POLITYKA
PRYWATNOŚCI I BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH W PRZYCHODNI REHABILITACYJNEJ FIT-MED SP. Z O.O.

wydana w dniu 25 maja 2018 roku przez FIT-MED Sp. z o.o.
na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz.U.2016.922 j.t oraz § 3 i § 4 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U 2004 nr 100, poz. 1024).

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych przez FIT-MED Sp. z o.o. zwaną dalej przychodnią lekarską przed zagrożeniami wewnętrznymi i zewnętrznymi.

Polityka obowiązuje wszystkich pracowników przychodni lekarskiej oraz dostawców, podmioty współpracujące z przychodnią lekarską na podstawie umowy cywilnoprawnej, mających kontakt z danymi osobowymi objętymi ochroną. Przetwarzanie danych osobowych odbywa się w przychodni lekarskiej w wersji papierowej oraz elektronicznej. Administratorem danych w przychodni lekarskiej jest FIT-MED Sp. z o.o. . Administratorem Bezpieczeństwa Informacji jest Jacek Bejrowski wyznaczony przez Administratora danych.

POJĘCIA:
1. Ustawa – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2016, poz. 922)
2. Administrator Danych Osobowych – rozumie się przez to przychodnię lekarską.
3. Administrator Bezpieczeństwa Informacji – osoba, która odpowiada za bezpieczeństwo danych osobowych w systemie informatycznym oraz tradycyjnym systemie, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
4. Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
5. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
6. Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów.
7. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

8. Identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
9. Hasło – ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
10. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
11. Integralność danych – funkcjonalność zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
12. Poufność danych – funkcjonalność zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

§ 1.

Wykaz zbiorów danych przetwarzanych w przychodni lekarskiej wymieniony jest w załączniku nr 1 do niniejszej polityki bezpieczeństwa, będącym jej integralną częścią.

§ 2.
Zakres danych osobowych przetwarzanych w przychodni lekarskiej.

1. W przychodni lekarskiej znajdują się następujące bazy danych (informatyczne):

Baza Pacjentów znajdująca się w chmurze serwisowanej i zabezpieczanej przez firmę Eurosoft Sp. z o.o.

2. W przychodni lekarskiej znajdują się następujące zbiory danych (tradycyjne-papierowe):

Zbiór danych zawierający dane Pacjenta (imię, nazwisko, wiek, PESEL, adres zamieszkania, nr kontaktowy) oraz jego wyniki badań, a także formularze zawierające zgody na zabieg igłowania oraz w niektórych przypadkach rozliczenia dot. Pacjenta z Przychodnią Rehabilitacyjną.

§ 3.
Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe.

1. Przetwarzanie danych osobowych odbywa się w przychodni rehabilitacyjnej w 84-200 Wejherowo, ul. I Brygady Pancernej oraz w jej filli w Sopocie przy ul. Dworcowej 7.
2. Dane osobowe są przetwarzane w następujących pomieszczeniach: recepcja Przychodni.

§ 4.
Zadania Administratora Danych Osobowych

1. Zadaniem Administratora Danych Osobowych jest czuwanie nad stosowaniem i przestrzeganiem w przychodni lekarskiej przepisów ustawy oraz nadzorowanie pracy Administratora Bezpieczeństwa Informacji.

2. Administrator danych osobowych nadaje i odwołuje upoważnienia do przetwarzania danych osobowych **(wzór załącznik nr 2 i 3)** oraz prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych (**wzór załącznik nr4)** .

§ 5.

Zadania Administratora Bezpieczeństwa Informacji

1. Ochrona i bezpieczeństwo danych osobowych zawartych w zbiorach prowadzonych sposobem tradycyjnym oraz poprzez system informatyczny.
2. Podejmowanie stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym.
3. Niezwłoczne informowanie Administratora Danych Osobowych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych.
4. Nadzór i kontrola systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.
5. Nadzór i kontrola systemu przetwarzania danych osobowych sposobem tradycyjnym.

§ 6.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1. Praktyka lekarska realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki informatyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza przed:
1) udostępnieniem ich osobom nieupoważnionym,
2) zabraniem przez osobę nieuprawnioną,
3) przetwarzaniem z naruszeniem ustawy, utratą, uszkodzeniem lub zniszczeniem.

2. Każda osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do pracy przy przetwarzaniu danych osobowych składa pisemne oświadczenie, że została zaznajomiona z przepisami ustawy z dnia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2016, poz.922), aktami wykonawczymi do w/w ustawy oraz, że rozumie zasady dotyczące ochrony danych osobowych opisane w Polityce bezpieczeństwa, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w przychodni lekarskiej oraz, że zobowiązuje się do ich przestrzegania. **(wzór oświadczenia załącznik nr 5)**.

Załącznik nr 1

do Polityki bezpieczeństwa
przychodni lekarskiej

Wykaz zbiorów danych przetwarzanych w przychodni lekarskiej FIT-MED Sp. z o.o.

Lp.	Nazwa zbioru danych (1)	Forma danych/Baza danych (2)	Zabezpieczenie informatyczne (3)	Nazwa programu służącego do przetwarzania danych osobowych (4)	Lokalizacja (nr pokoju)	Zabezpieczenie inne niż informatyczne
1.	Kartoteki Pacjentów (imię, nazwiska, PESEL, adres zamieszkania, wiek, nr kontaktowy)	Windows	hasło założone do komputera stacjonarnego oraz hasło do programu znajdującego się w chmurze	Eurosoft	komputer stacjonarny znajdujący się w recepcji	
2.	Kartoteki Pacjentów (imię, nazwiska, PESEL, adres zamieszkania, wiek, nr kontaktowy)	dokumenty papierowe	nie dotyczy	nie dotyczy	recepcja	szafka zabezpieczona zamkiem na klucz
3.	Formularze dot. Rozliczania usług z ubezpieczalnią (imię, nazwisko, PESEL, rodzaj wykonywanej usługi)	Windows	hasło nałożone na formularz rozliczeniowy	Excel	recepcja-komputer stacjonarny	
4.	Formularze dot.	dokumenty papierowe	nie dotyczy	nie dotyczy	recepcja	szafka zabezpieczon

	Rozliczania usług z ubezpieczalnią (imię, nazwisko, PESEL, rodzaj wykonywanej usługi)					a zamkiem na klucz

Opis:

(1) Nazwa zwyczajowa lub własna
(2) Windows, SQL, dokumenty papierowe
(3) Indywidualne hasło dostępu, wydzielona fizyczna sieć
(4) Np. kraty w oknach, alarm, drzwi antywłamaniowe, kontrola dostępu, ochrona całodobowa

Załącznik nr 2
do Polityki bezpieczeństwa
przychodni lekarskiej

Wzór upoważnienia imiennego do przetwarzania danych osobowych.

....., dnia .....

Upoważnienie imienne do przetwarzania danych osobowych w przychodni lekarskiej.....

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2016, poz. 922), upoważniam Panią/Pana

.....
(imię i nazwisko osoby upoważnionej)

zatrudnioną/niego w .....
(nazwa przychodni)
na stanowisku .....

do przetwarzania od dnia ..... danych osobowych w zakresie:

.....

.....
(podpis administratora danych osobowych)

Załącznik nr 3
do Polityki bezpieczeństwa
przychodni lekarskiej

Wzór odwołania upoważnienia imiennego do przetwarzania danych osobowych.

....., dnia .....

Odwołanie upoważnienia imiennego do przetwarzania danych osobowych w przychodni lekarskiej FIT-MED Sp. z o.o.

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2016, poz.922), odwołuję upoważnienie Pani/Pana
.....
(imię i nazwisko osoby upoważnionej)

zatrudnionej/niego w.....
(nazwa przychodni)
na stanowisku .....

do przetwarzania od dnia ..... danych osobowych w zakresie:
.....

i cofam prawo do korzystania z identyfikatora .....
(dotyczy tylko wersji elektronicznej).

.....
(podpis administratora danych osobowych)

Załącznik nr 4

do Polityki bezpieczeństwa
przychodni lekarskiej

Wzór

Ewidencja osób upoważnionych do przetwarzania danych osobowych w przychodni lekarskiej **..... .**

L. p.	Imię i nazwisko użytkownika	Identyfikator użytkownika (dotyczy wersji elektronicznej	Zakres uprawnień	Data nadania uprawnień	Data odebrania uprawnień	Przyczyna odebrania uprawnień	Podpis administratora danych lub ABI

Załącznik nr 5
do Polityki bezpieczeństwa
przychodni lekarskiej

Wzór

Oświadczenia osoby upoważnionej do przetwarzania danych osobowych w przychodni lekarskiej

....., dnia.....

OŚWIADCZENIE

Oświadczam, że przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona z przepisami ustawy z dnia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. z 2016, poz. 922), aktami wykonawczymi

do w/w ustawy. Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w Polityce bezpieczeństwa, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w przychodni lekarskiej..... i zobowiązuję się do ich przestrzegania.

.....

podpis

OBOWIĄZEK INFORMACYJNY ADMINISTRATORA DANYCH OSOBOWYCH SYSTEM MONITORINGU WIZYJNEGO

Zgodnie z art.13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L 2016 Nr 119, str. 1 ogólne rozporządzenie o ochronie danych, zwane dalej RODO), w szczególności art. 6 ust. 1 lit. f oraz art.22² § 1 ustawy z dnia 26 czerwca 1974 roku – Kodeks pracy, Centrum Medyczne Karpacz Spółka Akcyjna informuje, że Administratorem danych osobowych zawartych w systemie monitoringu wizyjnego (obraz) jest FIT-MED. SP. Z O.O. z siedzibą w Wejherowie ul. I Brygady Pancernej W.P. 10, zwana dalej Administratorem.

1. Przetwarzanie Pani/Pana danych jest niezbędne do celów wynikających z prawnie uzasadnionych interesów Administratora (podniesienia bezpieczeństwa ludzi i mienia), ochrony żywotnych interesów osób przebywających na terenie Przychodni Rehabilitacyjnej FIT-MED. Sp. z o.o. oraz zabezpieczenie materiału dowodowego w przypadkach zarejestrowania zdarzeń niezgodnych z prawem.
2. Zakres operacji dokonywanych w systemie nagrywania obrazu bez dźwięku to: zapisywanie, przeglądanie, udostępnianie, usuwanie.
3. Zapisy z monitoringu wizyjnego będą przechowywane przez okres do 90 dni, po którym zostaną trwale usunięte.
4. Pani/Pana dane osobowe nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu.
5. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego.
6. Przysługuje Pani/Panu prawo wniesienia skargi do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych, w przypadku gdy przetwarzanie Pani/Pana danych osobowych naruszają przepisy dotyczące danych osobowych.
7. Pani/Pana dane będą mogły być przekazywane wyłącznie podmiotom uprawnionym do uzyskania danych osobowych na podstawie przepisów prawa (Policja, Sąd, Prokuratura) na pisemny w niosek ze strony tych instytucji.
8. Osoba zainteresowana zabezpieczeniem danych z systemu monitoringu wizyjnego na potrzeby przyszłego postępowania może zwrócić się pisemnie do Administratora z prośbą o ich zabezpieczenie przed usunięciem po upływie standardowego okresu ich przechowywania. Wniosek należy złożyć do Inspektora Ochrony Danych Osobowych

w siedzibie Administratora, w terminie do 3 dni licząc od dnia, w którym zdarzenie mogło być zarejestrowane (oznacza to dzień wystąpienia zdarzenia). Wniosek można złożyć osobiście, drogą elektroniczną na adres: fitmed@onet.eu lub pocztą tradycyjną.

9. Odpowiedź na wniosek otrzyma Pani/Pan bez zbędnej zwłoki, najpóźniej w ciągu miesiąca od wpłynięcia wniosku.