ZARZĄDZENIE NR 42/2019

Dyrektora Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie
z dnia 14 czerwca 2019 r.

w sprawie wprowadzenia „Regulaminu ochrony danych osobowych w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie"

Na podstawie § 7 Statutu Centrum Onkologii – Instytutu im. Marii Skłodowskiej-Curie, zarządza się, co następuje:

§ 1

Wprowadza się do stosowania w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie „Regulamin ochrony danych w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie", stanowiący załącznik do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem wydania.

z up. DYREKTORA
Centrum Onkologii-Instytutu
im. Marii Skłodowskiej-Curie
Zastępca Dyrektora ds. Zarządzania
Milena Witczak

Regulamin Ochrony Danych Osobowych w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) dla:

1. pracowników bez względu na formę zatrudnienia,
2. współpracowników,
3. użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez administratora / podmiot przetwarzający.

SPIS TREŚCI

1 Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony, pamięci przenośne (w tym dyski).
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Zabrania się samowolnego demontażu sprzętu IT, instalowania dodatkowych podzespołów (np. dysków twardych, pamięci).
4. Zabrania się podłączania jakichkolwiek niezatwierdzonych przez Dział Informatyki urządzeń do sieci komputerowej.
5. Użytkownik zobowiązany jest do szyfrowania lub do usuwania plików z nośników/dysków do których mają dostęp użytkownicy nieupoważnieni do dostępu do plików z danymi osobowymi (np. podczas współużytkowania sprzętu IT).
6. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczyć płytę DVD w niszczarce). Pozostali użytkownicy zobowiązani są do przekazania protokolarnie pracownikowi Działu Informatyki nośników przeznaczonych do zniszczenia.

2 Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Tworzenie kont użytkowników wraz z uprawnieniami do użytkowania sprzętu IT (np. dla komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie przełożonych, a wykonywane jest przez pracowników Działu Informatyki / administratorów
2. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem systemu Windows na swoim komputerze).
3. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym pracowników Działu Informatyki / administratorów.
4. Użytkownik zobowiązany jest do uniemożliwienia osobom niepowołanym (np. pacjentom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. Polityka czystego ekranu.
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu (poprzez wciśnięcie kombinacji klawiszy: Klawisz z logo systemu Windows + L).
6. Użytkownik udostępniający stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązany jest wylogować się z programów (systemu informatycznego).
7. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z programów (systemu informatycznego),
    b) jeżeli jest to możliwe wyłączyć sprzęt komputerowy,
    c) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

3 Polityka haseł

1. Hasła powinny składać się z min. 9 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry + znaki specjalne.
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy naklejać ich na monitorze komputera, trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić. W wypadku braku możliwości zmiany hasła należy powiadomić o tym fakcie Dział Informatyki.
6. W celu podwyższenia poziomu ochrony danych osobowych przetwarzanych w formie elektronicznej (np. w programach komputerowych, witrynach internetowych) hasła dostępowe do tych danych powinny być zmieniane nie rzadziej, niż co 90 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła. W systemach zawierających dane medyczne hasło powinno być zmieniane nie rzadziej, niż co 30 dni.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po jego zmianie.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemach komputerowych Instytutu.
11. Zabrania się stosowania tego samego hasła do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi możliwy do odgadnięcia klucz (np. nazwa kolejnego miesiąca).

4 Zabezpieczenie dokumentacji z danymi osobowymi w wersji papierowej

1. Pracownicy zobowiązani są do weryfikacji przydatności oraz niszczenia zbędnych dokumentów zawierających dane osobowe w niszczarkach lub przekazywania ich w bezpieczny sposób do utylizacji (zasady ustala kierownik komórki organizacyjnej / bezpośredni przełożony).
2. Zabrania się wyrzucania niezniszczonych dokumentów zawierających dane osobowe.
3. Pracownicy zobowiązani są zabezpieczać dokumenty znajdujące się w ich posiadaniu. W miarę możliwości dokumenty zamykamy w szafach, biurkach, pomieszczeniach - zabezpieczmy je w ten sposób przed kradzieżą lub wglądem osób nieupoważnionych. Jeżeli jest taka możliwość zamykamy na klucz opuszczane pomieszczenia.
4. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.

5 Zasady wynoszenia nośników z danymi poza Instytut

1. Użytkownicy nie mogą bez zgody kierownika komórki organizacyjnej / bezpośredniego przełożonego wynosić poza teren Instytutu nośników z zapisanymi danymi osobowymi.

Do nośników zaliczamy m.in. wymienne dyski twarde, pendrive, płyty CD, DVD, pamięci typu Flash.

2. Nośniki elektroniczne zawierające dane osobowe mogą być wynoszone poza miejsce pracy tylko w postaci zaszyfrowanej (szyfrowane dyski, pliki zabezpieczone hasłem).
3. Dokumentacja papierowa musi być odpowiednio zabezpieczona na czas transportu. Należy zamknąć ją np. teczce, plecaku lub opakowaniach do tego przeznaczonych. Pracownik przewożący dokumenty zobowiązany jest do zabezpieczenia ich przed zagubieniem, kradzieżą, zniszczeniem, dekompletacją.
4. W sytuacji przekazywania nośników z danymi osobowymi poza obszar Instytutu zaleca się stosowanie następujących zasad bezpieczeństwa:
   a. adresat powinien zostać powiadomiony o przesyłce,
   b. dane przed wysłaniem powinny zostać zaszyfrowane a hasło podane adresatowi inną drogą.

6 Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane bez zgody pracownika Działu Informatyki.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub treści zakazane przez prawo.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty elektronicznej). Dotyczy to w szczególności stron, gdzie podajemy loginy, hasła, PIN-y, numery kart płatniczych.
6. W czasie, gdy komputer użytkownika podłączony jest do infrastruktury informatycznej Instytutu, zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo).

7 Zasady korzystania ze służbowej poczty elektronicznej

1. Adres e-mail tworzony jest wg następującego wzoru: imię.nazwisko@coi.pl lub nazwa stanowiska / działu@coi.pl.
2. Służbowa skrzynka pocztowa przeznaczona jest wyłącznie do korespondencji służbowej i działalności zawodowej.
3. Dostęp do skrzynki pocztowej odbywa się przez stronę https://email.coi.pl/ lub przez program pocztowy skonfigurowany na komputerze pracownika przez pracownika Działu Informatycznego.
4. Załączniki zawierające zbiory danych osobowych należy przesyłać w formie pliku zabezpieczonego hasłem. Instrukcja zabezpieczenia pliku hasłem znajduje się na wewnętrznej stronie Instytutu http://www.intranet.coi.pl/ w zakładce podstawowe-informacje/ochrona-danych-osobowych.

5. W przypadku skrzynek pocztowych wykorzystywanych do rejestracji pacjentów na wizyty, pracownik musi pamiętać o sprawdzaniu skrzynki pocztowej przynajmniej raz dziennie a po zarejestrowaniu i poinformowaniu pacjenta o terminie i godzinie wizyty niezwłocznie usunąć wiadomość od pacjenta z prośbą rejestracji na wizytę.
6. **WAŻNE:** Należy zachować szczególną ostrożność przy prowadzeniu korespondencji z osobami spoza kręgu "zaufanych nadawców". Nie wolno otwierać załączników w poczcie niewiadomego pochodzenia oraz "klikać" na hiperlinki (odnośniki do stron). Załączniki (a także strony internetowe) mogą zawierać szkodliwe oprogramowanie (szpiegujące, szyfrujące dane, blokujące komputer, itp.).
7. Użytkownicy poczty elektronicznej powinni zgłaszać do Działu Informatyki przypadki podejrzanych wiadomości.
8. Użytkownicy powinni okresowo kasować niepotrzebne wiadomości z poczty elektronicznej.
9. Przy korzystaniu z poczty elektronicznej, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
10. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie przyjętych zasad.

8 Zakres i uprawnienia kontrolne pracodawcy dotyczące służbowej korespondencji elektronicznej pracownika

1. E-maile wysłane z firmowej skrzynki pocztowej stanowią własność pracodawcy i pracodawca może je kontrolować.
2. Z uwagi na konieczność zapewnienia ochrony bezpieczeństwa i wizerunku Instytutu pracodawca zastrzega sobie prawo do wglądu we wszystkie wiadomości pracownika o charakterze służbowym (zarówno w skrzynce odbiorczej, jak i w wiadomościach wysłanych).
3. Kontrola służbowej korespondencji pracowników oraz ich poczty elektronicznej może nastąpić po wcześniejszym uprzedzeniu pracownika.
4. Pracodawca ma prawo kontroli przestrzegania przez pracownika zasad korzystania ze służbowej poczty elektronicznej określonych w niniejszym regulaminie.

9 Ochrona antywirusowa

1. Zabrania się podłączania do komputerów nośników danych (np. pendrive) pochodzących z niewiadomego źródła (znane są przypadki „podrzucania" użytkownikom zainfekowanych nośników).
2. Zakazane jest wyłączanie programu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów np. „Twój system jest zainfekowany", „Zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie pracownika Działu Informatyki lub kierownika komórki organizacyjnej / bezpośredniego przełożonego.

10 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba przetwarzająca dane osobowe zobowiązana jest do powiadomienia kierownika komórki organizacyjnej / bezpośredniego przełożonego w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych. Raport z incydentu naruszającego bezpieczeństwo danych osobowych ze względu na poufność, dostępność i integralność stanowi załącznik nr 1 do niniejszego regulaminu.
2. Do sytuacji wymagających powiadomienia kierownika komórki organizacyjnej / bezpośredniego przełożonego, należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek),
    d. zdarzenia losowe zewnętrzne (pożar obiektu / pomieszczenia, zalanie wodą),
    e. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, utrata / zagubienie danych),
    f. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych / sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów / danych, działanie wirusów).
3. Typowe przykłady incydentów wymagające reakcji:
    a. ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
    b. dokumentacja zawierająca dane osobowe jest niszczona bez użycia niszczarki,
    c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
    d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
    e. ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
    f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia kierownika komórki organizacyjnej / bezpośredniego przełożonego,
    g. udostępnienie danych osobowych osobom nieupoważnionym (w formie papierowej, elektronicznej i ustnej),
    h. telefoniczne próby wyłudzenia danych osobowych,
    i. kradzież, zagubienie komputerów lub płyt, twardych dysków, pendrive z danymi osobowymi,
    j. e-maile zachęcające do ujawnienia identyfikatora, hasła,
    k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputera,
    l. obecność haseł do systemów w pobliżu komputera.

11 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób upoważnionych do przetwarzania danych osobowych jest zobowiązana do:
    a. przetwarzania danych osobowych wyłącznie w zakresie i celach określonych przez kierownika komórki organizacyjnej / bezpośredniego przełożonego,

b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań,
c. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
d. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.

2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania Instytutu, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Instytut, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
5. Każda osoba przetwarzająca dane osobowe zobowiązana jest do zapoznania się z przepisami o ochronie danych osobowych, w tym z niniejszym regulaminem oraz zobowiązana jest do podpisania Oświadczenia (wzór oświadczenia stanowi załącznik nr 2 do niniejszego regulaminu).

12 Odpowiedzialność

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy. Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia powstania incydentu nie podjęła działań, a w szczególności nie powiadomiła kierownika komórki organizacyjnej / bezpośredniego przełożonego, możne zostać wszczęte postępowanie dyscyplinarne.
2. Za naruszenie ochrony danych osobowych pracownik (współpracownik) może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 kodeksu pracy albo odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego. Osoba upoważniona może także ponieść odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego.

RAPORT Z INCYDENTU NARUSZAJĄCEGO BEZPIECZEŃSTWO DANYCH OSOBOWYCH ZE WZGLĘDU NA POUFNOŚĆ, DOSTĘPNOŚĆ I INTEGRALNOŚĆ

Sporządzający raport:

.....

imię i nazwisko, stanowisko (funkcja)

Komórka organizacyjna:

.....

1) Rodzaj lub sposób naruszenia ochrony danych:

.....

.....

2) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

.....

.....

3) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

.....

.....

4) Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych (świadkowie):

.....

.....

5) Informacje o danych, które zostały lub mogły zostać ujawnione:

.....

.....

6) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

.....

.....

7) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korekcyjne, korygujące, zapobiegawcze):

.....

.....

.....

Data i podpis osoby sporządzającej raport

Załącznik Nr 2 do
Regulaminu Ochrony Danych Osobowych
w Centrum Onkologii - Instytucie
im. Marii Skłodowskiej-Curie w Warszawie

.....

(imię i nazwisko)

Oświadczenie

Oświadczam, że zapoznałem się z Regulaminem Ochrony Danych Osobowych w Centrum Onkologii – Instytucie im. Marii Skłodowskiej-Curie w Warszawie.

Oświadczam, że zobowiązuję się przestrzegać zasad i przepisów z zakresu ochrony danych osobowych podczas wykonywania obowiązków służbowych, w tym zobowiązuję się do:

1. przetwarzania danych osobowych wyłącznie w celu i zakresie przewidzianym w powierzonych mi zadaniach
2. przetwarzania danych osobowych zgodnie z obowiązującymi w tym zakresie przepisami prawa i regulacjami wewnętrznymi, w szczególności do zabezpieczenia przetwarzanych danych przed ich:
    a) udostępnieniem osobom nieupoważnionym,
    b) zabraniem przez osobę nieuprawnioną,
    c) przetwarzaniem z naruszeniem przepisów prawa,
    d) nieuprawnioną zmianą lub zniszczeniem,
    e) utratą,
    f) uszkodzeniem.
3. do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia.

.....

(data i podpis składającego oświadczenie)

Oświadczenie zostało złożone w obecności pracownika: