INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
VitalMed

grupowej praktyce fizjoterapeutów wykonywanej w ramach indywidualnych działalności gospodarczych prowadzonych przez:

Jakuba Mędralę
prowadzącego działalność gospodarczą pod firmą
JAKUB MĘDRALA VITALMED FIZJOTERAPIA&OSTEOPATIA
NIP 7471737488

Marcina Witkowskiego
prowadzącego działalność gospodarczą pod firmą
VitalMed FIZJOTERAPIA&OSTEOPATIA Marcin Witkowski

sporządzona
w dniu 01.04.2019
we Wrocławiu

Niniejsza *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych VitalMed przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 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 (dalej RODO).

Definicje:

1. **Administrator Danych**

a) Jakub Mędrala - Wrocław, Kunickiego, 57A, 54 - 616
b) Marcin Witkowski - Wrocław, Kunickiego, 57A, 54 - 616

2. **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
3. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu Przetwarzania danych
4. **Użytkownik** – osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych w VitalMed.
5. **Sieć lokalna** – połączenie Systemów informatycznych Administratora Danych wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych

6. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie
7. **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
8. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem
9. **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie

10. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi)

I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1. Za bezpieczeństwo Danych osobowych w Systemie informatycznym VitalMed i za właściwy nadzór odpowiedzialny jest Administrator Danych.
2. Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora Danych,
3. Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4. Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5. Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6. Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.

II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1. W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfikator użytkownika.
2. Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.

3. Minimalna długość Hasła przydzielonego Użytkownikowi wynosi 10 znaków alfanumerycznych i znaków specjalnych.
4. Zabrania się używania identyfikatora lub Hasła drugiej osoby.
5. Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
a) daty pierwszego wprowadzenia danych do systemu,
b) identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu,
c) informacji o odbiorcach, którym Dane osobowe zostały udostępnione.

III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przez Użytkowników systemu

1. Pracownik po przyjściu do pracy uruchamia stację roboczą.
2. Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3. Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4. W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
5. Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

IV. Tworzenie kopii zapasowych Zbiorów danych

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach VitalMed.
2. Do archiwizacji służy platforma internetowa IGabinet.
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.

V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających Dane osobowe oraz kopii zapasowych

1. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
2. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.
3. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
4. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
5. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

VI. Sposób zabezpieczenia Systemu informatycznego przed działalnością wirusów komputerowych, nieuprawnionym dostępem oraz awariami zasilania

1. System informatyczny jest zabezpieczony przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawionego dostępu oraz przed działaniami inicjowanymi z sieci zewnętrznej. Zabezpieczenie obejmuje:

A) Obszar chroniony - Stacje robocze:
Rodzaj ochrony:

1. System antywirusowy
2. Firewall
3. Szyfrowanie nośników danych

B) **Obszar chroniony -** Sieć Wewnętrzna:

1. System antywirusowy
2. Firewall

C) **Obszar chroniony -** Poczta e – mail:
1. Szyfrowanie danych
2. System antiwirusowy i antyspamowy

2. Użytkowany system jest automatycznie skanowany z częstotliwością 7 dni
3. Aktualizacja bazy wirusów odbywa się poprzez automatyczne pobieranie bazy wirusów przez program antywirusowy.
4. W przypadku wykrycia wirusa należy:
a) uruchomić program antywirusowy i skontrolować użytkowany system,
b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.
Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
a) zakończyć pracę w systemie komputerowym,
b) odłączyć zainfekowany komputer od sieci,
c) powiadomić o zaistniałej sytuacji Administratora Danych lub ABI.
5. Urządzenia i nośniki zawierające Dane osobowe przekazywane poza obszar, w którym są one przetwarzane, zabezpiecza się w sposób zapewniający poufność i integralność danych.

VII. Poczta elektroniczna

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3. Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy

bądź z podejrzanym tytułem (tzw. *phishing e-mail*). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII. Sposoby realizacji w systemie wymogów dotyczących Przetwarzania danych (sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych)

1. Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2. Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3. Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1. Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.
2. Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,
b) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
c) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych,
d) w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do Danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia danych osobowych.

JAKUB MĘDRALA **Marcin Witkowski**