznej EDM;
17) Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020r w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

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

4. Przez cele zdrowotne rozumie się:

1) **profilaktykę zdrowotną** - w szczególności poprzez informowanie pacjentów o możliwości pobierania świadczeń zdrowotnych, przekazywanie materiałów edukacyjnych,
2) **diagnozę medyczną oraz leczenie** - w szczególności poprzez udzielanie świadczeń zdrowotnych, zleceń badań diagnostycznych oraz prowadzenie dokumentacji medycznej,
3) **zapewnienie usług psychologicznych –** w szczególności zapewnienie diagnozy psychologicznej, wydanie opinii, realizacji terapii grupowej lub indywidualnej, zapewnienie stałej opieki psychologicznej,
4) **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.
5) **realizacje szkoleń/mentoringu** dla podmiotów medycznych, oświatowych oraz innych jednostek samorządowych,

6) Administrator przetwarza dane osobowe Pacjentów na podstawie **art. 9 ust. 2 lit. h.** 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 oraz zastosowany system monitoringu wizyjnego.

5. Zgoda, o której mowa w pkt 5 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.

6. Działalność administratora jako Pracodawcy regulują w szczególności:

1) Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy;
2) Ustawa z dnia 13 kwietnia 2007 r. o Państwowej Inspekcji Pracy;
3) Ustawa z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych;
4) Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny;
5) Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych;
6) Rozporządzenie Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r. w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy;
7) Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej;
8) Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 29 maja 2019 r. zmieniające rozporządzenie w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy;
9) Rozporządzenie Rady Ministrów z dnia 1 lipca 2009 r. w sprawie ustalania okoliczności i przyczyn wypadków przy pracy;

7. Jako Pracodawca , administrator przetwarza dane osobowe Pracowników/Zleceniobiorców na podstawie **art. 9 ust. 2 lit. b** oraz **Art. 6 ust. 1 lit. c** Rozporządzenia.

8. Przez zatrudnienie rozumie się:

1) **profilaktykę zdrowotną** - w szczególności poprzez zapewnienie profilaktycznej opieki zdrowotnej nad Pracownikami,
2) **prowadzenie dokumentacji pracowniczej**- w szczególności prowadzenie i przechowywanie dokumentacji w sprawach związanych ze stosunkiem pracy i akt osobowych pracowników,

3) **realizację obowiązków związanych z zatrudnieniem** - w szczególności poprzez:
   - rozliczenia czasu pracy;
   - rozliczenia finansowe;
   - rozliczenia podatkowe;
   - zgłaszanie Pracowników i członków ich rodzi do ZUS;
   - udzielanie, rozliczanie świadczeń z ZFŚS;
   - obsługa zwolnień lekarskich;
   - zapewnienie spełnienia wymogów BHP;
   - realizacja szkoleń związanych Z podnoszeniem kwalifikacji zawodowych.

9. W zakresie wykraczającym poza cele zatrudnienia wymienione powyżej przetwarza dane na podstawie:
1) zgody Pracownika (art. 6 ust. 1 lit. a Rozporządzenia) – np: udostępnienie adresu e-mail do korespondencji
2) prawnie uzasadnionego interesu administratora (art. 6 ust. 1 lit. f Rozporządzenia) - w celu dochodzenia roszczeń i obrony przed roszczeniami oraz zastosowany system monitoringu wizyjnego.

10. Działalność administratora w relacjach z dostawcami/Kontrahentami regulują w szczególności:
1) Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny;
2) Ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych;
3) Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych;
4) Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług;
5) Ustawa z dnia 29 września 1994 r. o rachunkowości;
6) Rozporządzenia Ministra Finansów 1)z dnia 3 grudnia 2013r. w sprawie wystawiania faktur;
7) Rozporządzenie Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie;
8) Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie ogłoszeń zamieszczanych w Biuletynie Zamówień Publicznych.

Administrator przetwarza dane osobowe Kontrahentów na podstawie **art. 6 ust. 1 lit. b** oraz **Art. 6 ust. 1 lit. c** Rozporządzenia.

11.Administrator danych - zadania i obowiązki

1) ADO obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę

nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

2) realizuje obowiązek informacyjny wobec osoby, której dane dotyczą oraz przestrzega praw osoby, której dane dotyczą, m.in. prawa do dostępu oraz poprawiania swoich danych; prawa do sprzeciwu czy prawa do przenoszenia danych;
3) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jej obowiązków;
4) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych;
5) zapewnia przetwarzanie danych zgodnie z uregulowaniami Polityki Bezpieczeństwa Ochrony Danych Osobowych, sprawuje nadzór nad bezpieczeństwem danych osobowych;
6) współpraca z organem nadzorczym;
7) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z konsultacjami związanymi oceną skutków dla ochrony danych oraz we wszelakich innych sprawach;
8) pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy.

12. Osoby odpowiedzialne za przetwarzanie danych osobowych – zadania i obowiązki:

Inspektor ochrony danych (IOD)

Administrator jako podmiot publiczny zobowiązany jest do wyznaczenia Inspektora Ochrony Danych Osobowych, w szczególności jeżeli:

1) jego główna działalność polega na przetwarzaniu na dużą skalę danych szczególnej kategorii (danych o stanie zdrowia);
2) jest podmiotem publicznym (w szczególności samodzielnym publicznym zakładem opieki zdrowotnej).

Administrator wyznaczył Inspektora Ochrony Danych i dokonał zawiadomienia o wyznaczeniu Inspektora do Urzędu Ochrony Danych Osobowych.

Administrator stwarza Inspektorowi Ochrony Danych odpowiednie warunki, aby mógł

realizować swoje obowiązki, w szczególności poprzez:

1) niezwłoczne oraz odpowiedne włączanie go we wszystkie sprawy dotyczące ochrony danych osobowych;
2) zapewnienie zasobów niezbędnych do wykonywania jego zadań oraz utrzymania jego fachowej wiedzy;
3) zapewnienie mu niezależności w sprawowaniu jego funkcji, m.in. poprzez niewydawanie instrukcji dotyczących wykonywania przez niego jego zadań,
4) nieponoszenie przez Inspektora negatywnych konsekwencji za wypełnianie przez niego jego zadań,
5) zapewnienie odpowiedniej struktury organizacyjnej aby podlegał jedynie najwyższemu kierownictwu.

Zadania Inspektora ochrony danych obejmują w szczególności:

1) 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;
2) 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;
3) wykonywanie audytów w kwestiach związanych z przetwarzaniem danych osobowych;
4) uczestniczenie oraz wspieranie Administratora w dokonywaniu oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny tych skutków;
5) współpraca z Urzędem Ochrony Danych Osobowych;
6) sprawowanie funkcji punktu kontaktowego dla Pacjentów w kwestiach związanych z przetwarzaniem danych osobowych;
7) prowadzenie Rejestr czynności przetwarzania, na bieżąco aktualizowany i udostępniany przez Administratora na każde żądanie Urzędu Ochrony Danych Osobowych.
8) informowanie Administratora, podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych wymagań praw.

Osoba upoważniona do przetwarzania danych:

1) Może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez Administratora Danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy bądź odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.
2) Musi zachować tajemnicę danych osobowych oraz przestrzegać procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia u Administratora, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji.
3) Musi zapoznać się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Polityki Bezpieczeństwa.
4) Stosuje określone przez Administratora Danych procedury oraz wytyczne mające na celu przetwarzanie danych osobowych zgodnie z obowiązującym prawem.
5) Korzysta z systemu informatycznego Administratora Danych w sposób zgodny z procedurami. Zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

Obowiązki personelu medycznego

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

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.

IV. Przetwarzanie Danych Osobowych

1. Pomieszczenia w których przetwarza się dane osobowe:

1) Pomieszczeniami tworzącymi obszar, w którym znajdują się przetwarzane dane osobowe obejmuje lokalizacje:
   - siedziba Zarządu przy ul. Aleja Zjednoczenia 46, 01-801 Warszawa
   - Poradnia psychologiczna dla dzieci Warszawa-Bielany przy ul. Gustawa Daniłowskiego, 01-833 Warszawa
   - Poradnia psychologiczna dla dzieci Warszawa-Żoliborz przy ul. Szamocka 10c 01-748 Warszawa
   - Poradnia psychologiczna dla dzieci w Piasecznie ul. Powstańców Warszawy 29 05-550 Piaseczno
   - Poradnia Psychologiczna dla dzieci i młodzieży w Radomiu - ul. Plac Stare Miasto 1, 26-610 Radom
   - Poradnia Psychologiczna dla dzieci i młodzieży w Białymstoku, ul. Sikorskiego 6a 15-667 Białystok
   - Poradnia Psychologiczna dla dzieci i młodzieży w Piotrkowie Trybunalskim ul. Sikorskiego 15 97-300 Piotrków Trybunalski
   - Poradnia Psychologiczna dla dzieci i młodzieży w Rzeszowie ul. Malczewskiego 12 35-114 Rzeszów

- Poradnia Psychologiczna dla dzieci i młodzieży w Węgrowie ul. Mickiewicz 12, 07-100 Węgrów
- Poradnia Psychologiczna dla dzieci i młodzieży w Sierpcu ul. Jana Pawła II 1 G, 09-200 Sierpc
- Poradnia Psychologiczna dla dzieci i młodzieży w Ożarowie Mazowieckim ul. Konopnickiej 8, 05-850 Ożarów Mazowiecki
- Poradnia Psychologiczna dla dzieci i młodzieży w Piotrkowie Trybunalskim -
- ul. Słowackiego 15 Piotrków Trybunalski

2) w pomieszczeniach tych, znajdują się zbiory danych w formie kartotek, rejestrów i innej oraz stacjonarny sprzęt komputerowy, w którym są przetwarzane dane osobowe.
3) Przebywanie w pomieszczeniach znajdujących się wewnątrz obszaru przetwarzania, osób nieuprawnionych do dostępu do danych osobowych, jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu tych danych.
4) Pomieszczenia, w których przetwarzane są dane osobowe powinny być zamykane i chronione na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych, w sposób uniemożliwiający dostęp do nich osób trzecich.
5) Dokumentację medyczną należy zabezpieczyć przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych. Wymagane jest fizyczne zabezpieczenie pomieszczeń i znajdującej się w niej dokumentacji.
6) Każdorazowo wyjście z gabinetu, Rejestracji musi być połączone z zamknięciem drzwi (także drzwi wewnętrznych, przejściowych).
7) Po zakończonej pracy wszystkie szafy muszą być zamknięte na klucz, a klucze umieszczone w bezpiecznym, zabezpieczonym miejscu. Niedozwolone jest zostawianie kluczy w zamkach.

v. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności przetwarzanych danych

W Placówce rozróżnia się następujące kategorie środków zabezpieczeń danych osobowych:

1. Zabezpieczenia fizyczne:
   - pomieszczenia zamykane na klucz,
   - szafy metalowe zamykane na klucz,
   - alarm, nadzór firmy ochrony

- zamki szyfrowe

2. Zabezpieczenia procesów przetwarzania danych w dokumentacji papierowej:
   - przetwarzanie danych osobowych następuje w wyznaczonych pomieszczeniach,
   - przetwarzanie danych osobowych następuje przez wyznaczone do tego celu osoby.
3. Zabezpieczenia organizacyjne:
   - Administrator Systemu Informatycznego na bieżąco kontroluje pracę systemu informatycznego z należytą starannością, zgodnie z aktualnie obowiązującą w tym zakresie wiedzą i z obowiązującymi procedurami,
   - sporządzono i wdrożono wewnętrzną politykę bezpieczeństwa,
   - sporządzono i wdrożono Instrukcję Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych,
   - sporządzono Rejestr czynności przetwarzania,
   - sporządzono Analizę ryzyka,
   - sporządzono Rejestr Naruszeń,
   - ustalono regulamin obiegu dokumentacji medycznej,
   - do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora danych, bądź osobę przez niego upoważnioną,
   - stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych,
   - osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego,
   - osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy,
   - przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych,
   - przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych,
   - wprowadzono zasadę „czystego biurka" i „białej kartki",
   - dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób,

- informacji telefonicznych o stanie zdrowia/wyniku badania nie udziela się, względnie udziela się po zidentyfikowaniu rozmówcy i stwierdzeniu jego upoważnienia do uzyskania danych,
- stworzono procedurę postępowania z kluczami.

4. Organizacja pracy przy przetwarzaniu danych osobowych i zasady przetwarzania:
   - w Placówce jest stworzony rejestr osób upoważnionych, który na bieżąco jest aktualizowany,
   - przetwarzać dane osobowe mogą jedynie pracownicy, którzy posiadają stosowne upoważnienie,
   - w trakcie przetwarzania danych osobowych, pracownik jest osobiście odpowiedzialny za bezpieczeństwo powierzonych mu danych,
   - przed przystąpieniem do realizacji zadań związanych z przetwarzaniem danych osobowych, pracownik winien sprawdzić, czy posiadane przez niego dane były należycie zabezpieczone, oraz czy zabezpieczenia te nie były naruszone,
   - w trakcie przetwarzania danych osobowych, pracownik winien dbać o należyte ich zabezpieczenie przed możliwością wglądu, bądź zmiany przez osoby do tego celu nieupoważnione,
   - po zakończeniu przetwarzania danych pracownik winien należycie zabezpieczyć dane osobowe przed możliwością dostępu do nich osób nieupoważnionych.

VI. Kontrola wewnętrzna stanu ochrony danych osobowych i przestrzegania zasad ich ochrony

1) Inspektor Ochrony Danych (na polecenia ADO) sprawdza zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, a następnie opracowuje w tym zakresie sprawozdanie dla Administratora Danych.
2) ADO sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych. ADO lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.
3) Zaobserwowane błędy oraz zaniechania w przestrzeganiu Polityki Bezpieczeństwa Danych Osobowych przedstawia się Administratorowi Danych Osobowych oraz pracownikom upoważnionym do przetwarzania danych osobowych.

VII. Szkolenia lub zapoznawanie osób z zasadami ODO

1) Każda osoba przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami w wersji papierowej winna być poddana przeszkoleniu lub zapoznana z:
    a. podstawami prawnymi dotyczącymi bezpieczeństwa danych osobowych,
    b. zasadami ochrony danych osobowych zawartymi w niniejszej Polityce.
2) Za przeprowadzenie szkolenia lub zapoznania z zasadami ochrony danych osobowych odpowiada ADO.
3) W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia za pomocą listy obecności z przeprowadzonego szkolenia.
4) Każda nowozatrudniona osoba po odbytym szkoleniu lub po zapoznaniu z zasadami ochrony danych osobowych zobowiązana jest do podpisania Zobowiązania do zachowania poufności.
5) Podpisane Oświadczenia zostają zarchiwizowane, w aktach osobowych lub teczkach pracowników.

VIII. Praca zdalna w związku z sytuacją pandemiczną wywołaną koronawirusem SARS-CoV-2

1. Pracownik może korzystać z papierowej dokumentacji zawierającej dane osobowe wyłącznie za zgodą pracodawcy. Obszar przetwarzania takich danych musi być jasno określony przez przełożonego.
2. Administratorem danych osobowych przetwarzanych przez pracowników podczas pracy zdalnej jest pracodawca. Na pracodawcy spoczywa obowiązek zapewnienia przestrzegania zasad bezpieczeństwa danych, zarówno tych przetwarzanych za pośrednictwem urządzeń elektronicznych, jak i zawartych w dokumentacji papierowej.
3. Pracownik może przetwarzać dane osobowe wyłącznie w związku z wykonywaniem powierzonych mu obowiązków służbowych, z zachowaniem ustalonej przez pracodawcę polityki bezpieczeństwa i procedur w tym zakresie.
4. Pracodawca powierzając wykorzystywanie dokumentacji papierowej podczas pracy zdalnej winien spełnić następujące warunki:
    a) zadbać o ewidencjonowanie powierzonej dokumentacji zawierającej dane osobowe,
    b) zapewnić ograniczone przechowywanie materiałów — papierowe dokumenty z danymi osobowymi mają być przechowywane przez pracownika wyłącznie na czas wykonywania określonego zadania czy projektu,
    c) ograniczenie liczby dokumentów, które zdalny pracownik wynosi z siedziby

Administratora — powierzona dokumentacja ma być niezbędna do celu przetwarzania danych osobowych przez pracownika,

d) przenoszone dokumenty muszą być odpowiednio zabezpieczone, np. w zabezpieczonej teczce, zamykanej na kod walizce, w sposób niewidoczny dla osób trzecich,

e) dokumenty muszą być również odpowiednio zabezpieczone w miejscu wykonywania pracy zdalnej, np. w szafkach i biurkach zamykanych na klucz, w miejscach niedostępnych dla nieuprawnionych osób trzecich, np. członków rodziny pracownika,

f) zapewnienie, aby pracownik wykorzystywał powierzoną dokumentację wyłącznie w tym celu, w jakim byłaby ona wykorzystywana w stałym miejscu pracy,

g) ustalenie procedury niszczenia dokumentów, np. zakaz wyrzucania ich do domowego kosza, konieczność odpowiedniego zabezpieczenia w celu zniszczenia ich po zakończonym projekcie (np. rekrutacja) w niszczarce znajdującej się w biurze — jeśli pracownik nie ma w domu takiego sprzętu, pracodawca ma obowiązek poinstruowania pracownika o konieczności zgłoszenia każdego incydentu naruszenia bezpieczeństwa danych osobowych. Pracodawca jako Administrator danych musi w takiej sytuacji wywiązać się z obowiązku, o którym mowa w artykule 33 ust. 1 Rozporządzenia RODO (zgłoszenie naruszenia danych osobowych organowi nadzorczemu nie później niż w terminie 72 godzin po stwierdzeniu incydentu).

Jeśli nie jest możliwe zastosowanie wyżej wymienionych rozwiązań, należy rozważyć pracę na kopiach dokumentów zawierających dane osobowe, a pracownik ma obowiązek chronić na równi dane osobowe zawarte w kopii i oryginalnym dokumencie.

5. Pracownik nie powinien przenosić dokumentacji papierowej z biura do miejsca wykonywania pracy zdalnej w następujących przypadkach:
   a. pracodawca wdrożył elektroniczny obieg dokumentów, więc pracownik ma bezpieczny dostęp do niezbędnych danych osobowych za pośrednictwem środków komunikacji elektronicznej,
   b. pracodawca może udostępnić zdalnemu pracownikowi odpowiednio zaszyfrowane elektroniczne kopie dokumentów zawierających dane osobowe,
   c. pracodawca może szybko i bezpiecznie wdrożyć elektroniczny obieg dokumentacji w firmie.
6. Pracodawca ma obowiązek każdorazowo ocenić niezbędność wykorzystania przez zdalnego pracownika papierowej dokumentacji zawierającej dane osobowe. W tym celu musi uwzględnić dostępne środki, charakter danych oraz cele, dla których te dane są przetwarzane.
7. Przyjmowane rozwiązania pracy zdalnej muszą już w fazie ich projektowania być

zgodne z rozporządzeniem RODO – zasada privacy by design (art. 25 rozporządzenia RODO).

8. Należy zapewnić każdemu z pracowników odpowiednie szkolenie z zakresu obowiązującej w firmie procedury bezpieczeństwa oraz zasad korzystania z narzędzi i również zadbać o udokumentowanie tego faktu.
9. Wdrożyć oświadczenia o zachowaniu poufności oraz upoważnienia do przetwarzania danych osobowych, jak również sam rejestr takich upoważnień.
10. Pracodawcy, biorąc pod uwagę zawodowy charakter ich działalności i obowiązek dołożenia należytej staranności, powinni uregulować kwestie pracy zdalnej w dokumentacji wewnętrznej tj. wdrożyć regulamin pracy zdalnej.
11. Pracodawca winien ewidencji urządzeń przenośnych, które mają dostęp do danych firmowych.
12. Pracodawca winien ewidencjonować pozyskane zgody na przetwarzanie danych osobowych np. w formie ewidencji zgód.
13. Pracodawca powinien przypominać pracownikom o konieczności dopełniania obowiązku informacyjnego wobec klientów, kontrahentów np. w formie komunikatu lub instrukcji zgodnie z art. 24 ust. 2 rozporządzenia RODO, który przewiduje obowiązek wdrożenia polityk ochrony danych osobowych, gdy jest to proporcjonalne w stosunku do czynności przetwarzania.
14. Konieczność pracy zdalnej i związane z tym ryzyka i wyzwania w zakresie ochrony danych osobowych stanowią o podstawie do samoregulacji przez Administratorów danych osobowych.

IX. Teleporady w związku z sytuacją pandemiczną wywołaną koronawirusem SARS-CoV-2

Zgodnie z treścią Zarządzenia Prezesa NFZ Nr 182/2019/DSOZ Teleporady realizowane z wykorzystaniem systemów teleinformatycznych dotyczą świadczeń wymienionych w załącznikach 1a i 1c do obowiązującego zarządzenia, teleporady realizowane z wykorzystaniem systemów teleinformatycznych dotyczą świadczeń wymienionych w załącznikach 1a i 1c do obowiązującego zarządzenia Prezesa Narodowego Funduszu Zdrowia w sprawie określenia warunków zawierania i realizacji umów o udzielanie świadczeń opieki zdrowotnej w rodzaju ambulatoryjna opieka specjalistyczna. Z wizyty na odległość mogą skorzystać pacjenci kontynuujący opiekę w konkretnej poradni specjalistycznej, zgodnie z ustalonym planem leczenia i stanem klinicznym. W sprawie określenia warunków zawierania i realizacji umów o udzielanie świadczeń opieki zdrowotnej w rodzaju ambulatoryjna opieka specjalistyczna. Z wizyty na odległość mogą skorzystać pacjenci kontynuujący opiekę w konkretnej poradni specjalistycznej, zgodnie z ustalonym planem leczenia i stanem klinicznym.

Art. 40 ust. 1 Ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, podstawowym obowiązkiem lekarza jest zachowanie tajemnicy informacji dotyczących pacjentów przyjmowanych w ramach wykonywania zawodu. Wynika to z etyki zawodowej lekarzy, a także z obowiązujących przepisów prawa. Teleporada czy też wizyta lekarska online jest świadczeniem równoprawnym do wizyt odbywanych w tradycyjnej formie. Podobnie jak w przypadku usługi medycznej wykonywanej w obecności pacjenta, musi być wykonywana zgodnie z obowiązującymi zasadami etyki lekarskiej, czyli m.in. z zachowaniem tajemnicy zawodowej. Obowiązki Placówek medycznych względem RODO są następujące:

1. Pracodawca winien zapewnić bezpieczne kanały komunikacji na linii pacjent-lekarz. Należy zadbać o to, by żadne informacje nie wydostały się poza krąg osób uprawnionych.
2. Podczas wizyty lekarz powinien przebywać w ustronnym miejscu, gdzie nikt nie będzie mógł podsłuchać jego rozmowy.
3. Należy zabezpieczyć linię telefoniczną lub komunikator, za pośrednictwem którego odbywa się połączenie. Do komunikacji z pacjentem powinno się używać tylko zaufanych kanałów, które mają stosowne zabezpieczenia.
4. W przypadku teleporady możliwa jest zdalna weryfikacja tożsamości bazująca na oświadczeniu pacjenta. Taka opcja w trakcie stanu epidemicznego aż do odwołania obowiązuje na podstawie Rozporządzenia Rady Ministrów z dnia 10 kwietnia 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii. Pacjent podaje dane za pośrednictwem systemu teleinformatycznego lub systemu łączności. W przypadku pacjentów, którzy byli już w placówce leczniczej, dane weryfikuje się na podstawie tych, które przekazali oni osobiście.
5. Teleporada jest równoznaczna z tradycyjną konsultacją medyczną. W związku z tym należy ją traktować tak samo również pod względem prowadzenia dokumentacji medycznej. Świadczenie telemedyczne powinno być udokumentowane.
6. Należy sporządzić opis medyczny i notatkę, w której wskazana będzie forma udzielenia konsultacji, narzędzie, za pomocą którego się odbyła oraz czas jej trwania.
7. Procedura pracy zdalnej powinna uwzględniać kwestie przesyłania danych. Dobrze, by znalazły się w nich nawet tak szczegółowe informacje, jak np. sposób wysyłki i szyfrowania dokumentacji medycznej, a także sposoby zabezpieczania haseł.
8. Zaleca się aby rejestratorzy medyczni stanowiący pierwszą linię w kontaktach z pacjentami – byli odpowiedzialni nie tylko za wizerunek, ale również właściwy przepływ informacji w placówce.
9. Zaleca się szkolenia dla podwyższenia jakości pracy zdalnej pod kątem zgodności działań z RODO oraz postępowaniem z „trudnym" pacjentem.
10. Świadczeniodawcy POZ zobowiązani zostali do zachowania standardu w zakresie

udzielania teleporad m.in. przy ustalaniu tożsamości, jak i w obowiązku dokonywania oceny adekwatności teleporady do stanu zdrowia pacjenta.

Zasady postępowania w trakcie realizacji świadczeń medycznych w ramach teleporady

1. Przed rozpoczęciem udzielania porad telemedycznych należy sprawdzić działanie sprzętu i oprogramowania wykorzystywanego w tym celu. Należy sprawdzić działanie programu antywirusowego. Ponadto, jeżeli w systemie informatycznym zauważymy niestandardowe zachowanie, które może świadczyć o działaniu złośliwego oprogramowania, należy niezwłocznie poinformować o tym fakcie informatyka.
2. Porady telemedyczne należy udzielać przy zachowaniu pełnej poufności przetwarzanych danych.
3. Należy poinformować pacjenta że w trakcie teleporady będą poruszane tematy dotyczące danych medycznych, dlatego należy zadbać o poufność w trakcie przeprowadzanej rozmowy.
4. Należy dokonać weryfikacji tożsamości Pacjenta.

a. W przypadku Pacjenta który wcześniej odwiedził Placówkę należy zadać pytania kontrolne na podstawie informacji zawartych w dokumentacji medycznej. Należy zweryfikować np. numer PESEL, ostatni problem zdrowotny, który był powodem odwiedzin w Placówce.
b. W przypadku Pacjentów pierwszorazowych zaleca się przeprowadzenie porady telemedycznej poprzez system umożliwiający transmisję obrazu (rozmowa wideo), co umożliwi weryfikację Pacjenta z dokumentu tożsamości. Należy pamiętać że nie można żądać przesłania zdjęcia dokumentu tożsamości, kopiowanie dokumentów tożsamości do dokumentacji medycznej jest zabronione.
c. W przypadku Pacjentów małoletnich należy zweryfikować Pacjenta oraz przedstawiciela ustawowego.

5. Fakt odbycia porady telemedycznej wraz z opisem przebiegu oraz konkluzji należy udokumentować w dokumentacji medycznej.
6. W przypadku teleporad psychiatrycznych świadczenie odbywa się wyłącznie na rzecz pacjentów kontynuujących leczenie, zgodnie z ustalonym planem terapeutycznym lub planem terapii i zdrowienia, adekwatnie do stanu klinicznego pacjenta.
7. W trakcie przeprowadzania porad telemedycznych należy przestrzegać przyjętych procedur z zakresu ochrony danych osobowych.

X. Prawa osób, których dane dotyczą

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

Administrator prowadzi **rejestr zgłoszonych żądań**, przez osoby, których danych dotyczą. Przed wykonaniem praw osoby, której dane dotyczą administrator dokonuje weryfikacji tożsamości osoby zgłaszającej żądanie, celem ustalenia, czy żądanie pochodzi od osoby uprawnionej.

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 przyczynie wydłużenia tego terminu oraz przewidywanym terminie realizacji żądania pacjenta.

Prawo do informacji

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.

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

Prawo dostępu do danych

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

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).

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

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

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

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)

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

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.

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

Prawo do ograniczenia przetwarzania

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

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

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

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.

XI. Postanowienia końcowe

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody ADO.
2. Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody ADO, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.

3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce.
4. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.
5. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa mają zastosowanie przepisy 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) oraz wydanych na jej podstawie aktów wykonawczych.
6. Zmiana dokonana w załączniku do niniejszej Polityki powoduje aktualizację danego załącznika, nie powoduje natomiast zmiany całości dokumentu. Po dokonaniu aktualizacji załącznika jego wcześniejsza wersja automatycznie traci ważność.

XI. Załączniki

Nr	1	Wykaz zmian
Nr	2	Analiza Oceny Ryzyka
Nr	3	Rejestr czynności przetwarzania
Nr	4	Rejestr kategorii czynności przetwarzania
Nr	5	Klauzula informacyjna (a-d)
Nr	6	Porozumienie w zakresie przetwarzania danych osobowych
Nr	7	Umowa powierzenia danych osobowych
Nr	8	Zgoda na przetwarzanie danych osobowych – Pracownik
Nr	9	Zgoda na udostępnienie wizerunku
Nr	10	Zgoda na udostępnienie adresu e-mail od Pacjenta