ZARZĄDZENIE NR 79/2016

Dyrektora Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie
z dnia 24 listopada 2016 r.

w sprawie wprowadzenia „Polityki bezpieczeństwa Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie”.

Na podstawie § 6 Statutu Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie, zarządza się, co następuje:

§ 1

1. Wprowadza się do stosowania w Centrum Onkologii – Instytucie im Marii Skłodowskiej-Curie w Warszawie „Politykę Bezpieczeństwa Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie” stanowiący załącznik do niniejszego zarządzenia.
2. Nadzór nad wykonaniem niniejszego zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 2

Traci moc zarządzenie Nr 44/2015 Dyrektora Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie z dnia 17 września 2015 r. w sprawie wprowadzenia „Polityki bezpieczeństwa Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie.

§ 3

Zarządzenie wchodzi w życie z dniem wydania.

D Y R E K T O R
Centrum Onkologii – Instytutu
im. Marii Skłodowskiej-Curie

Prof. dr hab. n. med. Jan Walewski

C E N T R U M O N K O L O G II - I N S T Y T U T
im. Marii Skłodowskiej - Curie w Warszawie

POLITYKA BEZPIECZEŃSTWA

Centrum Onkologii - Instytutu

im. Marii Skłodowskiej-Curie w Warszawie

WARSZAWA 2016 r.

Spis treści

1. WSTĘP

§ 1

W Centrum Onkologii – Instytucie im. Marii Skłodowskiej, zwanego dalej „Instytutem", funkcjonuje mieszany system podziału odpowiedzialności za obsługę elektronicznych danych medycznych (EDM). Funkcje Administratora Systemu/Administratora Lokalnego, podzielono pomiędzy pracowników Instytutu i podmioty zewnętrzne, świadczące usługi informatycznego wsparcia. W ramach zawartych umów na informatyczne wsparcie funkcjonujących w Instytucie systemów (outsourcing), w tym także na wsparcie systemu o strukturze terytorialnie rozproszonej (np. Krajowy Rejestr Nowotworów), wyznaczeni pracownicy Instytutu mają administracyjny dostęp do serwerów poszczególnych systemów, zarządzają kontami i uprawnieniami użytkowników systemu a także umożliwiają zdalny dostęp do serwera uprawnionemu podmiotowi na jego żądanie. Do obowiązków uprawnionych podmiotów należy instalacja, konfiguracja, aktualizacja oprogramowania, dbałość o bezpieczeństwo systemu, nadzorowanie, wykrywanie, eliminowanie nieprawidłowości i zagrożeń.

2. DEFINICJE

§ 2

1. **Administrator Danych Osobowych** (ADO) – organ, jednostka organizacyjna, pomiot lub osoba, decydująca o celach i środkach przetwarzania danych osobowych. Administrator Danych Osobowych jest powoływany na podstawie ustawy o ochronie danych osobowych, jest odpowiedzialny za przetwarzanie danych osobowych w systemie, wykonuje on czynności przewidziane w ww. ustawie. Administrator Danych Osobowych może powierzyć przetwarzanie danych innemu podmiotowi w drodze umowy zawartej na piśmie. Zgodnie z przepisem art. 7 pkt. 4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t. j. Dz. U. z 2016 r., poz. 922) w zw. z art. 23 i 24 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2016 r., poz. 371 ze zm.), Administratorem Danych Osobowych jest Dyrektor Instytutu.
2. **Administrator Bezpieczeństwa Informacji** (ABI) – osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za nadzór nad przestrzeganiem ustanowionych zasad ochrony danych osobowych. Administrator Bezpieczeństwa Informacji powoływany jest na podstawie ustawy o ochronie danych osobowych. Rolę Administratora Bezpieczeństwa Informacji może pełnić jedna osoba. W Instytucie jest to osoba wyznaczona przez Dyrektora Instytutu, działającą w jego imieniu, odpowiedzialna za nadzór nad bezpieczeństwem przetwarzanych danych osobowych.
3. **Administrator Systemów Informatycznych** (ASI) – osoba lub zespół odpowiedzialny za administrację systemem elektronicznych danych medycznych (EDM). W Instytucie jest nim Kierownik Działu Informatyki. Odpowiada on za nadzór nad prawidłowym przetwarzaniem elektronicznych danych medycznych, poprzez koordynację działań

pracowników Działu Informatyki, wyznaczonych pracowników komórek organizacyjnych, którym powierzono zadania Administratora Systemu/Administratora Lokalnego oraz podmiotów zewnętrznych świadczących usługi informatycznego wsparcia systemu (outsourcing). Zadaniem Administratora Systemów Informatycznych jest nadzór nad bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych Instytutu oraz przeciwdziałanie naruszeniom bezpieczeństwa tych danych.

4. **Administrator Systemu/Administrator Lokalny** - osoba lub zespół odpowiedzialny za administrowanie/zarządzanie sprzętem (komputery robocze, urządzenia mobilne) i zainstalowanym oprogramowaniem (system operacyjny, oprogramowanie antywirusowe) będącym w gestii Instytutu (wyznaczeni pracownicy Instytutu).
5. **Audytor Bezpieczeństwa** – osoba posiadająca kompetencje (wykazane cechy osobowości oraz wykazaną zdolność stosowania wiedzy i umiejętności) do przeprowadzenia audytu, czyli systematycznego, niezależnego i udokumentowanego procesu uzyskiwania dowodu z audytu (zapisów, stwierdzeń faktów, informacji, które są istotne z uwagi na kryteria audytu i możliwe do zweryfikowania) oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów audytu, czyli polityk, procedur, wymagań. Audytorem może być osoba będąca pracownikiem usługodawcy, niezależna od struktur odpowiedzialnych za bezpieczeństwo w organizacji lub instytucji zewnętrznej.
6. **Bezpieczeństwo systemu informatycznego** – rozumiane jest jako zapewnienie poufności, integralności i dostępności informacji na odpowiednim poziomie. Miarą bezpieczeństwa jest prawidłowe szacowanie ryzyka związanego z przetwarzaniem danych osobowych stanowiącym przedmiot Polityki Bezpieczeństwa Instytutu.
7. **Dalsze powierzanie danych** – przekazanie podwykonawcom przez podmioty zewnętrzne związane z Instytutem umową, danych osobowych powierzonych podwykonawcom przez Instytut.
8. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
9. **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi systemu.
10. **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
11. **Integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

12. **Kierownik placówki medycznej** – kierownik podmiotu leczniczego, w którym są przetwarzane dane medyczne i który odpowiada za zorganizowanie i zapewnienie odpowiednich środków ochrony danych.
13. **Lokalny Administrator Bezpieczeństwa Informacji** – (dotyczy Oddziału w Krakowie oraz Oddziału w Gliwicach) – osoba, wyznaczona przez Lokalnego Administratora Danych, działającą w jego imieniu, odpowiedzialna za nadzór nad bezpieczeństwem danych osobowych przetwarzanych w Oddziale, w tym w szczególności za przeciwdziałanie dostępowi do nich osób nieupoważnionych, oraz za podejmowanie odpowiednich działań w przypadku uzyskania informacji o wykryciu naruszeń w systemie zabezpieczeń.
14. **Lokalny Administrator Danych** – (Kierownik Oddziału w Krakowie oraz Kierownik Oddziału w Gliwicach) – osoba odpowiedzialna za przetwarzanie danych osobowych zgodnie z prawem i zapewniająca ich bezpieczeństwo.
15. **Powierzanie danych** – przekazanie podmiotom zewnętrznym danych osobowych na podstawie zawartej umowy.
16. **Przetwarzanie danych** – wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, w zwłaszcza te które wykonuje się w systemach informatycznych.
17. **Odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem:
    1) osoby, której dane dotyczą, bądź jej przedstawiciela;
    2) osoby upoważnionej do przetwarzania danych;
    3) organów administracji rządowej lub samorządu terytorialnego, lub sądom, którym dane są udostępniane w związku z prowadzonym postępowaniem.
18. **Osoba upoważniona do przetwarzania danych osobowych** – to osoba zatrudniona na umowie o pracę lub osoba związana umową cywilno-prawną z Instytutem, zaznajomiona z Polityką Bezpieczeństwa Instytutu oraz Instrukcją Ogólną Zarządzania Systemem Informatycznym Instytutu, a także posiadająca upoważnienie imienne do przetwarzania danych osobowych.
19. W systemach o strukturze terytorialnie rozproszonej (np. KRN, SZOI, EWUŚ, ApKolce) osobą upoważnioną jest :
    1) osoba zapoznana z Polityką Bezpieczeństwa Instytutu oraz z Instrukcją Ogólną Zarządzania Systemem Informatycznym Instytutu, której przydzielono konto i określono zakres dostępu do systemu (np. KRN, SZOI, EWUŚ, ApKolce),
    2) osoba, która stosować się będzie do Polityki Bezpieczeństwa Instytutu oraz Instrukcji Zarządzania Systemem Informatycznym Instytutu u Kierownika placówki medycznej w której jest zatrudniona. Przydzielono jej konto i określono zakres dostępu do systemu (np. KRN),

3) osoba, która wykonuje praktykę lekarską we własnym zakresie i stosuje się do zasad określonych w Ustawie o ochronie danych osobowych. Przydzielono jej konto i określono zakres dostępu do systemu(np. KRN).

20. **Osoba trzecia** – każda osoba nieupoważniona i przez to nieuprawniona do dostępu do danych osobowych lub zbiorów tych danych, w tym także osoba posiadająca upoważnienie wydane przez Dyrektora Instytutu, lecz podejmująca czynności przekraczające zakres udzielonego jej upoważnienia;
21. **Podmiot zewnętrzny** – osoba, organizacja lub inna jednostka, która nie wchodzi w skład Instytutu.
22. **Poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom lub innym podmiotom.
23. **Raport** – przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.
24. **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
25. **Rozporządzenie** – rozporządzenie 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. Nr 100, poz. 1024);
26. **Serwisant** – podmiot zewnętrzny, w tym jego pracownik zajmujący się sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego.
27. **Sieć publiczna –** (np. Internet) – sieć publiczna w rozumieniu art. 2 pkt. 29) ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (j. t. Dz. U. z 2016 r., poz. 1489 ze zm.).
28. **Sieć telekomunikacyjna** – sieć telekomunikacyjna w rozumieniu art. 2 pkt. 35) ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (j. t. Dz. U. z 2016 r., poz. 1489 ze zm.).
29. **Stacja robocza** – każdy komputer przeznaczony do bezpośredniej pracy, w tym w szczególności w sieciach komputerowych. Każdy komputer, który jest do tej sieci podłączony a który nie służy wyłącznie do jej obsługi;
30. **System informatyczny** – sprzęt komputerowy, oprogramowanie, dane przetwarzane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym, pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;
31. **Szyfrowanie wiadomości** – proces służący zabezpieczeniu danych podczas przesyłania, chroniący wiadomości elektroniczne przed uzyskaniem do nich dostępu przez osoby trzecie, gdy są przesyłane między nadawcą a odbiorcą.
32. **Teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;

33. **Uprawniony podmiot zewnętrzny** – to osoba lub firma, świadcząca na rzecz Instytutu usługi informatycznego wsparcia systemu/bazy danych (outsourcing IT), na podstawie umowy o świadczenie tych usług oraz umowy o zachowaniu poufności.
34. **Ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2016 r., poz. 922).
35. **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (wpisanie loginu i hasła w wyniku którego uzyskuje dostęp do danego systemu).
36. **Użytkownik systemu**:
    1) osoba upoważniona przez Administratora danych (lub działającego w jego imieniu Administratora bezpieczeństwa informacji). To osoba, która otrzymała Upoważnienie do przetwarzania danych osobowych, utworzono jej konto, nadano jej login i przyznano hasło;
    2) w systemach o strukturze terytorialnie rozproszonej (np. KRN) – to osoba, której utworzono konto i określono zakres dostępu do systemu (np. KRN).
37. **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym (np. wykonane w Excel-u zestawienia tabelaryczne pracowników, pacjentów z ich danymi personalnymi itp. - które można dowolnie sortować i wyszukiwać), dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.

3. POSTANOWIENIA OGÓLNE

§ 3

Cel polityki bezpieczeństwa

Celem wdrożenia niniejszej dokumentacji jest zapewnienie należytej ochrony danych, ustanowienie zasad i reguł postępowania, zapewniających bezpieczeństwo przetwarzania elektronicznych danych medycznych i dokumentacji w formie papierowej, będących w zasobach Administratora Danych Osobowych - odpowiednio do zagrożeń i kategorii danych osobowych objętych ochroną.

Przez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich integralności, poufności, rozliczalności, rozumianych jako:

1) rozliczalność - rozumie się właściwość zapewniającą, że działania osoby/podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie/ podmiotowi;
2) integralność danych - rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) poufność danych - rozumie się właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom/podmiotom.

§ 4

Zakres stosowania

1. Niniejsza Polityka Bezpieczeństwa dotyczy:
   1) pracowników Instytutu;
   2) osób, przy pomocy których Administrator Danych Osobowych - Dyrektor Instytutu, wykonuje swoje czynności, a w szczególności:
      a) osób współpracujących z Instytutem na podstawie umowy cywilno-prawnej;
      b) pracowników lub osoby działające w imieniu podmiotu zewnętrznego świadczącego usługi na rzecz Instytutu, jeśli wiąże się to z przetwarzaniem danych osobowych;
      c) stażystów, na podstawie umowy z Urzędem Pracy lub innym podmiotem leczniczym;
      d) praktykantów, na podstawie umowy ze szkołą wyższą;
      e) wolontariuszy, na podstawie umowy o wolontariat;
      f) podmiotów zewnętrznych, którym powierzono przetwarzanie danych osobowych w ramach podpisanej umowy powierzenia;
      g) także uprawnionych podmiotów zewnętrznych, świadczących usługi informatycznego wsparcia systemów informatycznych Instytutu, z którymi podpisano umowy o zachowaniu poufności;
      h) użytkowników systemów o strukturze terytorialnie rozproszonej(np. KRN, SZOI, EWUŚ, ApKolce), jeśli otrzymali/otrzymają upoważnienia do przetwarzania danych osobowych od Administratora Danych Osobowych Dyrektora Instytutu.

4. ŚRODKI TECHNICZNE I ORGANIZACYJNE PODJĘTE W CELU ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§ 5

1. Administrator Danych Osobowych, zapewnia bezpieczeństwo danych osobowych na poziomie wysokim, poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów technicznych i procedur organizacyjnych.
2. Administrator Bezpieczeństwa Informacji wraz z wyznaczonymi użytkownikami przeprowadzają okresową analizę ryzyka dla systemu i na tej podstawie przedstawiają Administratorowi Danych Osobowych propozycje dotyczące zastosowania środków technicznych i organizacyjnych (środków ochrony), celem zapewnienia właściwej ochrony przetwarzanych danych.
3. Zastosowane środki ochrony (techniczne i organizacyjne) są adekwatne do stwierdzonego

poziomu ryzyka dla poszczególnych systemów, baz danych i kategorii danych.

4. Środki ochrony, zastosowane przez ABI dla zapewnienia poufności, integralności, rozliczalności i ciągłości przetwarzanych danych, obejmują:
   1) środki ochrony fizycznej (np. drzwi ochronne, firma ochroniarska, monitoring);
   2) środki techniczne (np. firewall, antywirus, podtrzymanie zasilania UPS) ;
   3) środki organizacyjne (powołanie ABI, utworzenie Instrukcji Ogólnej Zarządzania Systemem Informatycznym Instytutu oraz Instrukcji zarządzania dla poszczególnych systemów informatycznych).
5. Zastosowane środki ochrony fizycznej pomieszczeń:
   1) serwery kluczowych dla funkcjonowania Instytutu systemów zlokalizowane są na X piętrze budynku klinicznego;
   2) pomieszczenie serwerowni zabezpieczone jest pod względem fizycznym w następujący sposób. Wejście do Działu Informatyki - zabezpieczone jest kodem dostępu – drzwi do serwerowni zabezpieczone są kartą magnetyczną;
   3) w pomieszczeniu serwerowni oraz na zewnątrz zainstalowany jest monitoring wizyjny z całodobowym rejestrowaniem na urządzeniu znajdującym się w serwerowni. Pomieszczenie ma zapewnioną właściwą wilgotność oraz klimatyzację;
   4) pomieszczenie jest zaciemnione a okna zabezpieczone przed włamaniem;
   5) pomieszczenie posiada instalację ppoż., połączoną z Centralą Dyspozytornią, gdzie jest prowadzony całodobowy nadzór;
   6) w godzinach pracy pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone są przez stałą obecność pracowników, wejście do wyznaczonych stref zabezpieczone są za pomocą kodów dostępu lub poprzez drzwi zamykane na zamki patentowe. Po godzinach pracy, oprócz wyżej wymienionych zabezpieczeń, zapewniony jest ściślejszy nadzór firmy ochroniarskiej;
6. Zastosowane środki techniczne:
   1) architektura sieci posiada mechanizmy kompleksowej ochrony sieci przed włamaniem. Wielofunkcyjna zapora sieciowa wykorzystuje mechanizmy ochrony: IPS (Intrusion Prevention System), firewall, sieciowy filtr antywirusowy, filtr antyspamowy i filtrowanie treści;
   2) dostęp do zewnętrznego Data Center gwarantuje uwierzytelnianie oraz szyfrowanie przesyłanych danych poprzez wykorzystanie bezpiecznego połączenia VPN;
   3) uwierzytelnianie użytkowników przy dostępie zdalnym następuje z wykorzystaniem wirtualnych sieci prywatnych (VPN) lub za pomocą zdalnego pulpitu;
   4) część systemów posiada wydzielone serwery (np. poczta), jednakże serwery kluczowych systemów działa na zasadzie „farmy serwerów”, co zwiększa prawdopodobieństwo bezawaryjnej pracy;

5) „farma serwerów” aktualnie nie jest podłączona do zasilania awaryjnego z agregatu prądotwórczego na wypadek braku zasilania z sieci miejskiej, jednakże podjęte będą prace mające na celu wyeliminowanie tego zagrożenia;
6) „farma serwerów” ma UPS-y pozwalające na bezpieczne zamknięcie - w przypadku przerwy w zasilaniu z sieci miejskiej;
7) stacje robocze użytkowników w newralgicznych miejscach mają UPS-y;
8) na większości stanowisk użytkowników możliwy jest dostęp do sieci Internet. Użytkownicy bezwzględnie muszą przestrzegać zasady zachowania szczególnej ostrożności przy otwieraniu przesyłek od nieznanego nadawcy i otwieranie dołączonych załączników;

7. Rozwiązania organizacyjne przetwarzania danych osobowych:
   1) powołanie Administratora Bezpieczeństwa Informacji;
   2) określenie obowiązków Administratora Systemów Informatycznych – Kierownika Działu Informatyki, Administratorów Systemów/Administratorów Lokalnych, kierowników podmiotów/komórek organizacyjnych, określenie obowiązków osoby upoważnionej, uprawnionego podmiotu zewnętrznego;
   3) określenie procedury nadawania uprawnień do przetwarzania danych osobowych;
   4) określenie metod i środków uwierzytelniania;
   5) określenie zasad korzystania ze służbowej poczty elektronicznej i Internetu;
   6) określenie stref bezpieczeństwa;
   7) postępowanie na wypadek wystąpienia awarii i katastrof;
   8) zapewnienie ciągłości funkcjonowania;
   9) szkolenie pracowników i osób współpracujących z Instytutem na podstawie umów cywilno-prawnych oraz innych osób, którym powierzono przetwarzanie danych osobowych w ramach umowy powierzenia.

5. ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

§ 6

Administrator Danych Osobowych

1. Administrator Danych Osobowych, deklaruje pełne zaangażowanie i determinację celem zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a także prawidłowego zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych. Zapewnia bezpieczeństwo danych osobowych na poziomie wysokim**.**
2. Administrator Danych Osobowych dokłada należytej staranności w celu ochrony interesów osób, których dane osobowe dotyczą, w szczególności jest obowiązany zapewnić, aby dane były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych celów,

3) merytorycznie poprawne,
4) adekwatne do celów w jakich są zbierane,
5) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą.

3. Przetwarzanie danych osobowych odbywa się na zasadzie:
   1. zgody wyrażonej na piśmie podczas zawierania stosunku pracy,
   2. zgody wyrażonej na piśmie przez osoby składające swoje CV,
   3. zgody wyrażonej na piśmie przez osoby przyjmowane w charakterze pacjenta lub gdy okoliczności uniemożliwiają uzyskanie zgody na piśmie, dopuszczalne jest przetwarzanie danych osobowych na podstawie art. 25 ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzecznika Praw Pacjenta (j.t. Dz. U. z 2016 r., poz. 186 ze zm.) oraz rozporządzenia Ministra Zdrowia z 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobów jej przetwarzania (Dz. U. z 2015 r., poz. 2069 ze zm.).
4. Przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą oraz następuje, w celach badań naukowych, dydaktycznych, historycznych lub statystycznych, z zachowaniem przepisów Ustawy.
5. Przetwarzania danych ujawniających, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, jest dopuszczalne, jeżeli:
   1) osoba, której dane dotyczą, wyrazi na to zgodę na piśmie, chyba że chodzi o usunięcie dotyczących jej danych;
   2) przetwarzanie jest niezbędne do wykonania zadań Dyrektora Instytutu odnoszących się do zatrudnienia pracowników i innych osób, jeśli zakres przetwarzanych danych jest zgodny z Ustawą;
   3) przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych;
   4) jest to niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego. Publikowanie wyników badań naukowych nie może następować w sposób umożliwiający identyfikację osób, których dane zostały przetworzone;

5) przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.
   a) Administrator Danych Osobowych nadzoruje jakie dane, kiedy i przez kogo zostały wprowadzone do nadzorowanych przez niego zbiorów, bądź z tych zbiorów usunięte oraz komu są przekazywane.
   b) Administrator Danych Osobowych na bieżąco dostosowuje system informatyczny Instytutu, służący do przetwarzania danych osobowych oraz sposoby zabezpieczeń przetwarzania danych do wymogów określonych w rozporządzeniu.

6. Administrator Danych Osobowych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, techniczne zastosowane w celu ich ochrony.

6. PODMIOTY/ KOMÓRKI ORGANIZACYJNE I OSOBY REALIZUJĄCE ZADANIA ADMINISTRATORA DANYCH OSOBOWYCH

§ 7

Lokalny Administrator Danych

Zasady określone w § 4 - § 6 stosuje odpowiednio Dyrektor Oddziału w Krakowie oraz Dyrektor Oddziału w Gliwicach, który jest odpowiedzialny za przetwarzanie danych osobowych zgodnie z prawem.

§ 8

Lokalny administrator bezpieczeństwa informacji

1. Lokalny administrator bezpieczeństwa informacji Oddziału w Krakowie oraz Oddziału w Gliwicach, to osoba wyznaczona przez Lokalnego administratora danych osobowych.
2. Stosuje on odpowiednio zasady określone w § 10 i § 11. Lokalny administrator danych osobowych jest odpowiedzialny za bezpieczeństwo danych osobowych przetwarzanych w systemie informatycznym, oraz przetwarzanych manualnie.

§ 9

Ogólne zadania osób przy pomocy których Administrator Danych Osobowych realizuje swoje zadania

Administrator Danych Osobowych, poprzez podległych mu kierowników podmiotów/komórek organizacyjnych Instytutu, zapobiega zagrożeniom wynikającym z przetwarzania danych na terenie Instytutu, takich jak:

1) oddziaływanie czynników zewnętrznych: pożar, wyładowanie atmosferyczne, zalanie pomieszczeń, katastrofa budowlana;

2) zagrożenia środowiskowe zakłócające pracę urządzeń komputerowych: nadmierna wilgotność, ciśnienie, wysoka temperatura, promieniowanie słoneczne, pył, oddziaływanie pola elektromagnetycznego, spadek napięcia;
3) włamanie, kradzież, wyłudzenie, wymuszenie, napad, działania terrorystyczne;
4) umyślne naruszenia ochrony danych powodujące awarie sprzętu lub oprogramowania;
5) niezamierzone rozproszenie danych w Internecie lub celowe z ominięciem zabezpieczeń systemu z wykorzystaniem błędów systemu informatycznego;
6) atak z sieci Internetowej lub Intranetowej;
7) pozostawienie serwisantów bez nadzoru, przyzwolenie na naprawę sprzętu zawierającego dane osobowe poza siedzibą administratora danych osobowych;
8) podejmowanie pracy w systemie z pominięciem procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania danych, próby stosowania cudzego hasła i identyfikatora przez osoby nieupoważnione;
9) nieprzestrzeganie procedur oraz zasad przez osoby upoważnione do przetwarzania danych osobowych, w tym:
    a) opuszczenie stanowiska pracy bez zabezpieczenia stanowiska komputerowego;
    b) pozostawienie po zakończeniu pracy niezabezpieczonych dokumentów;
    c) pozostawienie pokoju bez właściwego nadzoru;
    d) nie zabezpieczenie klucza do pomieszczeń po zakończonej pracy;
    e) nieautoryzowane przetwarzanie danych;
    f) nieumyślne udostępnienie lub ujawnienie osobom nieupoważnionym danych bądź procedur ochrony danych, stosowanych u Administratora Danych Osobowych;
    g) niewykonywanie stosownych kopii zapasowych baz danych;
    h) przetwarzanie danych osobowych w celach naukowych bez wiedzy i zgody Administratora Danych Osobowych;
    i) wprowadzanie zmian do systemu informatycznego Administratora Danych Osobowych i instalowanie programów bez zgody administratora systemu.

§ 10

Administrator Bezpieczeństwa Informacji

1. Administrator Danych Osobowych może wyznaczyć i zgłosić do rejestru prowadzonego przez GIODO Administratora Bezpieczeństwa Informacji, który jest odpowiedzialny za przetwarzanie danych zgodnie z ustawą oraz rozporządzeniami.
2. Zgłoszenia, o którym mowa powyżej dokonuje się według wzoru określonego rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. 2014, poz. 1934).

3. Administratora Bezpieczeństwa Informacji może wyznaczyć co najmniej jednego zastępcę. Zastępca Administratora Bezpieczeństwa Informacji musi spełniać wszystkie warunki, jak dla powołania Administratora Bezpieczeństwa Informacji.
4. Zastępca Administratora Bezpieczeństwa Informacji wykonuje wszystkie obowiązki należące do zakresu obowiązków Administratora Bezpieczeństwa Informacji podczas jego nieobecności.
5. W celu sprawnej realizacji nałożonych zadań, Administratorowi Bezpieczeństwa Informacji przysługują uprawnienia określone w rozporządzeniu Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji(Dz. U. Z 2015, poz. 745).
6. Administrator Bezpieczeństwa Informacji podlega bezpośrednio kierownikowi jednostki organizacyjnej.
7. Administrator Danych Osobowych zapewnia środki i organizacyjną odrębność Administratora Bezpieczeństwa Informacji, niezbędne do niezależnego wykonywania przez niego zadań.

§ 11

Zadania Administratora Bezpieczeństwa Informacji

1. Nadzoruje opracowanie i aktualizację dokumentacji oraz przestrzeganie zasad w niej określonych.
2. Wydaje w imieniu Administratora Danych Osobowych, upoważnienia do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi obowiązków.
3. Zapewnia zapoznanie osób upoważnionych z przepisami o ochronie danych osobowych.
4. Prowadzi:
   1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, którego wzór określa **załącznik Nr 10** do niniejszej Polityki Bezpieczeństwa;
   2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, którego wzór określa **załącznik Nr 11** do niniejszej Polityki Bezpieczeństwa;
   3) opis struktury zbiorów danych wskazujący na zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi bazami danych, którego wzór określa **załącznik Nr 12** do niniejszej Polityki Bezpieczeństwa;
   4) ewidencję osób przetwarzających dane osobowe posiadających upoważnienia, którego wzór określa **załącznik Nr 13** do niniejszej Polityki Bezpieczeństwa
5. Przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe pracowników i pacjentów Instytutu.

6. Prowadzi nadzór nad fizycznym zabezpieczeniem pomieszczeń w których przetwarzane są dane osobowe.
7. Prowadzi nadzór nad obiegiem oraz przechowywaniem dokumentów i wydawnictw zawierających dane osobowe generowane przez system informatyczny.
8. Prowadzi nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrolą dostępu do tych danych.
9. Prowadzi analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych i przygotowanie oraz przedstawia Administratorowi Danych Osobowych propozycję odpowiednich zmian do instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

§ 12

Administrator systemów informatycznych(wszystkich eksploatowanych w Instytucie)

1. Administrator systemów informatycznych (Kierownik Działu Informatyki) - osoba odpowiedzialna za administrację systemem elektronicznych danych medycznych (EDM) w Instytucie.
2. Odpowiada za nadzór nad prawidłowym przetwarzaniem elektronicznych danych medycznych, poprzez koordynację działań pracowników Działu Informatyki, wyznaczonych pracowników komórek organizacyjnych, którym powierzono zadania Administratora Systemu/Administratora Lokalnego oraz podmiotów zewnętrznych świadczących usługi informatycznego wsparcia systemów oraz baz danych.
3. Sprawuje nadzór nad bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych Instytutu oraz przeciwdziałanie naruszeniom bezpieczeństwa tych danych.

§ 13

Administrator systemu/Administrator lokalny

1. Administrator systemu informatycznego realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym, który mu powierzono, a w szczególności:
   1) przeciwdziała dostępowi osób nieuprawnionych do systemu informatycznego, w którym przetwarzane są dane osobowe;
   2) odpowiada za podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych;
   4) informuje Administratora Bezpieczeństwa Informacji o naruszeniu bezpieczeństwa i współdziała z uprawnionym podmiotem zewnętrznym świadczącym usługi informatycznego wsparcia systemu, przy usuwaniu skutków naruszenia;

5) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym;
6) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe a także nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego;
7) podejmuje działania służące zapewnieniu ciągłości działania systemu pod kątem niezawodności zasilania kluczowych elementów systemu;
8) nadzoruje systemem komunikacji w sieci komputerowej oraz przesyłanie danych za pośrednictwem urządzeń do teletransmisji(jeśli dotyczy);

2. Administrator systemu/Administrator lokalny oprócz obowiązków wymienionych w ust. 1, zgodnie z zawartą umową pomiędzy Instytutem a uprawnionym podmiotem zewnętrznym, świadczącym usługi informatycznego wsparcia systemu realizuje następujące zadania:
   1) przydziela konta użytkownikom, nadaje loginy i hasła startowe do systemu;
   2) odblokowuje dostęp do konta użytkownikowi systemu (na jego wniosek), jeśli zablokowanie nastąpiło z powodu wpisania nieprawidłowego hasła (zapomniał hasła);
   3) umożliwia administracyjny dostęp do serwera systemu uprawnionemu podmiotowi zewnętrznemu na jego żądanie, jeśli tak przewidują warunki umowy ;
   4) do końca każdego roku kalendarzowego, sporządza uaktualniony **załącznik Nr 1** do niniejszej Polityki Bezpieczeństwa i przedstawia Administratorowi Bezpieczeństwa Informacji;
   5) do końca każdego roku kalendarzowego, przedstawia Administratorowi Bezpieczeństwa Informacji, roczny raport dotyczący naruszeń bezpieczeństwa danych osobowych.
3. Administrator systemu/Administrator lokalny zobowiązany jest do stworzenia Instrukcji Zarządzania Systemem Informatycznym (za który odpowiada) i jej aktualizacji. Punktem odniesienia jest Instrukcja Ogólna Zarządzania Systemami Informatycznymi Instytutu.
4. Instrukcja Zarządzania Systemem Informatycznym Instytutu Administratora systemu/ Administratora lokalnego, musi zawierać kluczowe dane o systemie odnoszące się do bezpieczeństwa danych osobowych (zapewnienie ciągłości funkcjonowania, w tym częstość i rodzaje tworzonych kopii, podział zadań i odpowiedzialności w administrowaniu systemem z podmiotem zewnętrznym, miejsce usytuowania serwera oraz jego zabezpieczenie fizyczne).

§ 14

Uprawniony podmiot zewnętrzny

1. Uprawniony podmiot zewnętrzny, to osoba lub firma, świadcząca na rzecz Instytutu usługi informatycznego wsparcia systemu (outsourcing IT), na podstawie umowy

o świadczenie tych usług oraz umowy o zachowaniu poufności, której wzór stanowi **załącznik Nr 14** do Polityki Bezpieczeństwa.

2. Zadaniem uprawnionego podmiotu zewnętrznego, stosownie do uzgodnionego podziału obowiązków z Kierownikiem Działu Informatyki i Administratorem lokalnym, jest zapewnienie bezpieczeństwa przetwarzanym danym osobowym oraz zapewnienie ciągłości funkcjonowania systemu informatycznego zgodnie z podpisaną umową.

§ 15

Kierownik podmiotu/ komórki organizacyjnej Instytutu

1. Kierownik podmiotu/komórki organizacyjnej odpowiada za przestrzeganie zasad bezpiecznego przetwarzania danych osobowych, przez podległych mu użytkowników systemu, baz danych i aplikacji, wykorzystywanych do realizacji obowiązków właściwych ze względu na realizowane zadania.
2. Realizując zadania określone w ust. 1, Kierownik podmiotu/komórki organizacyjnej:
   1) określa indywidualne obowiązki i zakres odpowiedzialności przy przetwarzaniu danych osobowych podległym pracownikom;
   2) wykonuje zalecenia Administratora bezpieczeństwa informacji w zakresie ochrony danych osobowych;
   3) wdraża i nadzoruje przestrzeganie przepisów związanych ochroną danych osobowych w podległym mu podmiocie/komórce organizacyjnej;
   4) przekazuje na właściwym formularzu, którego wzór określa **załącznik Nr 1** do niniejszej Polityki Bezpieczeństwa, aktualne dane niezbędne Administratorowi Bezpieczeństwa Informacji do aktualizacji dokumentacji (niezwłocznie w przypadku zmiany struktury organizacyjnej Instytutu, skutkującej zmianą nazwy podmiotu/komórki organizacyjnej, zmianą systemu/programu z którego korzysta);
   5) wnioskuje do Administratora Bezpieczeństwa Informacji na formularzu, którego wg wzór stanowi **załącznik nr 2** do niniejszej Polityki Bezpieczeństwa o nadanie/zmianę/wyrejestrowanie:
      a) upoważnienia do przetwarzania danych osobowych dla nowego pracownika,
      b) upoważnienia dla pracownika, który zmienił komórkę organizacyjną, gdy pociąga to za sobą zmianę systemu/obsługiwanej bazy danych, zakresu uprawnień;
      c) zablokowanie dostępu do systemu/bazy danych pracownikowi, który przebywa na długotrwałym zwolnieniu lekarskim (ponad 30 dni),
      d) wyrejestrowaniu pracownika i zablokowanie dostępu z którym została rozwiązana umowa o pracę lub inny rodzaj umowy.
3. Kierownik podmiotu/komórki organizacyjnej przekazuje Administratorowi Bezpieczeństwa Informacji, zamiar utworzenia nowego zbioru danych, bądź zamiar dokonania zmian w zarejestrowanych zbiorach danych. Forma i treść danych musi być zgodna z przepisami Ustawy o ochronie danych osobowych.

§ 16

Osoba upoważniona do przetwarzania danych osobowych

1. Osoba upoważniona do przetwarzania danych osobowych to:
   1) osoba zatrudniona na umowie o pracę lub osoba związana umową cywilno-prawną z Instytutem, zaznajomiona z Polityką Bezpieczeństwa, oraz Instrukcją Ogólną Zarządzania Systemem Informatycznym Instytutu. Osoba ta, która złożyła oświadczenie (lub jest zwolniona z tego obowiązku na podstawie przepisów prawa), oraz otrzymała Upoważnienie według wzoru stanowiących **załącznik Nr 3 i załącznik Nr 4** do niniejszej Polityki Bezpieczeństwa.
   2) osoby reprezentujące podmiot zewnętrzny - realizujący umowę wiążącą się z przetwarzaniem danych osobowych - składają oświadczenie, którego wzór określa **załącznik Nr 5** do niniejszej Polityki Bezpieczeństwa;
2. W systemach o strukturze terytorialnie rozproszonej (np. KRN, SZOI, EWUŚ, ApKolce) osoba upoważniona to:
   1) osoba zapoznana z Polityką Bezpieczeństwa Instytutu oraz z Instrukcją Ogólną Zarządzania Systemem Informatycznym Instytutu, która podpisała oświadczenie (Załącznik nr 3), otrzymała od Dyrektora Instytutu Upoważnienie (Załącznik nr 4), przydzielono jej konto i określono zakres dostępu do Systemu (pracownicy KRN i WRN, pracownicy Instytutu korzystający z SZOI, EWUŚ, ApKolce);
   2) osoba, która stosować się będzie do Polityki Bezpieczeństwa Instytutu oraz Instrukcji Zarządzania Systemem Informatycznym u Kierownika placówki, przydzielono jej konto i określono zakres dostępu do systemu/bazy danych (w KRN, to pracownicy pozostałych ośrodków wojewódzkich oraz sprawozdających do nich szpitali);
   3) osoba, która wykonuje praktykę lekarską we własnym zakresie i stosuje się do zasad określonych w Ustawie o ochronie danych osobowych, przydzielono jej konto i określono zakres dostępu do systemu/bazy danych.

§ 17

Obowiązki osoby upoważnionej

1. Przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie przez kierownika komórki organizacyjnej a określonych w upoważnieniu, którego wzór stanowi **załącznik Nr 4** do niniejszej Polityki Bezpieczeństwa i tylko w celu wykonywania nałożonych lub uzgodnionych obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika systemu, niezbędnego do rozpoczęcia pracy w systemie.
2. Zachowania w tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Zachowanie tajemnicy danych osobowych obowiązuje przez cały okres zatrudnienia w Instytucie, a także po ustaniu stosunku pracy lub innego stosunku prawnego łączącego użytkownika systemu z Instytutem.
3. Osoba upoważniona zobowiązana jest do korzystania z urządzeń systemu, w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemu, oprogramowania i nośników.

4. Osoba upoważniona zobowiązana jest zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym.
5. Rozwiązanie stosunku pracy lub innego stosunku prawnego łączącego użytkownika systemu z Instytutem, jak również odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych.

§ 18

Obowiązek informacyjny

1. Kierownicy podmiotów/komórek organizacyjnych, w których przetwarzane są dane osobowe pacjentów a w szczególności kierownik Działu Obsługi Pacjenta, w odniesieniu do pacjentów pierwszorazowych lub na pisemny wniosek pacjenta, zobowiązani są do udzielania następujących informacji:
   1) administratorem danych jest Dyrektor Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie ul. Wawelska 15B, 02-034 Warszawa,
   2) o celu zbierania danych,
   3) o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej(rozporządzenia ministra zdrowia z 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobów jej przetwarzania),
   4) o prawie dostępu do swoich danych osobowych oraz możliwości ich poprawiania.
2. Osobom, których dane są przetwarzane w zbiorach danych osobowych w Instytutu, przysługuje prawo kontroli ich danych osobowych, a w szczególności prawo do uzyskania informacji na temat tych danych w zakresie wskazanym w ustawie. Wzór wniosku o udzielenie informacji na temat danych osobowych przetwarzanych przez Instytut a dotyczących wnioskującej osoby, stanowi **załącznik Nr 8** do niniejszej Polityki Bezpieczeństwa. Wnioskodawca, który wystąpi z wnioskiem o udzielenie tych informacji, powinien otrzymać odpowiedź na piśmie w terminie wynikającym z Kodeksu postępowania administracyjnego, w formie przedstawionej we wzorze określonym w **załączniku Nr 9** do niniejszej Polityki Bezpieczeństwa.
3. O udostępnienie danych osobowych ze zbioru danych Instytutu, może zwrócić się uprawniony podmiot zewnętrzny. Wzór wniosku stanowi **załącznik Nr 7** do niniejszej Polityki Bezpieczeństwa.
4. W przypadku wykazania przez osobę, której dane osobowe są przetwarzane w Instytucie, że są one niekompletne, nieaktualne, nieprawdziwe, albo są zbędne do realizacji celu, dla którego zostały zebrane, ma ona prawo do ich uzupełnienia, uaktualnienia lub sprostowania, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.
5. Kandydaci zgłaszający się do pracy w Instytucie, w procesie rekrutacji, powinni udzielić pisemnej zgody na przetwarzanie ich danych osobowych zawartej w CV lub przy wykorzystaniu druku, którego wzór stanowi **załącznik Nr 6** do niniejszej Polityki

Bezpieczeństwa. Osobą odpowiedzialną za uzyskanie takiej zgody jest Kierownik Działu Spraw Pracowniczych i Spraw Socjalnych.

7. STRATEGIA SZACOWANIA I ZARZĄDZANIA RYZYKIEM

§ 19

Strefy bezpieczeństwa

1. W obszarze przetwarzania danych w Instytucie wydziela się strefy bezpieczeństwa o ograniczonym dostępie do elementów infrastruktury i przechowywanych danych osobowych.
2. W pomieszczeniach o znaczeniu krytycznym (serwerownie) mogą przebywać:
   1) Administrator Danych Osobowych,
   2) Administrator Bezpieczeństwa Informacji,
   3) Administratorzy systemów informatycznych/Administratorzy Lokalni,
   4) pracownicy uprawnionych podmiotów świadczących usługi informatycznego wsparcia systemów - tylko w towarzystwie Administratora systemu/ Administratora lokalnego. Osoby postronne w ogóle nie mają tam dostępu (klucze do tych pomieszczeń podlegają zabezpieczeniu);
3. W obszarach o podwyższonym poziomie bezpieczeństwa, do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych, zgodnie z zakresami upoważnień do ich przetwarzania. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie Administratora Danych Osobowych (rejestracje, gabinety lekarskie, punkty pielęgniarskie, archiwa danych medycznych, pomieszczenia obsługi kadrowej i finansowej). Osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych.

§ 20

Ocena oczekiwanego poziomu bezpieczeństwa

1. Grupy błędów w ochronie informacji, mające wpływ na funkcjonowanie bezpieczeństwa, kwalifikuje się według następującej skali:
   1) błąd o stopniu krytycznym – utrata danych lub uszkodzenie sprzętu spowodują załamanie w funkcjonowaniu oraz wywierają szerokie niekorzystne skutki społeczne; należą do nich:
      a) sabotaż skutkujący dezintegracją zespołu serwerów(serwerowni), uszkodzenie węzłów dystrybucyjnych transmisji danych,
      b) pożar lub zalanie serwerowni uniemożliwiające jej normalna funkcjonowanie,
      c) awaria zasilania powodująca wyłączenie z eksploatacji serwerowni i węzłów dystrybucyjnych transmisji danych,
      d) kradzież macierzy dyskowych z danymi osobowymi,
      e) włamanie hakerskie do systemu i skopiowanie zawartych danych lub ich zakodowanie,

2) błąd o stopniu wysokim – utrata danych lub uszkodzenie sprzętu spowodują znaczne trudności w normalnym funkcjonowaniu, brak skutków społecznych; należą do nich:
   a) nieumyślne udostępnienie lub ujawnienie osobom nieupoważnionym procedur ochrony danych, stosowanych u Administratora Danych Osobowych;
   b) włamanie hakerskie do jednego z systemów autonomicznych i dezintegracja jego funkcjonalności,
   c) błąd użytkownika lub umyślne naruszenia ochrony danych powodujące awarie sprzętu lub oprogramowania,
   d) włamanie hakerskie do jednego z systemów autonomicznych i zakodowanie zasobów połączone z żądaniem okupu,
3) błąd o stopniu przeciętnym – utrata danych lub uszkodzenie sprzętu wpłyną nieznacznie na funkcjonowanie; należą do nich:
   a) skopiowanie i wyniesienie grupy danych, przez pracownika mającego dostęp w ramach nadanych uprawnień,
   b) uszkodzenie kabla transmisyjnego(stacje robocze-serwer) w czasie prac remontowych.
4) błąd o stopniu niskim – utrata danych lub uszkodzenie sprzętu wyrządzają niewielkie szkody, należą do nich:
   a) dokonanie przez pracownika zrzutu ekranu z pojedynczymi danymi i wyniesienie ich poza pracę,
   b) nieautoryzowane przetwarzanie danych,
   c) opuszczenie stanowiska pracy bez zabezpieczenia stanowiska komputerowego
   d) nieostrożne obchodzenie się ze sprzętem skutkujące drobnymi awariami(zalanie klawiatury komputera, uszkodzenie myszki itp.).

2. W przypadku wystąpienia błędów określonych w ust. 1, użytkownicy systemu/bazy danych Instytutu mają obowiązek poinformować o zdarzeniu Administratora lokalnego, który stosownie do stopnia zagrożenia podejmuje działania naprawcze lub powiadamia uprawniony podmiot zewnętrzny w celu wspólnego rozwiązania problemu. O zaistniałym incydencie oraz sposobie jego rozwiązania Administrator lokalny powiadamia Administratora systemów informatycznych Instytutu oraz Administratora bezpieczeństwa informacji celem przygotowania raportu z zaistniałej sytuacji dla Dyrektora Instytutu.
3. Za naruszenia bezpieczeństwa danych osobowych uznaje się także:
   1) infekcję wirusem komputerowym – administrator systemu zobowiązany jest do ustalenia źródła jego pochodzenia oraz podjęcia prób neutralizacji, podejmuje działania wykluczające powtórzenie się podobnego zdarzenia;
   2) błąd użytkownika systemu informatycznego o którym mowa w § 9 – administrator systemu zapewnia ponowne szkolenie wszystkich użytkowników systemu z obsługi systemu;
4. Za zaniedbanie ze strony użytkownika systemu – wobec użytkownika systemu będącego pracownikiem Instytutu mogą zostać wyciągnięte konsekwencje wynikające z Kodeksu pracy oraz z ustawy o ochronie danych osobowych.

5. W przypadku wykrycia naruszenia bezpieczeństwa danych osobowych lub podejrzenia naruszenia zabezpieczenia danych osobowych administrator systemu zobowiązany jest do:
   1) Podjęcia wszelkich możliwych kroków w celu zabezpieczenia systemu przed dalszymi naruszeniami bezpieczeństwa, minimalizacją szkód i zabezpieczeniem przed usunięciem śladów naruszenia bezpieczeństwa danych osobowych, dopuszcza się następujące rozwiązania:
      a) fizyczne odłączenie urządzeń i segmentów sieci, które prawdopodobnie mogły zostać wykorzystane do naruszenia zabezpieczeń systemu informatycznego;
      b) zablokowanie konta użytkownika podejrzanego o naruszenie zasad bezpieczeństwa;
      c) zmianę hasła administratora systemu oraz użytkowników systemu, w celu uniknięcia ponownej próby uzyskania dostępu do bazy danych przez np. konto użytkownika będącego na urlopie.
   2) Zapisania wszelkich informacji i okoliczności analizowanego zdarzenia z uwzględnieniem czasu i źródła uzyskania informacji.
   3) Wygenerowania wszelkich możliwych raportów i dokumentów, które mogą pomóc w ustaleniu przyczyn oraz osoby odpowiedzialnej za naruszenia bezpieczeństwa, każdą ze stron raportu oraz dokumentu należy autoryzować.
   4) Przystąpienia do szczegółowej analizy przyczyn zaistniałego zdarzenia, w tym do określenia skali zdarzenia i wstępnego określenia strat.
   5) Sprawdzenie zabezpieczeń oraz przygotowanie raportu dla administratora bezpieczeństwa informacji.
   6) Współpracy z kierownikiem komórki organizacyjnej oraz z administratorem bezpieczeństwa informacji w celu ustalenia szczegółów zaistniałego zdarzenia
   7) Przywrócenia normalnego działania systemu, przy czym, jeśli nastąpiło uszkodzenie bazy danych, odtworzenie jej z ostatniej kopii awaryjnej z zachowaniem wszelkich możliwych środków ostrożności mających na celu uniknięcie ponownego naruszenia bezpieczeństwa danych osobowych.

8. PROCES SZKOLENIA W ZAKRESIE OCHRONY DANYCH OSOBOWYCH

§ 21

Szkolenie pracowników oraz osób zatrudnionych na podstawie umowy cywilno-prawnej

1. Obowiązek szkolenia wynika z przepisów Ustawy o ochronie danych osobowych oraz rozporządzeń wykonawczych do tej ustawy.
2. Szkolenie dotyczy osób które:
   1) są w procesie przyjmowania ich do pracy w Instytucie;
   2) są w trakcie zawierania umowy cywilno-prawnej;
   3) są pracownikami Instytutu i zobowiązani są uczestniczyć w szkoleniu planowym.

3. Działając w imieniu i na rzecz Administratora Danych Osobowych, Administrator Bezpieczeństwa Informacji ustala następujący plan szkoleń:
   1) każdy nowo przyjęty pracownik zostaje przeszkolony z zasad przetwarzania danych osobowych w Instytucie, zgodnie z zakresem tematycznym szkoleń, co potwierdza podpisując stosowne oświadczenie wg wzoru stanowiący **załącznik Nr 3** do niniejszej Polityki Bezpieczeństwa. Podpisanie oświadczenia uprawnia pracownika do wystąpienia o wystawienie imiennego upoważnienia do przetwarzania danych osobowych na terenie Instytutu;
   2) posiadanie „Poświadczenia bezpieczeństwa osobowego" uprawniającego do dostępu do informacji niejawnych o klauzuli zastrzeżone lub wyższej, jest jednoznaczne z odbyciem szkolenia z zakresu przetwarzania danych osobowych i wszelkimi z tym związanymi obowiązkami Instytutu;
   3) dodatkowe szkolenia wewnętrzne osób upoważnionych do przetwarzania danych osobowych przeprowadzane będą w przypadku istotnej zmiany przepisów dotyczących przetwarzania danych osobowych, bądź zgłoszenia takiej potrzeby przez kierownika komórki organizacyjnej;
4. Cel tematyczny szkoleń:

   Celem szkoleń jest zapoznanie pracowników Instytutu z polskimi standardami ochrony danych osobowych oraz pogłębienie wiedzy w zakresie rozwiązań prawnych, dotyczących ochrony danych osobowych przyjętych w Polsce oraz nabycie praktycznych umiejętności wypełniania obowiązków nałożonych prawem w tym zakresie.
5. Zakres tematyczny szkoleń obejmuje następujące tematy:
   1) podstawy prawne przetwarzania danych osobowych;
   2) podstawowe pojęcia i definicje związane z ochroną danych osobowych;
   3) przepisy wewnętrzne dotyczące przetwarzania danych osobowych;
   4) prawo do informacji a ochrona prywatności (zakres prawa do prywatności);
   5) prawa osoby, której dane dotyczą (do informacji, do modyfikacji danych, żądania zaprzestania przetwarzania danych, żądania usunięcia danych);
   6) dane wrażliwe – szczególne kategorie danych osobowych;
   7) prawidłowe zasady powierzania i podpowierzania przetwarzania danych osobowych;
   8) obowiązki osób upoważnionych do przetwarzania danych osobowych;
   9) zadania administratora bezpieczeństwa informacji;
   10) mechanizmy kontrolne;
   11) konsekwencje naruszenia ustawy – odpowiedzialność karna i dyscyplinarna.

9. UDOSTĘPNIANIE DANYCH OSOBOWYCH

§ 22

Zasady udostępniania danych osobowych

1. Instytut udostępnia dane osobowe przetwarzane we własnych zbiorach danych, tylko osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa, na ich wniosek.

2. Informacje o miejscu przetwarzania, osobach przetwarzających dane osobowe oraz metodach zabezpieczenia danych sporządzone zgodnie z **załącznikiem Nr 1** do niniejszej Polityki Bezpieczeństwa dostępne są u kierownika komórki organizacyjnej oraz Administratora Bezpieczeństwa Informacji.
3. Ze względów bezpieczeństwa, szczegóły techniczne i procedury opracowane na wypadek sytuacji awaryjnych, znajdują się u Administratorów lokalnych , odpowiedzialnych za bazy danych w danej komórce organizacyjnej.

10. POSTEPOWANIE NA WYPADEK AWARII/KATASTROF I UTRATY DANYCH. ZAPEWNIENIE CIĄGŁOŚCI DZIAŁANIA

§ 23

1. W Instytucie, przygotowany jest plan postępowania na wypadek wystąpienia poważnych awarii systemu, uszkodzeń lub utraty danych w wyniku pożaru, zalania lub innych nie dających się przewidzieć zdarzeń.
2. W przypadku zdarzenia, które uniemożliwia zachowanie ciągłości działania podstawowych zasobów informatycznych, uruchamiana jest procedura przywracania kluczowych funkcji systemu. Służy temu procedura tworzenia kopii zapasowych systemów - właściwa dla danego systemu a także procedura tworzenia kopii bezpieczeństwa i kopii archiwalnych(tam gdzie zasoby pamięci to umożliwiają).
3. Główną przyczyną zaprzestania funkcjonowania podstawowego systemu do obsługi pacjentów (CliniNet), systemu obsługi kadrowej (Simple), Krajowego Rejestru Nowotworów, systemu obsługującego Zakład Patologii i Diagnostyki Laboratoryjnej (Patarch), może być brak zasilania z sieci miejskiej. Rozwiązania obecnie istniejące nie umożliwiają podtrzymania zasilania serwerów z agregatów prądotwórczych, gdyż nie są one podłączone do tych obwodów. UPS-y pozwalaj tylko na bezpieczne wyłączenie serwerów. Stacje robocze użytkowników w 95% nie posiadają UPS-ów. Ze względu na rozwiązania systemowe, gdzie serwery kluczowych systemów pracują w „farmie" i nie ma pojęcie serwera odpowiedzialnego za dany system, pojęcie serwer systemu, jest pojęciem wirtualnym. Wydzielone systemy mają oddzielne serwery (np. poczta) i restartowane są według procedur przewidzianych dla tych systemów. Proces przywracania systemu do funkcjonowania po zaniku zasilania, polega na odtworzeniu systemu z kopii bezpieczeństwa tworzonych codziennie. Zasoby pamięci nie pozwalają na tworzenie cyklicznie kopii archiwalnych. W sytuacji braku zasilania, do czasu przywrócenia kluczowych funkcji systemu, wypełnia się dokumentację w formie papierowej a po przywróceniu systemu wprowadza się do niego dane z dokumentacji formie papierowej.
4. Systemy autonomiczne, aplikacje (Aria, IntraRis, Spectra Pacs, Oncentra, Mosaiq, iView, XVI1, XVI2, XVI3, Oncentra Brachy, Oncentra Prostate), przywracane są do działania w trybie właściwym dla tych systemów i aplikacji, zgodnie z procedurami opracowanymi przez Administratorów tych Systemów lub przez firmy zewnętrzne (dostawcy usług), zobowiązane na podstawie podpisanych przez Instytót umów.

5. Systemy, dla których Instytut jest Gestorem (Baza Danych ZSI-CRN), przywraca się do działania zgodnie z procedurą właściwą dla systemów, których wirtualne serwery umiejscowione są w „farmie”.
6. W Instytucie ustalony jest Zespół Zarządzania Kryzysowego, który w sytuacji kryzysowej - podejmuje odpowiednie działania.
7. W skład zespołu wchodzą:
   1) Zastępca Dyrektora ds. Zarządzania i Finansów
   2) Administrator Systemów Informatycznych – Kierownik Działu Informatyki
   3) Administratorzy Systemu/Administratorzy Lokalni
   4) Przedstawiciele uprawnionych podmiotów zewnętrznych świadczących usługi informatycznego wsparcia systemu (wg potrzeb).

11. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA

§ 24

Polityka Bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Administrator Bezpieczeństwa Informacji może zarządzić przegląd Polityki Bezpieczeństwa stosownie do potrzeb oraz dokonać aktualizacji, przedkładając projekt stosownych zmian Dyrektorowi Instytutu. Administrator Bezpieczeństwa Informacji, po uzgodnieniu z Dyrektorem Instytutu, może stosownie do potrzeb przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami ustawy . Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z Administratorem Systemu. Zakres, przebieg i rezultaty audytu dokumentowane są na piśmie w protokole podpisywanym zarówno przez Administratora Bezpieczeństwa Informacji, jak i Kierownika Działu Informatyki.

12. POSTANOWIENIA KOŃCOWE

§ 25

Dla zapewnienia bezpieczeństwa całości systemu wszelkie zmiany powinny podlegać formalnym procedurom, inicjowanym i zatwierdzonym przez Kierownika Działu Informatyki oraz Administratora Bezpieczeństwa Informacji. W szczególności procedury te powinny uwzględniać następujące procesy:

1) identyfikacja i prowadzenie dokumentacji istotnych zmian systemu – klasyfikacja zasobów;
2) prowadzenie analiz potencjalnego zagrożenia, wynikająca z wprowadzonych zmian;
3) ustalanie poziomu zabezpieczeń dla wprowadzanych zmian;
4) zatwierdzanie proponowanych zmian;
5) wprowadzanie zatwierdzonych zmian z uwzględnieniem procesu szkoleniowo-informacyjnego.

FORMULARZ AKTUALIZACYJNY

(NAZWA KOMÓRKI ORGANIZACYJNEJ)

OSOBY PRZETWARZAJĄCE DANE OSOBOWE W SYSTEMACH INFORMATYCZNYCH

KIEROWNIK KOMÓRKI ORGANIZACYJNEJ

Nazwisko	Imię	Stanowisko	e-mail

ADMINISTRATOR SYSTEMU/SYSTEMÓW LUB FIRMA ZEWNĘTRZNA

Nazwisko	Imię	Nazwa podmiotu zewnętrznego	Adres podmiotu zewn.	e-mail	nr telefonu

PRACOWNICY KOMÓRKI ORGANIZACYJNEJ PRZETWARZAJĄCY DANE OSOBOWE W SYSTEMACH INFORMATYCZNYCH

Lp.	Nazwisko	Imię	Stanowisko	Numer upoważ-nienia	Data nadania upoważn	Data zakończ upoważn	Identyfi-kator /login	Nazwa bazy danych /systemu	Zakres upraw-nień
1									
2									
3					.				

Zakres uprawnień: 1. Wprowadzanie danych. 2. Przeglądanie danych. 3. Modyfikacja danych. 4. Generowanie wydruków. 5. Udostępnianie danych. 6. Usuwanie danych. 7. Wykonywanie kopii bezpieczeństwa. 8.Administrowanie systemem/bazą danych.

PRZECHOWYWANIE ORAZ CZĘSTOTLIWOŚĆ WYKONYWANIA KOPII AWARYJNYCH SYSTEMU/ BAZY DANYCH

Lp.	Nazwa systemu/bazy danych	Miejsce zapisu danych (serwer syst., bazy danych, stacja robocza	Rodzaj i częstotliwość wykonywania kopii (kopie przyrostowe, awaryjne, archiwalne)	Lokalizacja		Opis zabezpieczeń pomieszczenia, w którym znajdują się kopie*	Osoba odpowiedzialna za tworzenie kopii	Uwagi
				Piętro	Nr pokoju			
1								

*Opis zabezpieczeń pomieszczenia, w którym znajdują się kopie:1. drzwi antywłamaniowe, 2. zamki atestowane, 3. szyby oklejone folią antywłamaniową, 4. kraty w oknach, 5. brak okien, 6. instalacja alarmowa, 7. firma ochroniarska, 8. dyżur 24h, 9. inne ...(proszę wymienić)

LOKALIZACJA STANOWISK KOMPUTEROWYCH WYKORZYSTYWANYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Lp.	Lokalizacja		Opis zabezpieczeń pomieszczenia*	Opis zabezpieczeń danych**	Uwagi
	Piętro	Nr pokoju			
1					

Opis zabezpieczeń pomieszczenia:1. drzwi antywłamaniowe, 2. zamki atestowane, 3. szyby oklejone folią antywłamaniową, 4. kraty w oknach, 5. brak okien,6. instalacja alarmowa, 7. firma ochroniarska, 8. dyżur 24h, 9. inne ...(proszę wymienić).

**Opis zabezpieczeń danych: 1. indywidualne konta użytkowników 2. program antywirusowy 3. dostęp na hasło 4. inne ...(proszę wymienić).

WYKAZ ZEWNĘTRZNYCH BAZ DANYCH* W SYSTEMACH INFORMATYCZNYCH, DO KTÓRYCH KOMÓRKA ORGANIZACYJNA MA DOSTĘP.

Lp.	Nazwa zewnętrznej bazy danych	Lokalizacja stanowisk z dostępem do zewnętrznej bazy danych		Wykaz osób posiadających uprawnienia do dostępu do zewnętrznej bazy danych	Uwagi
		Piętro	Nr pokoju		

1					
2					

*Wykaz zewnętrznych baz danych: bazy danych do których mamy dostęp a nie są tworzone przez Instytut.

PRZECHOWYWANIE DANYCH OSOBOWYCH PRZETWARZANYCH MANUALNIE

Lp.	Nazwa zbioru danych	Lokalizacja		Sposób fizycznego zabezpieczenia zbioru danych osobowych*	Uwagi
		Piętro	Nr pokoju		
1					
2					

*Sposób fizycznego zabezpieczenia zbioru danych osobowych: 1. drzwi antywłamaniowe, 2. zamki atestowane, 3. szyby oklejone folią antywłamaniową, 4. kraty w oknach, 5. brak okien, 6. instalacja alarmowa, 7. firma ochroniarska, 8. dyżur 24h, 9. inne ...(proszę wymienić).

OPIS DANYCH OSOBOWYCH GROMADZONYCH W ZBIORZE DANYCH KOMÓRKI ORGANIZACYJNEJ
(krótki opis, co to są za Dane)

Dane aktualne na dzień: ...../...../.....

Sporządził: .....
(imię, nazwisko, stanowisko)

Warszawa, dn. ... - … - 20 … r.

_____
(pieczęć komórki/jednostki organizacyjnej)

Administrator Bezpieczeństwa Informacji

_____
(w miejscu)

W N I O S E K

Zgodnie z art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.), wnioskuję o:

¤ nadanie

¤ zmianę

¤ pozbawienie uprawnień;

……
(imię i nazwisko pracownika/strona innej umowy)

……
(stanowisko/komórka organizacyjna/nazwa firmy świadczącej usługę)

imiennego upoważnienia do przetwarzania danych osobowych w Centrum Onkologii Instytucie im. Marii Skłodowskiej-Curie w Warszawie w systemie/systemach* informatycznych:

…… Nazwa systemu i zakres(dozwolone czynności):

…… .. Nazwa systemu i zakres(dozwolone czynności):

……... Nazwa systemu i zakres(dozwolone czynności):

…….. Nazwa systemu i zakres(dozwolone czynności):

- Uprawnienia zgodne z zakresem obowiązków na zajmowanym stanowisku;
- Uprawnień większe niż wynika to z zajmowanego stanowiska(użytkownik uprzywilejowany);
- Pozbawienie uprawnień z powodu rozwiązania umowy o pracę;
- Pozbawienie uprawnień(inny powód) ……

Zakres (dozwolone czynności)**:**
1. Wprowadzanie danych.
2. Przeglądanie danych.
3. Modyfikacja danych.
4. Generowanie wydruków.
5. Udostępnianie danych.
6. Usuwanie danych.
7. Wykonywanie kopii bezpieczeństwa.
8 Administrowanie systemem/bazą danych.

……..……..
(podpis kierownika komórki/jednostki organizacyjnej)

* *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

……..…..
(imię i nazwisko pracownika)

……
(stanowisko)

OŚWIADCZENIE PRACOWNIKA

Centrum Onkologii – Instytutu im. Marii Skłodowskiej – Curie w Warszawie

Ja niżej podpisany/a* oświadczam, ze zostałem zapoznany/na* z przepisami dotyczącymi ochrony danych osobowych i zobowiązuje się do ich przestrzegania:

1. ustawy z dnia 29 sierpnia 1997 r. (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.) o ochronie danych osobowych,
2. 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. Nr 100, poz.1024),
3. instrukcji ogólnej określającej sposób zarządzania systemem informatycznym zbiorów danych osobowych w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie,
4. Polityki Bezpieczeństwa obowiązującej w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie.

…….
(data i podpis pracownika)

Oświadczenie zostało złożone w obecności pracownika:

…….
(podpis i pieczęć imienna pracownika)

* *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

_____
(pieczęć nagłówkowa pracodawcy)

Upoważnienie imienne do przetwarzania danych osobowych

nr …/…/…

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz. U. z 2014 r., poz. 1182 ze zm.) upoważniam Pana/Panią*:

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

……...
(nazwa komórki/ jednostki organizacyjnej lub nazwa pracodawcy)

……...
(stanowisko)

Obsługiwany system/baza danych/program*:

Zakres upoważnienia:

(**Zakres:** 1. wprowadzanie danych. 2. przeglądanie danych. 3. modyfikacja danych. 4. generowanie wydruków. 5. udostępnianie danych. 6. usuwanie danych. 7. wykonywanie kopii bezpieczeństwa. 8. administrowanie systemem/bazą danych.)
Jednocześnie zobowiązuję do zachowania w tajemnicy wszelkich informacji dotyczących przetwarzanych danych osobowych oraz sposobu ich zabezpieczenia również po rozwiązaniu umowy o pracę.

Upoważnienie ważne od dnia wystawienia do odwołania lub rozwiązania umowy o pracę.

Wszystkie wydane wcześniej Panu/Pani* upoważnienia do przetwarzania danych osobowych w Centrum Onkologii –Instytucie im. Marii Skłodowskiej-Curie w Warszawie w dniu otrzymania niniejszego upoważnienia tracą ważność.

.....
(podpis Administratora Danych)

* *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

……...
(pieczęć pracodawcy)

……..
(imię i nazwisko pracownika)

……
(stanowisko)

OŚWIADCZENIE
(dla osób reprezentujących podmiot zewnętrzny)

Ja niżej podpisany/a* oświadczam, ze zostałem zapoznany/na* z przepisami dotyczącymi ochrony danych osobowych i zobowiązuje się do ich przestrzegania przez podmiot, w imieniu którego działam oraz przez osoby, które będą wykonywały przedmiot umowy z ramienia podmiotu, który reprezentuję:

1. ustawy z dnia 29 sierpnia 1997 r. (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.) o ochronie danych osobowych,
2. 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. Nr 100, poz.1024),
3. instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w …….
4. Polityki Bezpieczeństwa obowiązującej w ……..

…….……
(data i podpis pracownika)

* *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

OŚWIADCZENIE PRACOWNIKA

Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie o wyrażeniu zgody na przetwarzanie danych osobowych w celach rekrutacyjnych

Wyrażam zgodę na przetwarzanie mich danych osobowych przez Centrum Onkologii-Instytut im. Marii Skłodowskiej-Curie w Warszawie zawartych w niniejszym wniosku dla potrzeb niezbędnych do realizacji procesu rekrutacji zgodnie z ustawą z dnia 29 sierpnia 1997 r. (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.) o ochronie danych osobowych.)

Równocześnie oświadczam, że zostałem/am* poinformowany/a* o tym, że podanie moich danych osobowych jest dobrowolne oraz przysługuje mi prawie wglądu, poprawiania i uzupełniania moich danych osobowych za pośrednictwem Działu Spraw Pracowniczych i Spraw Socjalnych.

……
(data i podpis pracownika)

Oświadczam, że podane we wniosku oraz załącznikach do wniosku dane są zgodne z aktualnym stanem faktycznym (zgodnie z art. 233 §1 Kodeksu karnego - kto składając zeznanie mające służyć za dowód w postępowaniu sądowym lub w innym postępowaniu prowadzonym na podstawie ustawy, zezna nieprawdę lub zataja prawdę, podlega karze pozbawienia wolności do lat 3).

Przyjmuję do wiadomości, że Działu Spraw Pracowniczych i Spraw Socjalnych Instytutu może zażądać przedstawienia do wglądu oryginałów dokumentów potwierdzających dane zapisane we wniosku.

……..……
(data i podpis pracownika)

Oświadczenie zostało złożone w obecności pracownika:

…….
(podpis i pieczęć imienna pracownika)

* *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

……..
(wnioskodawca)

Dyrektor
Centrum Onkologii –Instytutu
im. Marii Skłodowskiej - Curie
02-034 Warszawa, ul. Wawelska 15B

WNIOSEK
podmiotu zewnętrznego o udostępnienie danych osobowych

Zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.), wnioskuje o udostępnienie danych osobowych ze zbioru danych Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie w Warszawie.

Cel udostępnienia:

……

Zakres udostępnionych danych osobowych:

……

Wskazanie podstawy prawnej uprawniającej do dostępu do w/w dokumentów:

……

Informacje umożliwiające wyszukanie w zbiorze żądanych danych:

……

Sposób udostępnienia danych:

……
(wgląd w siedzibie Instytutu, sporządzenie kopii, itp.)

Sposób odbioru dokumentacji:

……

……
(data, podpis wnioskodawcy)

Decyzja Dyrektora

.....
(data, podpis, pieczęć)

Warszawa, dn. ... - … - 20 … r.

……..
(imię i nazwisko osoby wnioskującej*)

……
(adres)

Centrum Onkologii – Instytut
im. Marii Skłodowskiej-Curie
ul. Wawelska 15 B
02-034 Warszawa

WNIOSEK

o udzielenie informacji na temat danych osobowych przetwarzanych przez Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie

Ja niżej podpisany/a** jako osoba, której dane osobowe przetwarzane są w zbiorze danych osobowych prowadzonym przez Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie, na podstawie art. 33. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.), zwracam się z uprzejmą prośbą o udzielenie następujących informacji:

1. o celu, zakresie i sposobie przetwarzania danych,
2. od kiedy przetwarzane są dane dotyczące mojej osoby,
3. o źródle z którego pochodzą, przetwarzane przez Państwa, moje dane osobowe,
4. o odbiorcach, którym moje dane są udostępniane,
5. o sposobie udostępniania moich danych osobowych.

……..……..……
(data i podpis wnioskodawcy)

Oświadczenie zostało złożone w obecności pracownika:

…….
(podpis i pieczęć imienna pracownika)

* *nazwisko, imię, adres zamieszkania lub nazwa podmiotu zewnętrznego adres, NIP*;
** *niepotrzebne skreślić*

Warszawa, dn. ... - … - 20 … r.

Centrum Onkologii – Instytut
im. Marii Skłodowskiej-Curie
ul. Wawelska 15 B
02-034 Warszawa

...……..
(imię i nazwisko osoby wnioskującej)

……
(adres)

INFORMACJA

o danych osobowych przetwarzanych przez Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie

W związku z Pana/i* wnioskiem z dnia …….. o udzielenie informacji na temat danych osobowych przetwarzanych przez Centrum Onkologii – Instytut im. Marii Skłodowskiej-Curie, działając na podstawie art. 33. ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j. t. Dz. U. z 2014 r., poz. 1182 ze zm.) uprzejmie informuje, że:

1. Pana/i* dane osobowe są dostępne a administrator danych nie zaprzestał ich przetwarzania,
2. Administratorem Danych Osobowych jest Dyrektor Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie, ul. Wawelska 15B, 02-034 Warszawa,
3. Pana/i* dane osobowe są dostępne w następującym zakresie: ……..……...…,
4. dane przetwarzane są w celu ……...,
5. dane przetwarzane są od dnia ……....,
6. dane zostały uzyskane ……..……...,
7. dane (nie*) są udostępniane innym podmiotom ……..….,
8. na podstawie ……... .

……
(podpis Administratora Danych Osobowych

* *niepotrzebne skreślić*

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

załącznik do „Polityki Bezpieczeństwa" nr 10 zgodnie z § 4 pkt. 1 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

Lp.	Dokładny adres *(np. adres gdzie przetwarzane są dane)*	Komórka organizacyjna użytkująca pomieszczenie	Nr pokoju lub pomieszczenia	Rodzaj zastosowanego zabezpieczenia pomieszczenia	Uwagi
1.	*Pełny adres podmiotu*	*np. gabinet dyrektora*	*10*	*drzwi zamykane na klucz, kraty w oknach*	
2.	*Pełny adres podmiotu*	*np. punkt pielęgniarski*	*jeśli nie jest nadany to powtórzyć nazwę*	*monitoring*	
3.	*Pełny adres podmiotu*	*np. księgowość*	*14*	*służba ochrony budynku*	
4.	*Pełny adres podmiotu*	*np. kadry*	*17*	*alarm*	
5.	*Pełny adres podmiotu*	*np. punkt obsługi pacjenta*	*25*		

Data i podpis Administratora Danych

….....

Należy wypisać wszystkie pomieszczenia w których dane osobowe są przetwarzane (pobierane, zmieniane, przechowywane itp.).

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

Lp.	Nazwa zbioru danych *(np. dane pacjentów, pracowników itd.)*	Programy zastosowane do przetwarzania danych *(np. program księgowy, papierowa ewidencja pracowników, adres internetowy aplikacji itd.)*	Uwagi
1.	*np. akta osobowe pracowników*	*wersja papierowa*	
2.	*np. faktury*	*wersja elektroniczna - optima*	
3.	*np. korespondencja*	*wersja papierowa*	
4.	*np. księga ewidencji dzieci*	*wersja papierowa*	
5.	*np. ewidencja pacjentów*	*wersja papierowa i elektroniczna*	

Data i podpis Administratora Danych Osobowych

….....

W tym załączniku należy wyszczególnić wszystkie zbiory danych osobowych jakie występują w podmiocie. Zbiór danych osobowych to zbiór o charakterze osobowym (imiona, nazwiska, data urodzenia, pesel), który jest w jakiś sposób uporządkowany (np. pola w kwestionariuszu osobowym, czy rekordy w bazie danych). Należy pamiętać o podaniu formy w jakiej zbiór jest przetwarzany, może to być zarówno wersja papierowa jak i elektroniczna. Wersją elektroniczną będą tylko te bazy prowadzone w systemach które mają możliwość wyszukania po odpowiednim kluczu osoby z pełnej bazy danych, więc edytory tekstu typu Word będą traktowane nadal jako wersja papierowa.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami

Lp.	Nazwa zbioru danych *(np. dane pacjentów, pracowników itd.)*	Struktura zbiorów *(np. imię i nazwisko, e-mail, telefon itd.)*	Przepływ danych (np. wydruk danych z internetu)	Uwagi
1.	*Akta osobowe pracowników*	*Imię, nazwisko, data urodzenia, miejsce urodzenia, imiona rodziców, adres zamieszkania, numer telefonu, PESEL, NIP, numer i seria dowodu osobistego, wykształcenie, stan zdrowia.*	*np. wersja papierowa → system kadry → serwer x →wydruk*	
2.	*Dziennik korespondencyjny*	*Imię, nazwisko, adres.*	*brak przepływu z wersji papierowej*	

Data i podpis Administratora Danych Osobowych

….....

Na strukturę składa się informacja z jakich danych tzn. z jakich pól informacyjnych składa się zbiór, czyli trzeba zadeklarować jego zakres, który będzie potrzebny do rejestracji zbiorów.

Przepływ danych dotyczy tylko zbiorów elektronicznych (w papierowych w ogóle on nie występuje), i jest opisywany na zasadzie drogi danych osobowych przez poszczególne etapy od pobrania z wersji papierowej, przez wprowadzenie do wersji elektronicznej, po drodze może występować zapis na serwerach lub liczne wydruki.

Ewidencja osób przetwarzających dane osobowe posiadających upoważnienia

Lp.	Nazwisko	Imię	Stanowisko	Numer upoważnienia	Data nadania upoważnienia	Data odwołania upoważnienia	Identyfikator /login	Nazwa bazy danych /systemu	Zakres uprawnień
1									
2									
3									

Zakres uprawnień:

1. Wprowadzanie danych.
2. Przeglądanie danych.
3. Modyfikacja danych.
4. Generowanie wydruków.
5. Udostępnianie danych.
6. Usuwanie danych.
7. Wykonywanie kopii bezpieczeństwa.
8. Administrowanie systemem/bazą danych.

UMOWA O ZACHOWANIU POUFNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu …..... r. pomiędzy: ..... z siedzibą w …..... …....., zarejestrowaną/ym w …..... pod numerem …....., posiadającą/ym numer NIP …..... oraz numer REGON …....., reprezentowaną/ym przez:…....., zwaną/ym dalej **Zleceniodawcą**, a ..... z siedzibą w ……..... , zarejestrowaną/ym w …..... pod numerem …....., posiadającą/ym numer NIP..... oraz numer REGON …....., reprezentowaną/ym przez: …....., zwaną/ym dalej **Zleceniobiorcą.**

§ 1
Definicje

1. Administrator Danych Osobowych (ADO) – Dyrektor XYZ, decydujący o celach i środkach przetwarzania danych osobowych;
2. Administrator Bezpieczeństwa Informacji (ABI) – osoba wyznaczona przez Dyrektora XYZ, odpowiedzialna za organizację i bezpieczeństwo danych osobowych;
3. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
4. Przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, udostępnianie, opracowywanie, zmienianie, usuwanie;
5. Ustawa – rozumie się prze to ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. nr 133, poz. 883 ze zm.);
6. Rozporządzenie – Rozporządzenie 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. z 2004 r. nr 100, poz. 1024);

§ 2
Przedmiot Umowy

1. Przedmiotem umowy jest nadanie upoważnienia Zleceniobiorcy do przetwarzania zbioru danych osobowych tj. …..,
2. Celem obsługi zbioru danych osobowych jest realizacja.....,
3. Zakres przetwarzania obejmuje dane osobowe....., w tym: …..
4. Upoważnienie umożliwia Zleceniobiorcy przetwarzanie danych osobowych udostępnianych przez Zleceniodawcę wyłącznie w celu realizacji: …..... w okresie niezbędnym dla jej realizacji.

§ 3

Zobowiązania Zleceniobiorcy dotyczące ochrony danych osobowych

1. Zleceniobiorca zobowiązuje się przetwarzać dane osobowe do których uzyskał upoważnienie wyłącznie w zakresie i celu przewidzianym w Umowie.
2. Zleceniobiorca zobowiązuje się do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
3. Zleceniobiorca zobowiązuje się do przetwarzania danych wyłącznie w systemach informatycznym Zleceniodawcy. Zabrania się jakiegokolwiek kopiowania i utrwalania tych danych poza systemem informatycznym Zleceniodawcy.
4. Zleceniobiorca w związku z wykonywaniem Umowy jest zobowiązany do przestrzegania zasad bezpieczeństwa ochrony danych osobowych opisanych w Polityce Bezpieczeństwa Zleceniodawcy, Ustawie i Rozporządzeniu.
5. Zleceniobiorca ponosi odpowiedzialność za będące następstwem jego zachowań szkody wyrządzone niezgodnym z Umową przetwarzaniem danych osobowych, w szczególności szkody wyrządzone udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 4

1. Zleceniobiorca zobowiązuje się do dopuszczania do przetwarzania danych wyłącznie osoby posiadające upoważnienie nadane przez Zleceniobiorcę, zgodnie z następującymi punktami:

   - Gdy zleceniobiorca w pełni zarządza osobami upoważnionymi:

     - Zleceniobiorca przeprowadza szkolenie z zasad ochrony danych osobowych i jeśli to ustalone, zgodnie z wytycznymi przekazanymi przez Zleceniodawcę;
     - Zleceniobiorca nadaje upoważnienia osobom wykonującym usługę do przetwarzania danych osobowych w ramach realizacji warunków Umowy;
     - Zleceniobiorca zobowiązuje się do uzyskania od osób upoważnionych pisemnych, imiennych Oświadczeń/Umów o poufności;
     - Zleceniobiorca zobowiązuje się do przekazania aktualnej listy osób upoważnionych do Zleceniodawcy.

   - Gdy dostępem do przetwarzania osób zatrudnionych przez Zleceniobiorcę zarządza Zleceniodawca:

     - Zleceniodawca zastrzega sobie prawo nadawania upoważnień pracownikom Zleceniobiorcy i prowadzenia ich aktualnej ewidencji;
     - Zleceniodawca przeprowadza szkolenie z zasad ochrony danych osobowych, zgodnie z Polityką Bezpieczeństwa Zleceniodawcy dla osób, którym nadaje upoważnienia
     - Zleceniodawca zastrzega sobie uzyskania od osób upoważnionych pisemnych, imiennych Umów o poufności;
     - Zleceniodawca zobowiązuje się do przekazania aktualnej listy osób upoważnionych do Zleceniobiorcy;

2. Upoważnienie i Oświadczenie, znajduje się w Załączniku 4 i 5 do Polityki Bezpieczeństwa CO-I.

§ 5

1. W przypadku, gdy Umowa uprawnia Zleceniobiorcę do jej wykonania przy udziale osób trzecich, postanowienia paragrafów poprzedzających rozciągają się również na te osoby, przy czym Zleceniobiorca odpowiada za działania lub zaniechania osób, którymi się posługuje lub którym powierza wykonanie niniejszej Umowy, jak za działania lub zaniechania własne.
2. W przypadku naruszenia przepisów Ustawy w ramach realizacji Umowy z przyczyn leżących po stronie Zleceniobiorcy, w następstwie którego Zleceniodawca zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Zleceniobiorca zobowiązuje się do zwrócenia równowartości odszkodowania lub grzywny poniesionych przez Zleceniodawcę.

§ 6

1. Wszelkie zmiany Umowy powinny być dokonane w formie pisemnej pod rygorem nieważności;
2. W sprawach nieuregulowanych Umową, zastosowanie znajdują przepisy polskiego prawa, w tym Ustawy oraz Kodeksu Cywilnego.
3. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Zleceniobiorca	Zleceniodawca
….....	….....