CENTRUM REHABILITACJI
im. Prof. Mieczysława Walczaka
w Osiecznej
64-113 Osieczna, ul. Zamkowa 2
tel./fax 65 520 34 95, 535 04 77, 535 03 49
NIP: 697-18-85-702

Polityka Bezpieczeństwa

2016/0001

CENTRUM REHABILITACJI IM. PROF. MIECZYSŁAWA WALCZAKA W OSIECZNEJ,

OSIECZNA ZAMKOWA 2

Osieczna, 2016

Dział A

Postanowienia wstępne.

§1

Polityka Bezpieczeństwa - zwana również w dalszej części dokumentu, jako PB - została wydana w oparciu o treść i w celu realizacji postanowień następujących aktów prawnych:

a) ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. t.j. 2002.101.926 z późn. zm.) - zwana również w dalszej części PB, jako ustawa,

b) rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. (Dz.U. 2004.100.1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – zwane również w dalszej części PB, jako rozporządzenie.

§2

W odniesieniu do CENTRUM REHABILITACJI IM. PROF. MIECZYSŁAWA WALCZAKA W OSIECZNEJ, OSIECZNA ZAMKOWA 2 w PB używane jest również określenie Świadczeniodawca.

§3

1. Polityka Bezpieczeństwa jest dokumentem jawnym niezawierającym szczegółów technicznych zabezpieczenia i przetwarzania danych osobowych.
2. Szczegóły techniczne o których mowa w ust. 1 uregulowane są w dokumencie poufnym – Instrukcji Zarządzania Systemem Informatycznym.

§4

1. PB określa zasady postępowania przy przetwarzaniu danych osobowych:
   a) dotyczących stanu zdrowia pacjentów i przetwarzanych w związku z udzielaniem usług medycznych, a gromadzonych w dokumentacji medycznej (Dział B Polityki Bezpieczeństwa) – wobec których Świadczeniodawca jest Administratorem Danych Osobowych,
   b) dotyczących stanu zdrowia pacjentów, a przetwarzanych poza dokumentacją medyczną w związku z obowiązkiem przekazywania danych przez Świadczeniodawców podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych i gromadzonych w dokumentach rozliczeniowych oraz raportach,a także przetwarzanych w ramach list osób oczekujących na świadczenie (Dział C Polityki Bezpieczeństwa) – wobec których Świadczeniodawca jest Administratorem Danych Osobowych,
   c) kandydatów do pracy, pracowników Świadczeniodawcy oraz osób świadczących na jego

rzecz usługi w oparciu o umowy cywilnoprawne (Dział D Polityki Bezpieczeństwa) – wobec których Świadczeniodawca jest Administratorem Danych Osobowych,

d) przetwarzanych przez Świadczeniodawcę w ramach zbioru jego kontrahentów (Dział E Polityki Bezpieczeństwa) – wobec, których Świadczeniodawca jest Administratorem Danych Osobowych.

2. W zbiorach danych osobowych szczegółowo opisanych w Działach B – E przetwarza się następujące grupy danych osobowych:
   a) wrażliwe dane osobowe przetwarzane przez Świadczeniodawcę w związku z udzielaniem usług medycznych oraz w związku z zatrudnieniem lub ubieganiem się u niego o zatrudnienie,
   b) niewrażliwe dane osobowe przetwarzane przez Świadczeniodawcę w związku z zawieraniem przez niego umów cywilnoprawnych z jego kontrahentami,
3. Dział A Polityki Bezpieczeństwa zawiera postanowienia wspólne dla sytuacji przetwarzania danych osobowych opisanych w Działach B – E .

§5

PB określa zasady przetwarzania oraz zabezpieczenie danych osobowych, których Administratorem jest Świadczeniodawca, a także prawa osób fizycznych, których dane osobowe dotyczą.

§6

1. Zapewnienie bezpieczeństwa przetwarzanych przez Świadczeniodawcę danych osobowych jest priorytetem jego działalności i w zakresie ochrony danych o stanie zdrowia jego pacjentów stanowi jeden z aspektów realizacji obowiązku ochrony tajemnicy zawodowej lekarza wyrażonej w treści art. 40 ustawy z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty.
2. Świadczeniodawca przestrzega zapisów Polityki Bezpieczeństwa, a także zobowiązuje do jej przestrzegania swoich pracowników oraz osoby zatrudnione na podstawie umów cywilnoprawnych.
3. Naruszenie przez pracowników Świadczeniodawcy lub osoby współpracujące z nim na podstawie umów cywilnoprawnych zapisów zawartych w PB lub w Instrukcji Zarządzania Systemem Informatycznym traktowane będzie przez niego, jako ciężkie naruszenie podstawowych obowiązków umownych.

§7

Świadczeniodawca przetwarza dane osobowe w sposób zapewniający ich:

a) poufność – co oznacza, iż dane te nie są udostępniane nieupoważnionym podmiotom,
b) integralność – co oznacza, iż dane te nie zostaną zmienione lub zniszczone w nieautoryzowany sposób,
c) rozliczalność - co oznacza, iż zabezpieczenia dotyczące danych będą charakteryzowały się właściwością, która zapewnia, iż działania danego podmiotu w stosunku do danych zawsze będą przypisane, w sposób jednoznaczny, tylko temu podmiotowi.

§8

1. Systemy informatyczne w których przetwarzane są dane osobowe wobec których Świadczeniodawca jest Administratorem są połączone z siecią publiczną w rozumieniu prawa telekomunikacyjnego.
2. Świadczeniodawca w celu prawidłowego zabezpieczenia danych osobowych wdraża wysoki – w rozumieniu rozporządzenia - poziom bezpieczeństwa przetwarzania danych osobowych w użytkowanych przez siebie systemach informatycznych.

§9

Przesyłanie danych osobowych, w sieci publicznej, wobec których Administratorem jest Świadczeniodawca następuje wyłącznie w postaci szyfrowanej .

§10

Świadczeniodawca:

a) podejmuje permanentne działania w zakresie identyfikacji i analizy zagrożeń oraz ryzyka na które mogą być narażone przetwarzane u Świadczeniodawcy dane osobowe,
b) definiuje potrzeby w zakresie zabezpieczenia danych osobowych z uwzględnieniem potrzeby kryptograficznej ochrony tych danych – w szczególności w trakcie przesyłania tych danych za pomocą urządzeń teletransmisji danych,
c) określa zabezpieczenia adekwatne do zagrożeń i ryzyka,
d) monitoruje w sposób permanentny działanie wdrożonych zabezpieczeń i niezwłocznie koryguje ewentualne błędy we wdrożonych zabezpieczeniach,
e) opracowuje i wdraża program szkoleń, osób zatrudnionych lub współpracujących z Świadczeniodawcą, a dotyczących problematyki ochrony danych osobowych.

§11

Świadczeniodawca opracowuje instrukcję określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych - ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji. Instrukcja zawiera w szczególności:

a) określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany,
b) określenie sposobu rejestrowania i wyrejestrowywania użytkowników oraz nadawania uprawnień,
c) opis zastosowanych metod i środków uwierzytelnienia,
d) procedury rozpoczęcia i zakończenia pracy – logowania i wylogowania z systemu,
e) metodę i częstotliwość tworzenia kopii zapasowych,
f) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz sposób ich usuwania,
g) sposób i czas przechowywania nośników informacji, w tym kopii informatycznych

i wydruków,

h) sposób dokonywania przeglądów i konserwacji systemu oraz zbiorów danych osobowych,

i) procedurę dotyczącą zarządzania użytkownikami systemu,

j) procedurę komunikacji wewnątrz sieci komputerowej.

§12

1. Świadczeniodawca wyznacza Administratora Bezpieczeństwa Informacji (ABI). Administrator Bezpieczeństwa Informacji jest osobą odpowiedzialną za bezpieczeństwo danych osobowych w systemie informatycznym, a w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.
2. Ilekroć PB adresuje określone obowiązki lub kompetencje - w zakresie odnoszącym się do stosowania środków technicznych oraz organizacyjnych zapewniających ochronę przetwarzanych danych osobowych – do Świadczeniodawcy (określanej również, jako ADO), to zapisy te adresowane są również do ABI.

§13

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby, którym ADO udzielił pisemnego upoważnienia do przetwarzania tych danych. Upoważnienie do przetwarzania danych osobowych określa w jakim celu oraz w jakim zakresie dana osoba uzyskała kompetencję do przetwarzania danych osobowych (np. praca na stanowisku rejestratorki, wykonywanie czynności z zakresu tzw. kadr i płac).
2. Przed udzieleniem danej osobie upoważnienia do przetwarzania danych osobowych bierze się pod uwagę w szczególności to, czy dana osoba charakteryzuje się cechą dyskrecji oraz, czy jej dotychczasowe zachowanie i wykonywanie dotychczasowych obowiązków daje rękojmię przestrzegania PB oraz innych dokumentów regulujących zabezpieczenie i ochronę danych osobowych przetwarzanych przez Świadczeniodawcę.
3. Udzielenie danej osobie upoważnienia do przetwarzania danych osobowych uzależnione jest od uprzedniego zobowiązania się przez tą osobę do zachowania w poufności treści przetwarzanych danych osobowych.
4. Świadczeniodawca prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
5. Upoważnienia do przetwarzania danych osobowych, zobowiązania osób upoważnionych do zachowania w poufności treści danych oraz ewidencja osób upoważnionych – przechowywane są w Budynek: Budynek Główny - Zamek, Pokój: Sekretariat i Kadry - Budynek Główny - Zamek.
6. Ewidencja osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym prowadzona jest również w postaci elektronicznej.
7. Osobom posiadającym tytuł zawodowy lekarza, pielęgniarki, położnej i wykonującym pracę na tych stanowiskach z uwagi na to, iż posiadają upoważnienie do uzyskiwania i przetwarzania danych zawartych w dokumentacji medycznej, wynikające wprost z treści art. 24 ust. 2 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, nie udziela się

upoważnień o których mowa w ustępach powyżej. Od osób o których mowa w zdaniu poprzednim odbiera się natomiast zobowiązania do zachowania w poufności treści danych pozyskanych z dokumentacji medycznej, a także uwzględnia się te osoby w treści ewidencji osób upoważnionych do przetwarzania danych osobowych.

§14

W stosunku do każdej osoby zatrudnionej przy przetwarzaniu danych osobowych (czy to na podstawie umowy o pracę, czy też na podstawie umowy cywilnoprawnej) określony zostaje, w treści upoważnienia, zakres odpowiedzialności za ochronę danych przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem – w stopniu odpowiednim do zadań tej osoby przy przetwarzaniu danych. W przypadku stwierdzenia braku wiarygodności osoby dopuszczonej do przetwarzania danych osobowych (stwierdzenie braku dbania o zachowanie w poufności treści przetwarzanych danych osobowych) Świadczeniodawca niezwłocznie blokuje dostęp tej osoby do zbioru danych osobowych.

§15

1. Każda osoba przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych zostaje zaznajomiona z przepisami dotyczącymi ochrony danych osobowych, a w szczególności z przepisami dotyczącymi zasad przetwarzania i zabezpieczenia danych osobowych oraz przepisami karnymi zamieszczonymi w ustawie.
2. Świadczeniodawca zapewnia osobom dopuszczonym do pracy przy przetwarzaniu danych osobowych dostęp do aktualnych tekstów aktów prawnych regulujących problematykę przetwarzania danych osobowych. Teksty aktów prawnych dostępne są w postaci wydruków oraz w sieci wewnętrznej Świadczeniodawcy.
3. Obowiązek przestrzegania treści przepisów regulujących problematykę danych osobowych wprowadzony zostaje do treści stosunku umownego łączącego Świadczeniodawcę z osobą dopuszczoną do pracy przy przetwarzaniu danych osobowych – poprzez uzupełnienie w tym przedmiocie zakresu obowiązków danej osoby.
4. Osoby dopuszczone do pracy przy przetwarzaniu danych osobowych podlegają okresowym szkoleniom obejmującym zagadnienia związane z ochroną danych osobowych oraz ochroną tajemnicy przedsiębiorstwa.

§16

Świadczeniodawca określa pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem sprzętu komputerowego, a także miejsca w których przechowywane są dane osobowe utrwalone w postaci pisemnej.

§17

1. W pomieszczeniach w których przetwarzane są dane osobowe, w godzinach otwarcia lokalu użytkowanego przez Świadczeniodawcę, zawsze jest obecna przynajmniej jedna osoba upoważniona do przetwarzania danych i odpowiedzialna za ich zabezpieczenie przed wglądem lub zabraniem przez osoby nieupoważnione. Jeżeli w danym pomieszczeniu nie jest obecna osoba o której mowa w zdaniu poprzednim pomieszczenie musi zostać wcześniej zamknięte.
2. Pomieszczenia w których są przetwarzane dane osobowe, poza godzinami pracy Świadczeniodawcy, są zawsze zamykane.
3. Wstęp do pomieszczeń w których przetwarzane są dane osobowe mają wyłącznie osoby upoważnione przez Świadczeniodawcę.
4. W przypadku osób nie posiadających upoważnienia do przetwarzania danych osobowych może być wydane upoważnienie dostępu do pomieszczenia, ale tylko przy założeniu, że wszystkie zbiory danych osobowych znajdujące się w tym pomieszczeniu zostały odpowiednio zabezpieczone w sposób uniemożliwiający wgląd przez osoby nieuprawnione.

§18

Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, a zasilane energią elektryczną, są zabezpieczone przed zaprzestaniem pracy i utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

§19

1. Komputery stacjonarne wykorzystywane przy przetwarzaniu danych osobowych i wyposażone w nośniki informacji zawierające dane osobowe - nie mogą być wynoszone poza obszar wyznaczony do przetwarzania danych osobowych z uwzględnieniem zasad przyjętych w punkcie 4.4 Instrukcji Zarządzania Systemem Informatycznym.
2. Komputery przenośne wykorzystywane przy przetwarzaniu danych osobowych mogą być wynoszone poza obszar przetwarzania danych osobowych wyłącznie w przypadku zaistnienia uzasadnionej przyczyny. W sytuacji, o której mowa w zdaniu poprzednim, przed wyniesieniem komputera przenośnego poza obszar przetwarzania danych osobowych, dane osobowe powinny zostać wcześniej zaszyfrowane.
3. Zapisy o których mowa w ust. 2 stosuje się odpowiednio do sytuacji wynoszenia, poza obszar przetwarzania danych, nośników na których przetwarzane są dane osobowe (np. przenośne dyski twarde, pamięci flash, karty SD).

§20

Urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe, a przeznaczone do:

a) likwidacji – pozbawia się wcześniej zapisu danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie,
b) przekazania innemu podmiotowi (który nie jest uprawniony do przetwarzania danych

osobowych) – pozbawia się wcześniej zapisu danych,

c) naprawy – pozbawia się przed naprawą zapisu danych albo naprawia się je pod nadzorem osoby upoważnionej do przetwarzania danych.

§21

Wydruki zawierające dane osobowe przeznaczone do usunięcia niszczy się w sposób uniemożliwiający ich odczytanie.

§22

Kopie zapasowe:

a) przechowuje się w innym pomieszczeniu, aniżeli przechowywane są zbiory danych osobowych eksploatowane na bieżąco,

b) sprawdza się okresowo pod względem ich dalszej przydatności do odtworzenia danych w razie awarii systemu,

c) bezzwłocznie usuwa się po ustaniu ich użyteczności.

§23

1. Ekrany monitorów stanowisk dostępu do danych osobowych są automatycznie wyłączane po upływie ustalonego czasu nieaktywności użytkownika.
2. Ekrany monitorów wykorzystywanych w działalności Świadczeniodawcy są ustawiane w sposób uniemożliwiający podejrzenie wyświetlanej treści przez osoby trzecie.

§24

System informatyczny, w którym przetwarzane są dane osobowe wyposażony jest w mechanizmy uwierzytelnienia użytkownika (weryfikacja deklarowanej tożsamości osoby ubiegającej się o dostęp do danych) oraz kontroli dostępu do danych osobowych, przy czym:

a) każdy użytkownik systemu informatycznego w którym przetwarzane są dane osobowe posiada ustalony, odrębny, identyfikator (ciąg znaków literowych, cyfrowych lub innych, a jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym) oraz hasło (ciąg znaków literowych, cyfrowych lub innych, a znanych jedynie osobie uprawnionej do pracy w systemie informatycznym),

b) identyfikator wpisywany jest wraz z imieniem i nazwiskiem do ewidencji użytkowników oraz rejestrowany jest w systemie informatycznym,

c) bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym możliwy jest wyłącznie po podaniu identyfikatora i właściwego hasła,

d) częstotliwość zmiany hasła użytkownika określa Instrukcja Zarządzania Systemem Informatycznym,

e) identyfikator użytkownika jest niezmienny, a po wyrejestrowaniu użytkownika z systemu

informatycznego nie może być przydzielony innej osobie,

f) hasła użytkownika umożliwiające dostęp do systemu informatycznego, mają charakter poufny - również po upływie terminu ich ważności,

g) identyfikator użytkownika, który utracił uprawnienia dostępu do danych osobowych, jest niezwłocznie wyrejestrowywany z systemu informatycznego, a jego hasło jest unieważniane - osoba taka nie ma dostępu do danych osobowych.

§25

1. Na podstawie art. 31 ustawy, w drodze umowy zawartej na piśmie, Świadczeniodawca może powierzyć przetwarzanie danych osobowych, zapisanych w systemie informatycznym, przedsiębiorcy zajmującemu się serwisowaniem oprogramowania komputerowego wspomagającego pracę Świadczeniodawcy - w celu wykonania zdalnej usługi serwisowej z której wykonaniem łączy się konieczność wglądu do zawartości bazy danych.
2. Przed powierzeniem do przetwarzania danych każdorazowo określa się datę i godzinę zdalnego połączenia serwisanta z bazą danych Świadczeniodawcy. Zdalny dostęp do bazy danych zawsze jest dostępem nadzorowanym przez Świadczeniodawcę lub jego pracownika, który na ekranie monitora (jeżeli to technicznie możliwe) obserwuje jakie czynności są wykonywane przez serwisanta w trybie zdalnego połączenia. Zdalny dostęp do bazy danych Świadczeniodawcy dokonywany jest wyłącznie z wykorzystaniem połączenia szyfrowanego. Po wykonaniu usługi serwisowej możliwość zdalnego połączenia jest wyłączana.
3. Świadczeniodawca może powierzyć przetwarzanie danych wyłącznie przedsiębiorcy, który oświadczył, iż podjął wcześniej środki zabezpieczające zbiór przetwarzanych danych osobowych zgodnie z przepisami o których mowa w treści art. 36 – 39 ustawy, a także spełnia wymagania określone w treści rozporządzenia.

§26

System informatyczny, w którym przetwarzane są dane osobowe zapewnia kontrolę nad tym:

a) jakie dane osobowe zostały do zbioru wprowadzone,

b) kiedy dane osobowe zostały do zbioru wprowadzone,

c) przez kogo dane osobowe zostały do zbioru wprowadzone,

d) komu dane zostały przekazane.

§27

Następujące Załączniki stanowią integralną część Polityki Bezpieczeństwa:

a) Załącznik 1 - Wykaz budynków, pomieszczeń i części pomieszczeń, w których przetwarzane są dane osobowe,

b) Załącznik 2 - Wykaz zbiorów danych osobowych ze wskazaniem programów zastosowanych do przetwarzania danych,

c) Załącznik 3 - Opis struktury zbiorów danych,

d) Załącznik 4 - Sposób przepływu danych pomiędzy systemami w ramach Systemu Informatycznego,
e) Załącznik 5 - Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

Dział B

Dane osobowe dotyczące stanu zdrowia pacjentów Świadczeniodawcy, a przetwarzane w ramach dokumentacji medycznej.

§1

1. Świadczeniodawca prowadzi dokumentację medyczną osób korzystających z udzielanych przez niego świadczeń zdrowotnych. Dokumentacja medyczna obejmuje dane i informacje medyczne odnoszące się do stanu zdrowia pacjenta lub udzielonych pacjentowi przez Świadczeniodawcę świadczeń zdrowotnych. Pacjent jest identyfikowany w treści dokumentacji medycznej między innymi poprzez wskazanie jego imienia i nazwiska, adresu zamieszkania oraz numeru PESEL.
2. Sposób prowadzenia dokumentacji medycznej i szczegółową treść wpisów w niej zawartych określa ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz rozporządzenia wykonawcze do przepisów regulujących prowadzenie dokumentacji medycznej. Świadczeniodawca prowadzi dokumentację w sposób zgodny z tymi przepisami.
3. Dane zawarte w dokumentacji medycznej Świadczeniodawca przetwarza w celu udzielania usług medycznych - w oparciu o treść i w granicach art. 27 ust. 2 pkt 7 ustawy o ochronie danych osobowych.
4. Świadczeniodawca tworzy dokumentację medyczną w użytkowanym przez siebie systemie informatycznym wspomagającym jego pracę, a następnie drukuje treść dokumentacji i podpisuje odręcznie zgodnie z wymogami przepisów regulujących prowadzenie dokumentacji medycznej. Świadczeniodawca prowadzi dokumentacje medyczną w postaci elektronicznej zgodnie z przepisami, o których mowa w ust. 2 powyżej.
5. Zapewnienie ochrony danych zawartych w treści dokumentacji medycznej jest priorytetem Świadczeniodawcy.

§2

1. Świadczeniodawca przechowuje dokumentacje medyczną przez okresy, o których mowa w art. 29 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Po upływie okresów, o których mowa w zdaniu poprzednim, Świadczeniodawca niszczy dokumentację w sposób uniemożliwiający identyfikacje pacjenta, którego dotyczyła – w przypadku dokumentacji prowadzonej w postaci tradycyjnej zniszczenia dokonuje się z wykorzystaniem niszczarek, a w przypadku dokumentacji prowadzonej w postaci elektronicznej zniszczenia dokonuje się poprzez trwałe usunięcie z nośnika danych.
2. Świadczeniodawca udostępnia dokumentacje medyczną podmiotom uprawnionym w świetle art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Dokumentacje medyczną udostępnia się w następujący sposób:
   a) do wglądu w siedzibie podmiotu udzielającego świadczeń zdrowotnych,
   b) poprzez sporządzenie jej wyciągów, odpisów lub kopii – zasady odpłatności reguluje ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta,

c) poprzez wydanie oryginału za pokwitowaniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu oraz wcześniejszym wykonaniem kopii wydawanej dokumentacji – oryginały dokumentacji wydawane są wyłącznie organom lub podmiotom uprawnionym do żądania oryginałów (np. sądy, prokuratura).

3. W przypadku:
   a) udostępniania dokumentacji przedstawicielowi ustawowemu pacjenta Świadczeniodawca - przed udostępnieniem dokumentacji – weryfikuje, czy dana osoba w rzeczywistości jest przedstawicielem ustawowym pacjenta, a następnie sporządza notatkę składaną do dokumentacji w której zaznacza komu, w jakiej dacie i na jakiej podstawie udostępniono dokumentację medyczną (do notatki załącza się kopie dokumentu z którego wynika umocowanie do działania w charakterze przedstawiciela ustawowego pacjenta – np. postanowienie Sądu o ustanowieniu opiekuna),
   b) udostępniania dokumentacji osobie upoważnionej przez pacjenta - przed udostępnieniem dokumentacji - Świadczeniodawca weryfikuje tożsamość osoby wymienionej w treści upoważnienia z tożsamością osoby posługującej się upoważnieniem, a następnie sporządza notatkę składaną do dokumentacji w której zaznacza komu, w jakiej dacie i na jakiej podstawie udostępniono dokumentację medyczną (do notatki załącza się kopię przedstawionego upoważnienia),
4. W sytuacji, gdy podstawą dla udostępnienia dokumentacji jest dokument (np. postanowienie Sądu, upoważnienie, umowa zawarta z zakładem ubezpieczeń upoważniająca zakład do wglądu w dokumentację po śmierci pacjenta) udostępnienie dokumentacji może nastąpić po okazaniu oryginału danego dokumentu lub jego kopii poświadczonej za zgodność z oryginałem przez notariusza.

Dział C

Dane osobowe dotyczące stanu zdrowia pacjentów Świadczeniodawcy, a przetwarzane poza dokumentacją medyczną w związku z raportowaniem do instytucji finansującej powszechne ubezpieczenie zdrowotne.

§1

1. Na podstawie art. 190 ust. 1 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. j.t. 2008.164.1027 z późn. zm.) Świadczeniodawca gromadzi, a następnie przekazuje podmiotowi finansującemu ze środków publicznych - powszechne ubezpieczenie zdrowotne - dane zdefiniowane w treści rozporządzenia Ministra Zdrowia z dnia 20 czerwca 2008 r. w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych (Dz.U. 2008.123.801 z późn. zm.).
2. Realizując obowiązek, o którym mowa w ust. 1 Świadczeniodawca prowadzi w postaci elektronicznej:
   a) Rejestr Świadczeń Opieki Zdrowotnej,
   b) Rejestr Deklaracji POZ,
   c) Listy Oczekujących Na Udzielenie Świadczenia.
3. Na dane osobowe przetwarzane w ramach rejestrów i list, o których mowa w ust. 2 składają się dane osobowe pacjentów (w tym dane o ich stanie zdrowia) oraz dane osobowe osób udzielających świadczenia zdrowotnego.
4. Dane, o których mowa w ust. 2 Świadczeniodawca przekazuje do instytucji finansującej ze środków publicznych świadczenia zdrowotne w postaci komunikatu elektronicznego. Komunikaty elektroniczne przechowywane są w systemie informatycznym wspomagającym pracę Świadczeniodawcy. Komunikat elektroniczny przekazywany jest instytucji finansującej ze środków publicznych świadczenia zdrowotne:
   a) w drodze teletransmisji. Teletransmisja danych ma charakter szyfrowany.
5. Świadczeniodawca przetwarza dane osobowe, o których mowa w niniejszym § wyłącznie w celu przekazania ich podmiotowi finansującemu ze środków publicznych świadczenia zdrowotne - tak, aby podmiot ten mógł realizować swoje zadania wynikające z ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych w zakresie monitorowania, planowania, zarządzania i rozliczania świadczeń zdrowotnych. Świadczeniodawca nie przekazuje innym podmiotom tych danych, poza sytuacją, gdy przekazania danych żądają podmioty upoważnione do tego na podstawie szczególnych przepisów powszechnie obowiązującego prawa (np. organy ścigania, sądy).
6. Dane osobowe o których mowa w niniejszym Dziale Polityki Bezpieczeństwa przetwarzane są na podstawie przepisów, o których mowa w ustępach powyżej niniejszego paragrafu oraz w oparciu o treść art. 27 ust. 2 pkt 7 ustawy.

Dział D

Dane osobowe przetwarzane przez Świadczeniodawcę w ramach zbioru danych osobowych kandydatów do pracy, pracowników Świadczeniodawcy oraz osób świadczących na jego rzecz usługi w oparciu o umowy cywilnoprawne.

§1

Świadczeniodawca przetwarza dane osobowe osób ubiegających się u niego o zatrudnienie, pracowników, współpracowników.

§2

1. Świadczeniodawca przetwarza dane osobowe kandydatów do pracy oraz dane osobowe pracowników w zakresie w jakim zezwala na to treść art. 22(1) Kodeksu pracy.
2. Dane osobowe, których przetwarzanie nie znajduje uzasadnienia w świetle przepisu art. 22(1) Kodeksu pracy przetwarzane są przez Świadczeniodawcę wyłącznie na podstawie zgody osoby, której dane dotyczą - zgoda może być wyrażona w dowolnej formie.
3. W przypadku przetwarzania danych osobowych, których treść wykracza poza dyspozycję art. 22(1) Kodeksu pracy Świadczeniodawca każdorazowo informuje osobę, której dane dotyczą o braku obowiązku wyrażenia zgody na przetwarzanie tych danych.
4. Postanowienia ust. 1 – 3 stosuje się odpowiednio do osób współpracujących z Świadczeniodawcą na podstawie umów cywilnoprawnych.

§3

1. Dane osobowe kandydatów do pracy przetwarzane są wyłącznie przez czas trwania i w celu rekrutacji danego kandydata do pracy. W przypadku negatywnego zakończenia procedury rekrutacji danej osoby dane dotyczące tej osoby podlegają zniszczeniu.
2. Dane osobowe pracowników lub współpracowników przetwarzane są wyłącznie w celach związanych z zatrudnieniem osób, których dane dotyczą.
3. Świadczeniodawca nie wykorzystuje danych osobowych do celów innych, aniżeli określone w ust. 1 – 2.

§4

1. Świadczeniodawca pozyskuje dane osobowe od osób, których dane dotyczą.
2. Świadczeniodawca może pozyskiwać dane osobowe kandydatów do pracy od podmiotów zajmujących się profesjonalnie pośrednictwem pracy, o ile przedsiębiorcy ci przetwarzają dane osobowe w sposób zgodny z powszechnie obowiązującymi przepisami prawa.

§5

Świadczeniodawca umożliwia osobom, których dane dotyczą wgląd do danych osobowych oraz stwarza możliwość ich poprawy oraz uzupełnienia.

§6

Dane osobowe pracowników Świadczeniodawcy przetwarzane są samodzielnie przez Świadczeniodawcę:

a) w systemie informatycznym wspomagającym pracę kadr,
b) w zbiorze prowadzonym w sposób tradycyjny – w aktach osobowych pracowników.

Dział E

Dane osobowe przetwarzane przez Świadczeniodawcę w ramach zbioru kontrahentów.

§1

Świadczeniodawca przetwarza dane swoich kontrahentów.

§2

1. Dane przetwarzane są w celu wystawienia faktury, rachunku, prowadzenia sprawozdawczości finansowej. Dane zawierają wyłącznie informacje konieczne dla wykonania czynności, o których mowa w zdaniu poprzednim. Dane te nie zawierają informacji o stanie zdrowia pacjentów, ani nie stanowią żadnych innych danych o charakterze wrażliwym w rozumieniu treści art. 27 ustawy o ochronie danych osobowych.
2. Dane są przetwarzane w postaci tradycyjnej, jak i elektronicznej.