POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

CEL

1. Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych i innych danych przetwarzanych przez Przychodnię HIH, przed wszelakiego rodzaju zagrożeniami wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi. Polityka została opracowana zgodnie z wymaganiami określonymi w przepisach dotyczących ochrony danych RODO oraz w oparciu o wewnętrzne i zewnętrzne wymagania. Jako element uzupełniający do niniejszej polityki opracowano i wdrożono procedury oraz instrukcje, które określają sposoby zarządzania systemem bezpieczeństwa informacji.
2. Polityka obejmuje wszystkich pracowników Przychodni oraz dostawców, podmioty współpracujące z Przychodnią na podstawie umowy cywilnoprawnej, mających kontakt z danymi osobowymi objętymi ochroną. Przetwarzanie danych osobowych odbywa się w Przychodni w wersji papierowej – m. in. historia choroby, skierowania, oświadczenia oraz w wersji elektronicznej.
3. Ochrona danych osobowych i innych danych jest realizowana poprzez: zabezpieczenia fizyczne, procedury / instrukcje, oprogramowanie systemowe oraz przez świadome działania użytkowników. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
    a. **poufność danych** - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
    b. **integralność danych** - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    c. **rozliczalność danych** - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
    d. **integralność systemu** - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.
    e. **Dostępność danych** – wymagane informacje są dostępne dla uprawnionych użytkowników zawsze, gdy są niezbędne.

DEFINICJE I SKRÓTY

Przez użyte w Polityce określenia należy rozumieć:

1. **Administrator Danych Osobowych** – rozumie się przez to właściciela HIH Przychodni
2. **Polityka** – Polityka bezpieczeństwa danych w Przychodni;
3. **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;
4. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

5. **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów;
6. **Usuwanie danych** – rozumie się przez to zniszczenie danych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
7. **Zgoda** osoby, której dane dotyczą - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
8. **Administrator** -osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
9. **Użytkownik** - pracownik Przychodni posiadający uprawnienia do pracy w systemie informatycznym, zgodnie z zakresem obowiązków służbowych;
10. **Zabezpieczenie systemu informatycznego** – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
11. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
12. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

SPOSÓB POSTĘPOWANIA

I.Zakres danych osobowych i miejsca przetwarzania w HIH Przychodni

1. W HIH Przychodni znajdują się następujące bazy danych (informatyczne): Rejestr podmiotów współpracujących z Przychodnią na podstawie umowy cywilnoprawnej, rejestr przyjętych pacjentów, oraz zbiory danych w wersji papierowej – m. in. historia choroby, skierowania, oświadczenia i inne.

2. W HIH Przychodni przetwarzanie danych osobowych odbywa się w gabinetach lekarskich, gabinecie pielęgniarskim oraz przy Rejestracji - ladzie.

II. Zadania Administratora Danych:

1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem - RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2. Czuwa nad stosowaniem i przestrzeganiem w Przychodni przepisów RODO przez pracowników.

3. **Nadaje i odwołuje upoważnienia do przetwarzania danych osobowych** oraz prowadzi **Ewidencję osób uprawnionych do przetwarzania danych osobowych.**

4. Chroni dane osobowe zawarte w zbiorach prowadzonych sposobem tradycyjnym – wersja papierowa oraz poprzez system informatyczny.

5. Podejmuje stosowne działania w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym.

6. Nadzoruje i kontroluje systemy informatyczne służące do przetwarzania danych osobowych i osób przy nim zatrudnionych.

7. Nadzoruje i kontroluje system przetwarzania danych osobowych sposobem tradycyjnym - wersja papierowa.

III. Środki techniczne i organizacyjne niezbędne dla zapewnienia ochrony danych

1. W celu ochrony danych spełniono wymogi, o których mowa w Rozporządzeniu RODO w szczególności:

a. przeprowadzono **Ocenę skutków dla ochrony danych;**

b. przeprowadzono **Analizę ryzyka** w stosunku do zasobów biorących udział w poszczególnych procesach działalności HIH Przychodni;

c. do przetwarzania danych zostały dopuszczone wyłącznie osoby upoważnione przed Administratora danych;

d. zawarto **Umowy powierzenia** przetwarzania danych dla podmiotów współpracujących z HiH Przychodnią na podstawie umowy cywilnoprawnej, m .in. Podmiot wykonujący badania laboratoryjne dla HIH Przychodni;

e. Została opracowana i wdrożona **Polityka Prywatności HIH Przychodni** dostępna dla wszystkich pracowników oraz kontrahentów Przychodni.

f. Została opracowana i wdrożona niniejsza **Polityka Bezpieczeństwa.**

1. **W celu ochrony danych osobowych stosuje się następujące środki ochrony fizyczne danych osobowych:**

a. Zbiory danych osobowych – m. in. historie chorób przechowywane są w siedzibie HIH Przychodni w szafach do tego przeznaczonych, zamykanych na klucz oraz chronionych przed dostępem osób nieupoważnionych. Szafy znajdują się w wyznaczonym miejscu za Ladą rejestracyjną. Przy Ladzie siedzi pracownik Przychodni przez cały czas otwarcia HiH Przychodni, który ma obowiązek chronić przed dostępem osób trzecich. Po zamknięciu przychodni oraz po opuszczenie miejsca pracy wyznaczonego pracownika, zostaje opuszczana roleta ochronna, która uniemożliwia wejścia komukolwiek. HiH Przychodnia poza godzinami pracy zamykana jest na klucz, oraz nadzorowana przez Ochronę, oraz monitoring budynku, w którym się znajduje.

b. Zbiory danych osobowych w gabinetach lekarskich chronione są przez pracowników - lekarzy, pielęgniarki, którzy są w posiadaniu dokumentacji pacjenta tylko wtedy, gdy pacjent umówiony jest na wizytę. Poza tą sytuacją, cała dokumentacja pacjentów znajduje się w zabezpieczonych szafach.

c. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

1. **W celu ochrony danych osobowych stosuje się następujące środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej:**

a. Komputery służące do przetwarzania danych osobowych nie są połączone z lokalna siecią komputerową.

b. Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonym komputerze przenośnym, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła.

c. Dostęp do systemu komputera, w którym przetwarzane są dane osobowe, zabezpieczony jest za pomocą procesu uwierzytelniania wykorzystaniem identyfikatora użytkownika oraz hasła.

d. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.

e. Zastosowano środki ochrony przed szkodliwym oprogramowaniem, takim jak: robaki, wirusy, konie trojańskie.

1. **W celu ochrony danych osobowych stosuje się następujące środki organizacyjne:**

a. Osoby zatrudnione w Przychodni HIH zostały zaznajomione z Przepisami dotyczącymi ochrony danych osobowych RODO.

b. Przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

c. Osoby zatrudnione w Przychodni przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy na podstawie **Oświadczenia o zachowania tajemnicy.**

d. Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane **Zasada Czystego Monitora.**

e. Biurka pracowników są czyste, bez zbędnej dokumentacji, na której umieszczone są dane osobowe pacjentów – **Zasada Czystego Biurka.**

f. **Kopie zapasowe** zbioru danych osobowych znajdują się na serwerze niedostępnym przed dostępem z zewnątrz.

IV. **Zarządzanie incydentami.**

1. Postępowanie alarmowe definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik Przychodni w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych, zobowiązany jest poinformować Administratora danych.
2. W każdym przypadku naruszenia ochrony danych osobowych Administrator danych weryfikuje, czy naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia organ nadzorczy, jednak nie później niż w ciągu 72 godzin od identyfikacji naruszenia.
4. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, chyba że zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka wystąpienia ww. naruszenia.
5. Do typowych zagrożeń bezpieczeństwa danych należą:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów w wersji papierowej

b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych

c. nieprzestrzeganie zasad ochrony danych przez pracowników (np. niestosowanie **zasady czystego biurka, czystego ekranu**, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),

1. Do typowych incydentów bezpieczeństwa danych należą:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania),

V. **Analiza ryzyka** dla zasobów biorących udział w procesach przeprowadza Administrator danych lub osoba przez niego wyznaczona. Analiza przeprowadzana jest nie rzadziej niż raz w roku i stanowi podstawę do aktualizacji sposobu postępowania z ryzykiem. Na podstawie wyników przeprowadzonej analizy ryzyka, wskazani przez Administratora danych właściciele procesów lub sam Administrator danych samodzielnie wdrażają sposoby postępowania z ryzykiem.

I. **Współpraca z podmiotami zewnętrznymi.** Każdorazowe korzystanie z usług podmiotu przetwarzającego dane osobowe jest poprzedzone zawarciem **Umowy powierzenia przetwarzania danych osobowych.**

I. **Realizacja praw pacjenta**

Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą m. in.:

a. Prawo dostępu do danych

b. Prawo do sprostowania danych

c. Prawo do usunięcia danych (za wyjątkiem obowiązku przechowywania dokumentacji medycznej przez okres 20 lat)

d. Prawo do przenoszenia danych

e. Prawo do sprzeciwu wobec przetwarzania danych

POLITYKA PRYWATNOŚCI PRZYCHODNI HIH

CEL: Ochrona danych osobowych.

DEFINICJE I SKRÓTY

Przez użyte w Polityce określenia należy rozumieć:

1. **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.
2. **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;
3. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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;

SPOSÓB POSTĘPOWANIA

Administratorem danych jest HIH Przychodnia S. C. wpisanym do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, z siedzibą przy ul. Jana Długosza 48D, 51-162 Wrocław, nr REGON: 930025129, nr NIP: 897-001-29-82

Jako Administrator danych, zapewniamy prawo dostępu do Twoich danych, możesz je modyfikować, żądać ich usunięcia lub ograniczenia ich przetwarzania. Możesz także skorzystać z prawa do złożenia wobec Przychodni sprzeciwu wobec przetwarzania Twoich danych oraz prawa do przenoszenia danych do innego administratora danych. W przypadku zgłoszenia ograniczenia lub zmiany uprawnień zgłoś się do Przychodni lub skontaktuj się drogą e-mailową.

Administrator w celu zabezpieczenia powierzonych do przetwarzania Danych Osobowych, zobowiązuje się podjąć środki techniczne i organizacyjne, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W szczególności obejmuje to środki, o których mowa w artykułach 24 oraz 32 RODO, w szczególności:

- wdrożenie odpowiednich polityk ochrony danych;
- wdrożenie środków technicznych i organizacyjnych aby zabezpieczenie danych pozwalało spełnić wymagania RODO;

- dokumentuje spełnienie wymagań dotyczących zabezpieczeń w celu wykazania zgodności z RODO.

Administrator w szczególności zobowiązuje się:

- wykorzystywać powierzone Dane Osobowe wyłącznie w określonym celu w zakresie Umowy;
- nie wykonywać żadnych czynności związanych z dalszym przekazywaniem Danych Osobowych nieuregulowanych w Umowie;
- dopuścić do obsługi służącego do przetwarzania powierzonych Danych Osobowych systemu informatycznego oraz wchodzących w jego skład urządzeń wyłącznie osoby posiadające wydane przez Administratora upoważnienie. Administrator zapewnia, że osoby upoważnione do przetwarzania Danych Osobowych zobowiązały się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
- niezwłocznie usunąć Dane Osobowe po osiągnięciu celu Umowy, w tym usunąć te dane ze wszelkich elektronicznych nośników danych, na których zostały one utrwalone przez Administratora dla realizacji celu określonego w Umowie. Obowiązek określony w zdaniu poprzednim nie dotyczy danych osobowych, wobec których Przychodnia stała się odrębnym administratorem danych osobowych, w szczególności danych osobowych znajdujących się w dokumentacji medycznej prowadzonej przez Świadczeniodawcę.

RODO formułuje 6 zasad przetwarzania danych osobowych, którymi kieruje się nasza Przychodnia, gdy przetwarzamy dane osobowe. Są nimi:

- zasada zgodności z prawem, rzetelności i przejrzystości: przetwarzamy dane osobowe w sposób zgodny z przepisami prawa. O wszystkich kwestiach z tym związanych informujemy wyczerpująco ustalonymi kanałami komunikacji i jak najprostszym językiem, by osoby, których dane dotyczą, były świadome, że zbieramy, przechowujemy lub w inny sposób przetwarzamy ich określone dane osobowe; zasada minimalizacji i adekwatności danych: przetwarzamy tylko te dane (adekwatne, stosowne), które są rzeczywiście potrzebne, by zrealizować dany cel;\
- zasada prawidłowości danych: dokładamy najwyższej staranności, by dane, które przetwarzamy, były zgodne z prawdą, aktualne i dokładne. Dlatego możemy co jakiś czas prosić osoby, których dane przetwarzamy, o to, by sprawdziły i zaktualizowały swoje dane. Prosimy ich też o to, by klienci informowali nas o wszelkich zmianach swoich danych osobowych (imię i nazwisko, adres itp.);
- zasada ograniczenia celu oraz przechowywania przetwarzanych danych: dane osobowe zbieramy jedynie w konkretnym, wyraźnym i prawnie uzasadnionym celu, którego nie moglibyśmy osiągnąć w inny sposób. Przechowujemy dane w formie, która umożliwia identyfikację osoby, której dane dotyczą. Przetwarzamy je tylko tak długo, jak jest to niezbędne, by zrealizować cel, dla którego je pozyskaliśmy (chyba, że do dalszego przetwarzania zobowiązują nas przepisy prawa);
- zasada integralności i poufności danych: zapewniamy takie rozwiązania informatyczne i organizacyjne, dzięki którym dane osobowe, które przetwarzamy, są bezpieczne. Chronimy dane przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem;
- zasada rozliczalności: jesteśmy w stanie wykazać (w sposób, jakiego wymaga od nas prawo), że w odniesieniu do danych osobowych działamy zgodnie z przepisami prawa, uwzględniamy ochronę danych w fazie projektowania (np. nowego produktu) oraz zapewniamy domyślną ochronę danych osobowych.

Twoje dane zdobyliśmy w związku z realizacją umowy na realizację usług w celach:

- realizacji usług medycznych
- bieżącej obsługi klienta,
- prowadzenia działań profilaktycznych i prozdrowotnych
- edukacyjnych i szkoleniowych
- statystycznych.

Większość danych podajesz nam sam. Świadczenie usług w ramach opieki zdrowotnej w Przychodni odbywa się na podstawie umowy zawartej pomiędzy Przychodnią a Twoim pracodawcą. Twoje dane udostępnia nam Twój pracodawca, lub Ty sam, jeśli Twój pracodawca nie ma podpisanej umowy z nami.

Korzystając z naszych usług, za pośrednictwem Twojego pracodawcy w pierwszej kolejności niezbędne jest otrzymanie zgłoszenia o objęciu Twojej osoby opieką zdrowotną. Do tego celu potrzebujemy Twoich danych: imię, nazwisko, nr PESEL, płeć oraz data urodzenia (w przypadku osób bez nr PESEL), adres zamieszkania. Warto również podać adres e-mail oraz numer telefonu, nie jest to niezbędne. Jeżeli z naszych usług korzystasz jako pacjent indywidualny, również potrzebujemy tych danych, aby móc zweryfikować Twoją tożsamość przed udzieleniem świadczenia zdrowotnego. Przed udzieleniem świadczenia konieczne jest potwierdzenie Twojej tożsamości, w szczególności poprzez zgłoszenie do objęcia opieką zdrowotną, weryfikacji danych podczas rozmowy z w celu Rezerwacji Wizyt, na stanowiskach recepcyjnych lub w gabinecie lekarskim.
Administrator będzie przetwarzał dane powierzone mu na podstawie Umowy z Firmą przez czas niezbędny do osiągnięcia celu przetwarzania, lecz nie dłużej, niż czas trwania Umowy. Po osiągnięciu celu Umowy przychodnia usuwa lub zwraca wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie. Strony dla jasności oświadczają, że obowiązek określony w zdaniu poprzednim nie dotyczy danych osobowych, wobec których przychodnia stała się odrębnym administratorem danych osobowych, w szczególności danych osobowych znajdujących się w dokumentacji medycznej prowadzonej przez Świadczeniodawcę.
Jako podmiot leczniczy zobowiązani jesteśmy do **prowadzenia i przechowywania dokumentacji medycznej** (Art. 9 ust. 2 lit. h RODO w zw. z art. 24 ust. 1 Ustawy o prawach pacjenta oraz Rozporządzenia MZ).
Zgodnie z obowiązującym prawem Twoja dokumentacja medyczna przechowywana jest przez podmiot leczniczy przez co najmniej 20 lat od dnia dokonania w niej ostatniego wpisu. Jeżeli dane były przez nas przetwarzane w celu dochodzenia roszczeń (np. w postępowaniach windykacyjnych) przetwarzamy dane w tym celu przez okres przedawnienia roszczeń, wynikający z przepisów kodeksu cywilnego. Wszelkie dane przetwarzane na potrzeby rachunkowości oraz ze względów podatkowych przetwarzamy przez 5 lat liczonych od końca roku kalendarzowego, w którym powstał obowiązek podatkowy. Jeżeli wyraziłeś nam zgodę na przetwarzanie danych w celach marketingowych, przetwarzamy Twoje dane od chwili wyrażenia zgody do czasu jej cofnięcia. Po upływie wyżej wymienionych okresów Twoje dane są usuwane lub poddawane anonimizacji.

Korzystanie z usług Przychodni jest w pełni dobrowolne. Jako podmiot leczniczy jesteśmy zobowiązani do prowadzenia dokumentacji medycznej w sposób określony przepisami prawa, w tym do oznaczenia tożsamości pacjenta z wykorzystaniem jego danych osobowych. W takim przypadku brak podania danych może skutkować odmową rezerwacji wizyty czy udzielenia świadczenia zdrowotnego. Ze względów rachunkowych czy podatkowych posiadamy obowiązek prawny przetwarzania Twoich danych, brak ich podania może skutkować np. brakiem możliwości wystawienia faktury czy imiennego rachunku.

Odbieramy i archiwizujemy **Twoje oświadczenia,** w których upoważniasz inne osoby do dostępu do Twojej dokumentacji medycznej oraz udzielania im informacji o stanie zdrowia zgodnie z prawem pacjenta (Art. 6 ust. 1 lit. c RODO w zw. z art. 9 ust. 3 oraz art. 26 ust. 1 Ustawy o prawach pacjenta oraz § 8 ust. 1 Rozporządzenia MZ).

Kontaktujemy się z Tobą poprzez podany przez Ciebie numer telefonu czy adresem e-mail, np. potwierdzamy Twoją umówioną wizytę, odwołujemy termin konsultacji, przypominamy Ci o konsultacji, informujemy o konieczności przygotowania się do zabiegu lub o możliwości odbioru wyników badań (Art. 6 ust. 1 lit. b oraz f RODO, jako tzw. prawnie uzasadniony interes administratora, jakim jest opieka około obsługowa nad pacjentem oraz sprawniejsze zarządzanie grafikami).
Podanie nam Twojego numer telefonu czy adresu e-mail jest dobrowolne. Brak ich nie będzie skutkował odmową udzielenia świadczenia zdrowotnego. Brak podania danych spowoduje jednak, że nie otrzymasz od nas potwierdzenia wizyty, nie będziesz miał możliwości odwołania jej poprzez np. SMS. Każde wyrażenie zgody marketingowej odbywa się dobrowolnie. Odmowa ich udzielenia nie uniemożliwi Ci skorzystania z usług Przychodni. Masz prawo do odwołania wyrażonej nam zgody w dowolnej chwili. Rezygnację możesz złożyć w Przychodni.

Pragniemy zapewnić Ci odpowiednią opiekę, jakość naszych usług, dlatego w trakcie trwania opieki lub po wykonaniu usługi możemy przesyłać Ci krótkie ankiety z prośbą o informację zwrotną. Ankiety te będą wysyłane z taką częstotliwością i w taki sposób, aby nie były uciążliwe, oraz aby nie naruszały prawa do prywatności. W każdej chwili zrezygnować z otrzymywania informacji. Na tej podstawie dokonamy blokady przesyłania do Ciebie komunikatów (Art. 6 ust. 1 lit. b oraz f RODO, jako tzw. prawnie uzasadniony interes administratora, którym jest poprawa jakości usług oraz ich dostosowanie do potrzeb pacjentów).
Jako administrator danych będący przedsiębiorcą mamy prawo do dochodzenia roszczeń z tytułu prowadzonej przez nas działalności gospodarczej i tym samym przetwarzania Twoich danych w tym celu (Art. 6 ust. 1 lit. b oraz f RODO, jako tzw. prawnie uzasadniony interes administratora, którym jest dochodzenie naszych roszczeń i obrona naszych praw).
Jako przedsiębiorca prowadzimy także księgi rachunkowe oraz spoczywają na nas obowiązki podatkowe -wystawiamy np. rachunki za wykonane przez nas usługi, co może się wiązać z koniecznością przetwarzania danych osobowych (Art. 6 ust. 1 lit. c RODO w zw. z art. 74 ust. 2 ustawy z dnia 29 września 1994 r. o rachunkowości).

Na podstawie otrzymanych danych możemy kierować do Ciebie komunikację marketingową dotyczącą działalności Przychodni taką jak oferty, informacje o usługach, promocjach, wydarzeniach przez nas organizowanych czy artykuły o tematyce prozdrowotnej.
Bezwzględnie dbamy o poufność danych naszych Pacjentów. Jednak ze względu na konieczność zapewnienia nam odpowiedniej organizacji pracy w zakresie np. infrastruktury informatycznej w sprawach dotyczących naszej działalności jako przedsiębiorcy, jak również realizacji Twoich praw jako pacjenta, Twoje dane osobowe mogą być przekazywane następującym grupom odbiorców:

- innym podmiotom leczniczym, współpracującym z Przychodnią w celu zapewnienia ciągłości leczenia oraz dostępności opieki zdrowotnej w postaci placówek współpracujących z Przychodnią,
- dostawcom usług zaopatrujących Przychodnię w rozwiązania techniczne oraz organizacyjne, umożliwiające udzielanie świadczeń zdrowotnych oraz zarządzanie

naszą organizacją (w szczególności dostawcom usług teleinformatycznych, dostawcom sprzętu diagnostycznego, firmom kurierskim i pocztowym),
- dostawcom usług wspierających Przychodnię w obszarze marketingowym (agencje reklamowe, firmy realizujące wysyłkę sms oraz e-mail),
- dostawcom usług prawnych i doradczych oraz wspierających Przychodnię w dochodzeniu należnych roszczeń (kancelariom prawnym, firmom windykacyjnym),
- osobom upoważnionym przez Ciebie w ramach realizacji Twoich praw pacjenta.

W sprawach nieuregulowanych niniejszym Dokumentem mają zastosowanie przepisy RODO oraz Kodeksu cywilnego.

UDOSTĘPNIANIE DOKUMENTACJI MEDYCZNEJ

CEL

Celem procedury jest ujednolicenie sposobu postępowania w zakresie udostępniania dokumentacji medycznej.
HIH Przychodnia udostępnia dokumentację medyczną poprzez: jej wglądu w/m, sporządzanie wyciągów, odpisów, kopii, wydanie oryginałów.
Procedura obowiązuje pracowników Przychodni, mających kontakt z pacjentem, a w szczególności: lekarzy, pielęgniarki, pracowników rejestracji.

DEFINICJE I SKRÓTY

DM – indywidualna dokumentacja medyczna pacjenta.
Opiekun prawny – osoba ustanowiona przez Sąd, np. dla osób ubezwłasnowolnionych, małoletniego którego rodzice są pozbawieni władzy rodzicielskiej lub nie żyją. Opiekun prawny powinien przedstawić postanowienie Sądu Opiekuńczego, z którego wynikają jego uprawnienia.
Przedstawiciel ustawowy – rodzice małoletniego dziecka (pacjenta) pozostającego pod ich władzą rodzicielską albo z orzeczenia organu (orzeczenie z reguły wydawane jest przez sąd) np.: opiekun dziecka wyznaczony przez sąd, kurator dziecka, opiekun osoby ubezwłasnowolnionej wyznaczony przez sąd.
Opiekun faktyczny – osoba sprawująca bez obowiązku ustawowego stałą opiekę nad pacjentem, który ze względu na wiek, stan zdrowia albo stan psychiczny opieki takiej wymaga.
Osoba bliska – małżonek, krewny lub powinowaty do drugiego stopnia w linii prostej (krewni: ojciec, matka, babcia, dziadek, syn, córka, wnuczek, wnuczka; powinowaci: teść, teściowa), osoba pozostająca we wspólnym pożyciu lub osoba wskazana przez pacjenta.

SPOSÓB POSTĘPOWANIA

I. Informacje ogólne

1. Przychodnia udostępnia dokumentację medyczną poprzez:
a. wgląd w dokumentację medyczną - w miejscu jej znajdywania,
b. sporządzanie wyciągów, odpisów, kopii – z miejsca jej znajdywania,
c. wydanie oryginałów za pokwitowaniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu,
d. za pośrednictwem środków komunikacji elektronicznej,
e. na informatycznym nośniku danych (np. płyta CD, pendrive).

2. Dokumentacja medyczna jest udostępniana zgodnie z zapisami Ustawy o prawach pacjenta i Rzeczniku praw pacjenta wyłącznie osobom do tego upoważnionym na wniosek:

- pacjenta,
- przedstawiciela ustawowego,
- osób upoważnionych przez pacjenta,
- uprawnionych organów i instytucji.

II. Udzielanie informacji

1. Pacjent ma prawo do zachowania w tajemnicy przez osoby wykonujące zawód medyczny, w tym udzielające mu świadczeń zdrowotnych, informacji z nim związanych, a uzyskanych w związku z wykonywaniem zawodu medycznego.
2. Osoby wykonujące zawód medyczny są zobowiązane zachować w tajemnicy informacje związane z pacjentem, w szczególności ze stanem zdrowia pacjenta.
3. Osoby wykonujące zawód medyczny są zwolnione z zachowania w tajemnicy informacji związanych z pacjentem, w szczególności ze stanem zdrowia pacjenta, tylko w przypadku gdy:
   a) tak stanowią przepisy odrębnych ustaw,
   b) zachowanie tajemnicy może stanowić niebezpieczeństwo dla życia lub zdrowia pacjenta lub innych osób,
   c) pacjent lub jego przedstawiciel ustawowy wyraża zgodę na ujawnienie tajemnicy,
   d) zachodzi potrzeba przekazania niezbędnych informacji o pacjencie związanych z udzielaniem świadczeń zdrowotnych innym osobom wykonującym zawód medyczny, uczestniczącym w udzielaniu świadczeń,
   e) dochodzi do postępowania przed Wojewódzką komisją do spraw orzekania o zdarzeniach medycznych.

1. Osoby wykonujące zawód medyczny są związane tajemnicą również po śmierci pacjenta, chyba że zgodę na ujawnienie wyrazi osoba bliska.
1. Zwolnienia z tajemnicy nie stosuje się, jeśli ujawnieniu tajemnicy sprzeciwi się inna osoba bliska.

III. Udostępnianie dokumentacji medycznej - Pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielanych mu świadczeń zdrowotnych.

1. Udostępnianie oryginału dokumentacji medycznej

a) W przypadku wydania oryginałów dokumentacji należy pozostawić jej kopie, chyba, że zwłoka w jej przekazaniu mogłaby narazić pacjenta na szkodę.

b) Wydanie oryginału następuje na podstawie wniosku organu uprawnionego lub wniosku pacjenta, przedstawiciela ustawowego, osób upoważnionych przez pacjenta, z zastrzeżeniem zwrotu po wykorzystaniu i za pokwitowaniem.

2. Udostępnianie dokumentacji medycznej pacjentowi w trakcie leczenia w Przychodni:

a) Pacjent leczony/ badany w przychodni / przedstawiciel ustawowy / osoba upoważniona przez pacjenta ma prawo wglądu do dokumentacji medycznej pacjenta za pośrednictwem lekarza prowadzącego leczenie lub innej osoby upoważnionej przez kierownika Przychodni.

b) Dokumentacja jest udostępniana (kserokopia, odpis) na wniosek pacjenta / przedstawiciela ustawowego / osoby upoważnionej przez pacjenta; w przypadkach pilnych (np. komisja lekarska, sąd) – dokumentacja wydawana jest niezwłocznie.

c) Pisma/wnioski dotyczące pacjentów w ciągłości leczenia są przekazywane sekretarce medycznej celem przygotowania potwierdzonej za zgodność z oryginałem kserokopii dokumentacji lub oryginału (jeśli uprawniony podmiot tego żąda); następnie dokumentacja jest przekazywana do szaf archiwum i udostępniana dalej zgodnie z procedurą. W przypadkach pilnych – osoba wyznaczona w Przychodni przygotowuje dokumentację do wydania bez zbędnej zwłoki (np. komisje lekarskie, prokurator).

3. Udostępnianie dokumentacji medycznej pacjentowi w pracowniach diagnostycznych:
a) Wyniki badań diagnostycznych wykonane w trakcie leczenia są własnością HiH Przychodni i stanowią integralną część historii choroby; nie są tym samym własnością pacjenta i nie mogą być mu przekazane w oryginale.
b) Wyniki innych badań diagnostycznych odbierane są osobiście przez pacjenta, jego przedstawiciela ustawowego lub osobę upoważnioną.
4. Udostępnianie dokumentacji medycznej po jej zakończeniu i na wypadek śmierci pacjenta:
a) przychodnia udostępnia dokumentację medyczną pacjentowi, jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta.
b) Po śmierci pacjenta, prawo wglądu w dokumentację medyczną ma osoba upoważniona przez pacjenta za życia. Jeżeli pacjent nie wskazał takiej osoby, zgodę może wydać sąd lub prokurator.
c) Pacjent, jego przedstawiciel ustawowy lub osoba upoważniona do otrzymywania kopii dokumentacji medycznej, zwraca się z pisemnym wnioskiem o jej wydanie bezpośrednio do Kierownika przychodni. Wzór wniosku przedstawia **Wniosek o udostępnienie dokumentacji medycznej pacjenta - zał. 1.** Wniosek należy złożyć w Przychodni. Po pozytywnym zaopiniowaniu wniosku Kierownika i uiszczeniu należnej opłaty, zgodnie z Cennikiem – kopia dokumentacji medycznej jest wydawana.
d) Dokumentacja medyczna jest wydawana w terminie do 2 tygodni; w sprawach bardzo pilnych niezwłocznie.
5. Udostępnianie dokumentacji medycznej organom i podmiotom uprawnionym:
a) Udostępnianie dokumentacji pacjenta organom i podmiotom uprawnionym następuje na ich pisemny wniosek (zgodnie z zapisami Ustawy o prawach pacjenta i Rzeczniku praw pacjenta):

- podmiotom udzielającym świadczeń zdrowotnych w celu zapewnienia ciągłości świadczeń zdrowotnych (np.: kontynuacja leczenia w innym szpitalu, przychodni);
- organom władzy publicznej, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom krajowym i wojewódzkim w zakresie niezbędnym do wykonywania przez te podmioty ich zadań
- wojewodom, konsultantom krajowym, jednostkom organizacyjnym podległym lub nadzorowanym przez Ministra właściwego do spraw zdrowia w zakresie niezbędnym do przeprowadzenia kontroli na zlecenie wyżej wymienionego ministra;
- Ministrowi właściwemu do spraw zdrowia;
- Sądom, prokuraturom, lekarzom sądowym i rzecznikom odpowiedzialności zawodowej (np. DIL, DIPiP), w związku z prowadzonym postępowaniem;
- organom rentowym oraz zespołom do spraw orzekania o niepełnosprawności (np.: ZUS, KRUS);
- podmiotom prowadzącym rejestry usług medycznych, w zakresie niezbędnym do prowadzenie rejestrów;
- zakładom ubezpieczeń za zgodą pacjenta;
- komisjom lekarskim podległym ministrowi właściwemu do spraw wewnętrznych, wojskowym komisjom lekarskim, komisjom lekarskim Agencji Bezpieczeństwa Wewnętrznego lub Agencji Wywiadu, podległym Szefom właściwych Agencji;
- wojewódzkim komisjom do spraw orzekania o zdarzeniach medycznych;
- spadkobiercom w zakresie prowadzonego postępowania przed wojewódzką komisją do spraw orzekania o zdarzeniach medycznych.

b) Udostępnianie upoważnionym funkcjonariuszom policji, biegłym sądowym następuje po okazaniu nakazu prokuratora, upoważnienia i legitymacji służbowej.

ODPOWIEDZIALNOŚĆ

Za prawidłowe stosowanie procedury odpowiadają pracownicy Przychodni upoważnieni do udostępniania dokumentacji medycznej.

Za nadzór nad realizacją procedury odpowiada Dyrektor Przychodni.