Wprowadzona decyzją Nr 01 /2018 z dnia 25 maja 2018 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Centrum Stomatologii „MATHIAS-DENT” Grażyna Mathias

§ 1.

Celem Polityki bezpieczeństwa danych osobowych w podmiocie leczniczym jest określenie zasad przetwarzania, ochrony i udostępniania danych osobowych, gromadzonych i przetwarzanych w podmiocie leczniczym pod firmą: Centrum Stomatologii „MATHIAS-DENT" Grażyna Mathias , zwanym dalej również *„PL"*, oraz nadzoru nad procesem przetwarzania tych danych.

§ 2.

Polityka bezpieczeństwa danych osobowych w podmiocie leczniczym obowiązuje wszystkie osoby realizujące jakiekolwiek zadania w PL lub na zlecenie PL, niezależnie od podstawy wykonywania tych zadań.

§ 3.

Polityka niniejsza opracowana została w oparciu o przepisy:

1) 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), dalej zwane również *„RODO"*,
2) ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta, a w szczególności przepisy jej rozdziału 7,
3) ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
4) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
5) rozporządzenia Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania.

§ 4.

Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, stanowi załącznik nr 1 do niniejszej Polityki.

§ 5.

1. Użyte w niniejszej Polityce określenia oznaczają:
   1) **Polityka bezpieczeństwa** lub **Polityka** – niniejszy dokument opisujący stosowane w PL zasady ochrony danych osobowych,
   2) **Administrator danych** – PL,
   3) **IOD** – inspektor ochrony danych w rozumieniu art. 37 – 39 RODO,
   4) **Ustawa** – ustawa z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
   5) **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

§ 6.

I. Zadania Administratora danych.

1. Administrator danych zobowiązany 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 udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu");
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
   4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
   5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania");
   6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").
3. Administrator danych wyznacza IOD.
4. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez Administratora danych. Osoby te są zobowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczania.
5. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.

II. Zadania IOD

1. IOD powołany przez PL odpowiada za bezpieczeństwo systemu informatycznego, w którym przetwarzane są dane osobowe.
2. Do obowiązków IOD należy:
   1) Wykonywanie zadań określonych w RODO, a w szczególności w przepisach art. 39 ust. 1 RODO,
   2) nadzór nad przestrzeganiem Polityki bezpieczeństwa i Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
   3) nadzór i kontrola systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych,
   4) nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe,
   5) nadzór nad wykorzystanym w placówce oprogramowaniem oraz jego legalnością,
   6) przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane

są dane osobowe,
7) podejmowanie odpowiednich działań w celu właściwego zabezpieczania danych,
8) badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych,
9) podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystanego do przetwarzania danych osobowych,
10) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, zawierających dane osobowe,
11) definiowanie haseł dostępu,
12) aktualizowanie oprogramowania antywirusowego i innego, chyba, że aktualizacje te wykonywane są automatycznie,
13) wykonywanie kopii zapasowych, ich przechowywanie oraz okresowe sprawdzanie pod kątem ich dalszej przydatności,
14) wdrożenie wewnętrznych szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych,
15) sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
16) zapewnienie ochrony i bezpieczeństwa danych osobowych znajdujących się w systemie informatycznym PL oraz w tradycyjnych zbiorach danych, ze szczególnym uwzględnieniem dokumentacji medycznej,
17) niezwłoczne informowanie Administratora danych lub osoby przez niego upoważnionej o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych,
18) podejmowanie, zgodnie z Polityką, stosownych działań w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym oraz danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
19) zapewnienie fizycznego bezpieczeństwa systemu informatycznego oraz systemu przechowywania i zabezpieczenia danych osobowych zgromadzonych i utrwalonych w innej formie, niż elektroniczna,
20) zapewnienie bezpieczeństwa funkcjonowania wszystkich urządzeń pracujących w systemie,
21) zapewnienie dostępu do systemu wyłącznie dla osób uprawnionych.

3. IOD prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która zawiera:
   a) imię i nazwisko osoby upoważnionej,
   b) datę nadania i ustania upoważnienia,
   c) podpis osoby upoważnionej, potwierdzający zapoznanie się ze wszystkimi dokumentami regulującymi bezpieczeństwo przetwarzania danych osobowych w PL.

III. Zadania pracowników i współpracowników PL

1. Wszyscy pracownicy i współpracownicy PL (dalej łącznie zwani *„pracownikami"*) mają obowiązek przestrzegać postanowień zawartych w niniejszej Polityce bezpieczeństwa i Instrukcji zarządzania systemem informatycznym.
2. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych, każdy pracownik zobowiązany jest do zapoznania się z przepisami dotyczącymi ochrony danych osobowych,

w tym z niniejszą Polityką. Fakt zapoznania się zostaje potwierdzony osobiście podpisanym oświadczeniem. Oświadczenie podlega włączeniu do akt pracownika lub dokumentów związanych z inna podstawą świadczenia usług w PL.

3. Pracownicy zobowiązani są dbać o bezpieczeństwo powierzonych im do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w placówce Polityką bezpieczeństwa, w tym między innymi:
   1) chronić dane przed dostępem osób nieupoważnionych,
   2) chronić dane przed przypadkowym zniszczeniem, utratą lub modyfikacją,
   3) chronić wszelkie nośniki zawierające dane osobowe, w szczególności nośniki magnetyczne, optyczne, nośniki pamięci półprzewodnikowej oraz wszelkiego rodzaju druki i wydruki, przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
   4) utrzymywać w tajemnicy hasła, częstotliwość ich zmiany oraz szczegóły technologiczne, także po ustaniu zatrudnienia w PL.
4. Zabrania się pracownikom:
   1) ujawniać dane, w tym dane osobowe zawarte w obsługiwanych systemach,
   2) kopiować bazy danych lub ich części bez wyraźnego upoważnienia,
   3) przetwarzać dane w sposób inny, niż wynikający z obowiązujących przepisów prawa.
5. Pracownicy zobowiązani są do udzielania pomocy IOD oraz do realizowania jego zaleceń przy wykonywaniu zadań dotyczących ochrony danych osobowych.
6. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące nienależyte wykonanie zobowiązania, w szczególności przez osobę, która wobec naruszenia nie powiadomiła o tym IOD.

§ 7.

1. Polityka niniejsza dotyczy przetwarzania wszystkich danych osobowych, przetwarzanych przez PL we wszelkiego rodzaju kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych, a także w systemach informatycznych będących w dyspozycji PL.
2. Wykaz pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (obszar przetwarzania danych osobowych), stanowi załącznik nr 2 do Polityki.
3. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów komputerowych zastosowanych do przetwarzania danych, stanowi załącznik nr 3 do Polityki.

§ 8.

1. Niezależnie od praw i obowiązków, określonych w niniejszej Polityce, przetwarzanie danych osobowych zawartych w dokumentacji medycznej prowadzonej w PL odbywa się w zakresie i zasadach określonych w:
   1) przepisach ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,
   2) przepisach rozporządzeń Ministra Zdrowia w sprawie rodzajów i zakresu dokumentacji medycznej, sposobu jej przetwarzania oraz wzorów określonych rodzajów dokumentacji medycznej, w szczególności wzoru książeczki zdrowia dziecka, wydanych na podstawie art. 30 ust. 1 ustawy wskazanej w pkt 1,
   3) innych przepisach szczególnych, w tym dotyczących:
      a) świadczeń opieki zdrowotnej finansowanych ze środków publicznych,

   b) zapobiegania oraz zwalczania zakażeń i chorób zakaźnych u ludzi,
   c) chorób zawodowych,
   d) medycyny pracy,
   e) ubezpieczeń społecznych oraz świadczeń pieniężnych z ubezpieczenia społecznego w razie choroby i macierzyństwa.
2. Przepisy, o których mowa w ust. 1, wskazują w szczególności:
   1) Podstawę przetwarzania danych osobowych,
   2) Zakres gromadzonych i przetwarzanych danych osobowych,
   3) Formę przetwarzania danych osobowych,
   4) Podstawę i zakres udostępniania danych osobowych posiadanych przez PL oraz podmiot uprawniony do dostępu do tych danych osobowych,
   5) Okres przetwarzania (przechowywania) tych danych osobowych.

§ 9.

1. Dane osobowe przetwarzane w systemach informatycznych przechowywane są na serwerach zlokalizowanych w Centrum Stomatologii „MATHIAS-DENT" Grażyna Mathias w budynku przy ul. Rejtana 8b w Wieliczce.
2. W odniesieniu do danych osobowych pracowników i współpracowników PL ich przetwarzanie może być prowadzone – na podstawie odrębnej umowy o powierzenie przetwarzania danych osobowych – z wykorzystaniem specjalistycznego oprogramowania będącego w dyspozycji wyspecjalizowanej firmy, która na zlecenie PL prowadzi obsługę rachunkowo-księgową PL.

§ 10.

1. Zdarzenia naruszające bezpieczeństwo danych osobowych lub grożące takim naruszeniem dzielą się na:
   1) zagrożenia losowe zewnętrzne (np. pożar, powódź, brak zasilania itp.), które mogą prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu oraz zakłócenia ciągłości jego pracy,
   2) zagrożenia losowe wewnętrzne (np. pomyłki pracowników, IOD, awarie sprzętowe, błędy oprogramowania itp.), które mogą prowadzić do zniszczenia danych, zakłócić ciągłość pracy systemu, powodować naruszenie poufności danych, integralności danych oraz ich prawidłowości,
   3) zagrożenia zamierzone, świadome i celowe, które polegać mogą na nieuprawnionym dostępie do systemu z jego wnętrza, nieuprawnionym przekazie danych, pogorszeniu jakości sprzętu i oprogramowania, bezpośrednim zagrożeniu materialnych składników systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia ochrony danych osobowych, w tym zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, to w szczególności:
   1) sytuacje losowe, nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu (np. pożar, zalanie pomieszczeń, katastrofa budowlana, itp.),
   2) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji, w tym danych osobowych (np. prace na danych osobowych w celach prywatnych, nie zamknięcie pomieszczenia, w którym znajduje się komputer lub urządzenie albo element wyposażenia do przechowywania danych osobowych, w szczególności dokumentacji medycznej, itp.),

3) niewłaściwe parametry środowiska, w którym pracuje sprzęt komputerowy (np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych itp.),
4) awaria sprzętu lub oprogramowania albo urządzenia lub elementu wyposażenia do przechowywania danych osobowych, w szczególności dokumentacji medycznej, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia zabezpieczeń lub ochrony danych, a także niewłaściwe działanie serwisu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) próba modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia,
8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych lub procedury przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń,
10) odstępstwa od założonego rytmu pracy wskazujące na złamanie lub zaniechanie ochrony danych osobowych, w tym praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywych nieautoryzowanych próbach logowania, itp.,
11) istnienie nieautoryzowanych kont dostępu do danych.

3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc i urządzeń służących do przechowywania danych osobowych na papierowych nośnikach, wydrukach, lub innych elektronicznych nośnikach zewnętrznych tych danych.

§ 11.

1. Podstawowym sposobem zabezpieczenia danych przetwarzanych w systemie informatycznym i dostępu do nich jest system definiowania loginów i haseł osób upoważnionych do przetwarzania danych osobowych. Są to zabezpieczenia programowe (logiczne) wmontowane w eksploatowane systemy uniemożliwiające dostęp do systemu osobom nieupoważnionym.
2. Podstawowym sposobem zabezpieczenia danych przetwarzanych w formie tradycyjnej, tj. na papierowych nośnikach danych, w tym dokumentacji medycznej, jest ograniczenie dostępu do niej za pomocą elementów zabezpieczeń fizycznych (ograniczenie dostępu do pomieszczeń i szaf lub innego wyposażenia biurowego, w których przechowywane są te dokumenty) oraz organizacyjnych (nadawanie, weryfikowanie i kontrolowanie dostępu do tych danych przez upoważnionych pracowników).
3. Zalogowanie się do systemu informatycznego wymaga podania loginu i hasła. Każdy pracownik samodzielnie ustala i zmienia hasło systemowe.
4. IOD ma dostęp do wszystkich loginów i haseł stosowanych przez wszystkich pracowników.
5. Hasła systemowe powinny być zmieniane nie rzadziej, niż co 90 dni.
6. Na każdym komputerze pracującym w systemie, który posiada dostęp do Internetu, jest zainstalowany odpowiedni program antywirusowy.
7. Wydruki zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.

§ 12.

1. Przed rozpoczęciem pracy użytkownik ma obowiązek sprawdzić, czy stan urządzenia (komputer lub pomieszczenia i urządzenia do przechowywania danych na papierowych nośnikach) nie wskazuje na naruszenie lub próbę naruszenia danych osobowych.
2. Użytkownicy mogą zakończyć pracę po wylogowaniu się z systemu. Osoby te są obowiązane do wylogowania się z sytemu także w przypadku czasowego opuszczenia stanowiska pracy.
3. W przypadku wykrycia korzystania z danych osobowych przez osoby nieuprawnione lub naruszenia zabezpieczeń dostępu do systemu, każdy kto stwierdził powyższe naruszenie, winien o tym powiadomić niezwłocznie IOD.

§ 13.

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
2. Za wykonywanie kopii zapasowych, umożliwiających odtworzenie sprawności systemu, odpowiada IOD. Są one przechowywane na serwerze oraz na nośnikach zewnętrznych. Nośniki zewnętrzne PL przechowuje poza obszarem przetwarzania danych, o którym mowa w załączniku nr 2.
3. Z nośników magnetycznych kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności w taki sposób, aby nie można było odtworzyć ich zawartości.

§ 14.

1. W ramach monitoringu systemu należy przeprowadzić przede wszystkim następujące działania:
   1) okresowe sprawdzanie kopii zapasowych pod względem przydatności do odtworzenia danych,
   2) kontrola ewidencji nośników magnetycznych i optycznych,
   3) sprawdzanie częstotliwości zmian haseł.
2. IOD przeprowadza kontrole oraz dokonuje ocen stanu bezpieczeństwa danych osobowych.
3. Ponadto IOD dokonuje analizy zagrożeń dla danych osobowych zgromadzonych przez PL. Wnioski z analizy zawiera raport sporządzony przez IOD.

§ 15.

1. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
   2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
   3) naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, albo naprawia się je pod nadzorem osoby upoważnionej przez Administratora danych lub w inny sposób gwarantujący zachowanie poufności tych danych.
2. Wydruki zawierające dane osobowe po ich wykorzystaniu są niszczone w sposób uniemożliwiający odczytanie znajdujących się na nich danych.

§ 16.

1. Każda osoba wykonująca jakiekolwiek zadania w PL, która stwierdzi lub podejrzewa naruszenie zabezpieczenia ochrony danych osobowych, zobowiązana jest niezwłocznie informować o tym IOD i Administratora danych.
2. Obowiązek, o którym mowa w ust. 1, dotyczy także sytuacji, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci (w odniesieniu do elektronicznych zbiorów danych) mogą wskazywać na naruszenie zabezpieczeń tych danych.
3. Osoba wykonująca jakiekolwiek zadania przy przetwarzaniu danych osobowych, która uzyskała informację lub sama stwierdziła naruszenie zabezpieczenia bazy danych osobowych w systemie informatycznym lub naruszenie zabezpieczenia zbioru danych przetwarzanych na papierowych nośnikach, zobowiązana jest niezwłocznie powiadomić o tym IOD, a przypadku jego nieobecności, Administratora danych.
4. IOD w pierwszej kolejności powinien:
   1) ustalić wszelkie okoliczności związane z tym zdarzeniem, w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
   2) niezwłocznie wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem, przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, a zwłaszcza do określenia skali naruszeń i metody dostępu do danych osobowych nieuprawnionej osoby.
5. Po wykonaniu ww. czynności, należy niezwłocznie podjąć dalsze odpowiednie kroki w celu powstrzymania lub ograniczania dostępu do danych osoby nieuprawnionej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji, w szczególności przez:
   1) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie nieuprawnionej, w szczególności poprzez dostęp z zewnątrz,
   2) przejściowe ograniczenie dostępu dla niektórych osób do danych osobowych przetwarzanych na papierowych nośnikach, w tym do dokumentacji medycznej, oraz dokonanie weryfikacji uprawnień do przetwarzania takich danych osobowych, jak również sprawdzenia i weryfikacji ustalonych zasad obiegu dokumentów, zawierających dane osobowe,
   3) zmianę hasła do konto, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania.
6. Po wyeliminowaniu bezpośredniego zagrożenia IOD powinien przeprowadzić wstępną analizę stanu systemu informatycznego, w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych.
7. W tym celu IOD powinien sprawdzić w szczególności:
   1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
   2) zawartość zbioru danych osobowych,
   3) sposób działania programu,
   4) jakość komunikacji w sieci,
   5) możliwość obecności wirusów komputerowych.
8. Po dokonaniu czynności, o których mowa powyżej, IOD powinien przeprowadzić szczegółową analizę stanu systemu informatycznego obejmującego identyfikację:

1) rodzaju zaistniałego zdarzenia,
2) metody dostępu do danych osoby nieuprawnionej,
3) skali zniszczeń.

9. Po przywróceniu normalnego stanu działania systemu przetwarzania danych osobowych, jeżeli nastąpiło uszkodzenie bazy danych lub zbioru tradycyjnego, niezbędne jest odtworzenie jej z dostępnych źródeł, w tym z ostatniej kopii zapasowej, z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego dostępu tą samą drogą przez osobę nieuprawnioną.
10. Po przywróceniu właściwego stanu bazy danych osobowych, należy przeprowadzić szczegółową analizę przyczyny naruszenia ochrony danych osobowych oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości. Jeśli przyczyną był:
    1) błąd osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych w systemie informatycznym, należy przeprowadzić szkolenie osób biorących udział przy przetwarzaniu danych,
    2) uaktywnienie wirusa, należy ustalić źródło jego pochodzenia oraz zainstalować zabezpieczenia antywirusowe lub sprawdzić stan istniejących zabezpieczeń,
    3) zaniedbanie ze strony osoby wykonującej jakiekolwiek zadania przy przetwarzaniu danych osobowych, należy wyciągnąć odpowiednie konsekwencje,
    4) włamanie w celu uzyskania bazy danych osobowych, należy dokonać szczegółowej analizy wdrożonych środków zabezpieczających w celu zapewnienia skutecznej ochrony danych osobowych,
    5) zły stan urządzenia, w tym urządzenia do przechowywania danych utrwalonych na papierowych nośnikach, lub sposób działania programu, należy niezwłocznie przeprowadzić kontrolne czynności serwisowe.
11. IOD zobowiązany jest przygotować szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia
12. Raport ten IOD niezwłocznie przekazuje Administratorowi danych, a w przypadku jego nieobecności osobie uprawnionej przez Administratora danych.

§ 17.

1. Rejestr czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO, stanowi załącznik nr 4 do Polityki.
2. Rejestr, o którym mowa w ust. 1, ma formę pisemną.
3.

§ 18.

1. Rejestr wszystkich kategorii czynności przetwarzania dokonywanych przez pracowników w imieniu Administratora danych, o którym mowa w art. 30 ust. 2 RODO, stanowi załącznik nr 5 do Polityki.
2. Rejestr, o którym mowa w ust. 1, ma formę pisemną .
3.

§ 19.

Rejestr przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych, o którym mowa w art. 33 ust. 5 RODO, stanowi załącznik nr 6 do Polityki.

§ 20.

Rejestr przypadków udostępnienia danych zawartych w dokumentacji medycznej, o którym mowa w art. 27 ust. 4 ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw

Pacjenta, stanowi załącznik nr 7 do Polityki.

§ 21.

Ustala się następujące wzory dokumentów:
Załącznik nr 8 - Upoważnienie do przetwarzania zbiorów danych osobowych.
Załącznik nr 9 - Odwołanie upoważnienia do przetwarzania zbiorów danych osobowych.
Załącznik nr 10 - Rejestr osób uprawnionych do przetwarzania danych osobowych.
Załącznik nr 11 – Oświadczenie o zachowaniu poufności i zapoznaniu się z przepisami .

Wieliczka, 25 maja 2018 r.