Wzór „Karty szkolenia w zakresie ochrony danych osobowych" – formularz przeznaczony dla osób przetwarzających medyczne dane osobowe

1/ Podstawa prawna przetwarzania medycznych danych osobowych – główne pozycje:

- ***Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)**, **zwanego w dalszej części „RODO"***
- ***Ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych Dz.U.2018.1000 z dnia 2018.05.24***
- ***Ustawa z dnia 15 kwietnia 2011 roku o działalności leczniczej Dz.U.2018.160 t.j. z dnia 2018.01.19***
- ***Ustawa z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta Dz.U.2017.1318 t.j. z dnia 2017.07.04***
- ***Ustawa z dnia 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych Dz.U.2017.1938 t.j. z dnia 2017.10.19***
- ***Ustawa z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia Dz.U.2017.1845 t.j. z dnia 2017.10.05***
- ***Ustawa z dnia 5 grudnia 1996 roku o zawodach lekarza i lekarza dentysty Dz.U.2018.617 t.j. z dnia 2018.03.26***
- ***Ustawa z dnia 15 lipca 2011 roku o zawodach pielęgniarki i położnej***

  Dz.U.2018.123 t.j. z dnia 2018.01.16
- ***Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 roku w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania Dz.U.2020.666 z dnia 2020.04.14***
- ***Rozporządzenie Ministra Zdrowia z dnia 20 czerwca 2008 roku w sprawie zakresu niezbędnych informacji gromadzonych przez świadczeniodawców, szczegółowego sposobu rejestrowania tych informacji oraz ich przekazywania podmiotom zobowiązanym do finansowania świadczeń ze środków publicznych Dz.U.2016.192 t.j. z dnia 2016.02.17***

2/ „Regulamin Przetwarzania i Ochrony Danych Osobowych" i „Procedury dotyczące stosowania Regulaminu Przetwarzania i Ochrony Danych Osobowych"

Na podstawie przepisów art. 24 ***Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)***, zwanego w dalszej części ***„RODO"*** – Dyrektor Szpitala Specjalistycznego w Brzozowie Podkarpackiego Ośrodka Onkologicznego im. Ks. Bronisława Markiewicza zarządzeniem Nr 65/2018 z dnia 25 maja 2018 roku wprowadził do stosowania ***„Regulamin przetwarzania i ochrony danych osobowych"*** **wraz z procedurami dotyczącymi stosowania tego Regulaminu,** które określają zasady i procedury obowiązujące przy przetwarzaniu danych osobowych we wszystkich zbiorach danych osobowych administrowanych przez Szpital Specjalistyczny w Brzozowie. Regulamin wraz z procedurami stanowi zbiór ogólnych i szczegółowych zasad postępowania, których przestrzeganie jest niezbędne do zapewnienia bezpiecznego przetwarzania danych osobowych. Jednocześnie regulacja ta będzie ulegać ciągłej modyfikacji, z uwagi na konieczność dostosowania zapisów w niej zawartych do stanu rzeczywistego oraz do zmieniających się przepisów prawa. Regulamin przetwarzania i ochrony danych

osobowych oraz wszelka dokumentacja dotycząca przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie dostępna jest dla wszystkich pracowników Szpitala – w formacie PDF – na stronie internetowej Szpitala pod adresem: **http://www.szpital-brzozow.pl/** w zakładce „Strefa Pracownika".

Zawartość tej zakładki mogą przeglądać wszystkie osoby przetwarzające dane osobowe na potrzeby Szpitala po zalogowaniu się i wpisaniu odpowiedniego hasła. Zawartość tej zakładki podlega ochronie – treści tam zawarte objęte są tajemnicą przedsiębiorstwa i przeznaczone są wyłącznie dla Pracowników Szpitala Specjalistycznego w Brzozowie oraz osób wykonujących na rzecz Szpitala pracę na podstawie zawartej ze Szpitalem umowy cywilnoprawnej.

3/ Szkolenie w zakresie ochrony danych osobowych

Osoby dopuszczone do przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie podlegają obowiązkowemu przeszkoleniu w tym zakresie – szkolenie obejmuje w szczególności treść obowiązujących przepisów dotyczących ochrony danych osobowych oraz wewnętrzne uregulowania. Nowo przyjmowani pracownicy, a także stażyści, studenci i wolontariusze podlegają obowiązkowemu przeszkoleniu przez Inspektora Ochrony Danych przed dopuszczeniem do przetwarzania danych osobowych. Po zakończeniu szkolenia osoby przeszkolone podpisują stosowne Oświadczenie (tzw. *„Klauzulę poufności"*) oraz potwierdzają odbycie szkolenia zgodnie z ***„Kartą szkolenia w zakresie ochrony danych osobowych".***

4/ Przetwarzanie danych

W Szpitalu Specjalistycznym w Brzozowie przetwarza się dane osobowe w następujących zbiorach danych osobowych:

- **dokumentacja dotycząca pacjentów i byłych pacjentów;**
- dokumentacja dotycząca **pracowników i byłych pracowników oraz członków ich rodzin**;
- dokumentacja dotycząca **kontrahentów** Szpitala;
- dokumentacja dotycząca **osób fizycznych będących stroną umów cywilnoprawnych** zawartych ze Szpitalem;
- dokumentacja dotycząca **kandydatów do pracy**;
- dokumentacja dotycząca **wolontariuszy, praktykantów i studentów**;
- dokumentacja dotycząca **nadawców i odbiorców korespondencji**;
- dokumentacja dotycząca **osób przyjmowanych do zakwaterowania do Hoteliku Szpitalnego (pacjenci i ich opiekunowie)**;
- dokumentacja dotycząca **osób fizycznych składających oferty w związku z postępowaniem prowadzonym w ramach zamówień publicznych**;
- dokumentacja dotycząca **wypadków przy pracy i w drodze do lub z pracy**;
- zbiór danych pochodzący z monitoringu wizyjnego;
- wykaz udostępnionej dokumentacji medycznej.

Bezpośredni nadzór nad przetwarzaniem danych osobowych sprawują **Administrator Danych Osobowych**, którym jest Szpital Specjalistyczny w Brzozowie, reprezentowany przez Dyrektora Szpitala, oraz wyznaczony przez niego **Inspektor Ochrony Danych**.
W przypadku danych osobowych przetwarzanych w systemach informatycznych, za bezpieczeństwo przetwarzania tych danych odpowiada **Administrator Systemów Informatycznych** oraz podlegli mu pracownicy Sekcji Obsługi i Konserwacji Urządzeń.

Wzór „Karty szkolenia w zakresie ochrony danych osobowych" – formularz przeznaczony dla osób przetwarzających medyczne dane osobowe

5/ Główne zadania Inspektora Ochrony Danych

1) informowanie Administratora Danych oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z tytułu przetwarzania danych osobowych i doradzanie im w tej sprawie;

2) monitorowanie przestrzegania przepisów dotyczących przetwarzania danych osobowych oraz polityk Administratora Danych w dziedzinie ochrony danych osobowych (działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty);

3) współpraca z organem nadzorczym, czyli z Prezesem Urzędu Ochrony Danych Osobowych oraz pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

6/ Ogólne pojęcia z zakresu przetwarzania danych osobowych

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

Wyróżniamy 2 kategorie danych osobowych:

1/ **dane osobowe zwykłe;**

2/ **szczególne kategorie danych osobowych**, w tym dane dotyczące zdrowia: wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. **Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej:** numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

Przetwarzanie danych osobowych oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak:

1/ zbieranie,

2/ utrwalanie,

3/ organizowanie,

4/ porządkowanie,

5/ przechowywanie,

6/ adaptowanie lub modyfikowanie,

7/ pobieranie,

8/ przeglądanie,

9/ wykorzystywanie,

10/ ujawnianie poprzez przesłanie,

11/ rozpowszechnianie lub innego rodzaju udostępnianie,

12/ dopasowywanie lub łączenie,

13/ ograniczanie,

14/ usuwanie

15/ niszczenie.

7/ Dane osobowe w ochronie zdrowia

Zgodnie z punktem 35 preambuły do rozporządzenia RODO za takie dane uważane są wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia konkretnej osoby. Do danych dotyczących zdrowia zaliczają się **także numery, symbole lub oznaczenia przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych, przy czym, chodzi tutaj o oznaczenia nadawane nie tylko podczas świadczenia usług opieki zdrowotnej, ale także rejestracji do tych usług. Tym samym unijny prawodawca wprowadził jednoznaczną zasadę, iż już na etapie rejestracji pacjenta, na przykład w poradni, jego dane osobowe, które są związane z udzielaniem świadczeń opieki zdrowotnej, zaliczane są do kategorii danych wrażliwych, podlegających szczególnej ochronie.**

W przypadku przetwarzania danych osobowych pacjenta, jeśli jest to niezbędne do realizacji celów zdrowotnych przetwarzania – nie jest wymagana zgoda pacjenta na przetwarzanie jego danych osobowych.

Zgoda pacjenta na przetwarzanie jego danych osobowych wymagana jest w następujących przypadkach:

1/ **dane osobowe przetwarzane będą w celach marketingowych** – za takie przetwarzanie danych nie uznaje się przetwarzania służącego bezpośrednio realizacji celów zdrowotnych;

2/ **dane osobowe przetwarzane będą w związku z realizacją badań klinicznych lub innych badań naukowych** – zgody pacjenta nie wymaga przetwarzanie danych na potrzeby udzielania świadczeń opieki zdrowotnej na rzecz pacjenta będącego uczestnikiem badania klinicznego (np. leczenie skutków działań niepożądanych, leczenie towarzyszące);

3/ nastąpi **przekazanie danych osobowych pacjenta do państwa trzeciego** – o ile Administrator danych nie posiada innej podstawy prawnej przetwarzania danych osobowych pacjenta.

8/ Przechowywanie zbiorów danych osobowych, dostęp do obszarów przetwarzania danych osobowych, procedura udostępniania danych oraz procedura niszczenia dokumentacji zbędnej zawierającej dane osobowe

1. Pomieszczenia, w których znajdują się przetwarzane zbiory danych osobowych muszą pozostawać zawsze pod bezpośrednim nadzorem upoważnionego do ich przetwarzania pracownika. Opuszczenie pomieszczenia, w którym znajdują się dane osobowe musi być zawsze poprzedzone odpowiednim ich zabezpieczeniem przed możliwością ingerencji przez osoby nieupoważnione do przetwarzania danych osobowych. **Przy planowanej dłuższej nieobecności pracownika pomieszczenie, w którym znajdują się dane osobowe musi być zamknięte na klucz.**

2. W Szpitalu Specjalistycznym w Brzozowie zainstalowane są systemy sygnalizujące włamania i pożary – systemy te zainstalowane są na Izbie Przyjęć Szpitala, serwerowni Szpitala, serwerowni Zakładu Radioterapii, Wentylatorni, w Zakładzie Radioterapii, Archiwum Szpitalnym, Kasie, Aptece Szpitalnej oraz w Dziale Organizacji, Nadzoru, Statystyki i Analiz Medycznych.

3. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy zobowiązani są do sprawdzenia stanu zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia. **W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, pracownik, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego przełożonego, który z kolei jest zobowiązany do niezwłocznego zawiadomienia Inspektora Ochrony Danych.**

Od momentu rozpoczęcia pracy do momentu jej zakończenia na pracownikach Szpitala spoczywa pełna odpowiedzialność za zabezpieczenie pomieszczeń Szpitala przed nieupoważnionym dostępem do tych pomieszczeń.

Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na:

- zabezpieczeniu dokumentacji i pieczęci służbowych;
- zabezpieczeniu komputerów i nośników informacji;
- wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
- zamknięciu okien i drzwi.

Klucze od biurek stanowiskowych i szaf biurowych są w posiadaniu pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

Duplikaty kluczy, będące kluczami zapasowymi do pomieszczeń administracyjnych są przechowywane w zamkniętej gablocie w gabinecie Kierownika Sekcji Gospodarczej.

Pracownik, któremu zostały powierzone klucze oraz kod cyfrowy do systemu alarmowego zobowiązany jest do:

- wykorzystywania ich zgodnie z przeznaczeniem;
- nie kopiowania oraz nie udostępniania osobom trzecim powierzonych kluczy – bez zgody

Dyrektora Szpitala;

- nie udostępniania kodu cyfrowego do systemu alarmowego osobom trzecim.

4. Dokumentacja zawierająca dane osobowe winna być archiwizowana w pomieszczeniach, w których systematycznie monitoruje się temperaturę i wilgotność powietrza – **w przypadku Szpitala Specjalistycznego w Brzozowie za prowadzenie archiwum dokumentacji odpowiedzialny jest Dział Organizacji, Nadzoru, Statystyki i Analiz Medycznych.**

5. Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie oraz w pełnej zgodności z przepisami prawa oraz wewnętrznymi procedurami.

Archiwalna dokumentacja medyczna zawierająca dane osobowe przechowywana jest w składnicy akt Szpitala Specjalistycznego w Brzozowie. Dokumentacja ta, zgodnie z obowiązującymi w tym zakresie przepisami, przechowywana jest przez wymagany okres czasu. Po upływie tego okresu dokumentacja podlega zniszczeniu, po uprzednim uzyskaniu zgody Archiwum Państwowego.

Dostęp do archiwalnej dokumentacji medycznej uzyskuje się za pośrednictwem pracowników Działu Organizacji, Nadzoru, Statystki i Analiz Medycznych w każdy dzień roboczy od poniedziałku do piątku w godzinach 7^{30}-8^{30} oraz 11^{00}-14^{00}, a w ostatni dzień roboczy miesiąca od godziny 7^{30} do godziny 12^{00}. W ostatni dzień roboczy danego roku udostępnianie archiwalnej dokumentacji medycznej następuje w godzinach od 7^{30} do 8^{30}.

Wydawanie dokumentacji medycznej do wykorzystania zawartych w niej danych w celach naukowych na indywidualne potrzeby lekarzy lub pielęgniarek odbywa się wyłącznie za pisemną zgodą Zastępcy Dyrektora ds. Lecznictwa, po wcześniejszym wydaniu opinii w tej sprawie przez Inspektora Ochrony Danych. Pod nieobecność Zastępcy Dyrektora ds. Lecznictwa, zgodę na wydanie tej dokumentacji może wydać również Administrator Danych.

W wypadku przekazywania dokumentacji papierowej należy każdorazowo uzyskać potwierdzenie odbioru z datą i podpisem osoby odbierającej (jeśli przekazujemy dokumentacje za pomocą poczty, to dopuszczalna jest tylko i wyłącznie forma „za potwierdzeniem odbioru").

9/ Dane medyczne przetwarzane w formie elektronicznej

Dane osobowe pacjentów Szpitala Specjalistycznego w Brzozowie przetwarzane są w ramach systemu „AMMS" firmy „ASSECO POLAND S.A." w następujących modułach (podzbiorach):

- „Apteka",
- „Apteczka Oddziałowa",
- „Laboratorium",
- „Gabinet",
- „Recepcja",
- „Rehabilitacja",
- „Statystyka",
- „Rozliczenia NFZ",
- „Patomorfologia",
- „Zakażenia",
- „Izba Przyjęć",
- „Oddziały Szpitalne",
- „Punkty Pobrań",
- „Pracownia".

Ponadto, Szpital Specjalistyczny w Brzozowie wykorzystuje oprogramowanie umożliwiające pracę różnych urządzeń służących do wysokospecjalistycznej diagnostyki pacjentów (oprogramowanie

wewnętrzne urządzeń) – aparatów USG, RTG, bronchoskopów, tomografów komputerowych, akceleratorów, mammografów, rezonansu magnetycznego i innych – w której przetwarza się dane osobowe pacjentów. Ma to zastosowanie w szczególności do takich komórek organizacyjnych Szpitala jak: Zakład Radioterapii, Zakład Brachyterapii, Zakład Radiologii i Diagnostyki Obrazowej, Zakład Fizyki Medycznej, Pracownia Rezonansu Magnetycznego, Pracownia Tomografii Komputerowej, Pracownia USG, Pracownia Mammografii, Laboratorium Mikrobiologiczne, Pracownia Endoskopii.

Dane osobowe pacjentów i personelu medycznego Szpitala w postaci elektronicznej przetwarzane są również w następujących portalach internetowych:

- aplikacja „Krajowy Rejestr Nowotworów",
- aplikacja „Obsługa Karty DILO",
- aplikacja „Kolejki Centralne",
- aplikacja „System Informatyczny Monitorowania Profilaktyki" (SIMP),
- portal „Świadczeniodawcy".

Dokumentacja medyczna zawiera następujące dane osobowe: identyfikator pacjenta; nazwisko; imiona; data urodzenia; miejsce urodzenia; płeć; numer PESEL; seria i numer dowodu osobistego; dane o ubezpieczeniu zdrowotnym; stały adres zamieszkania; tymczasowy adres zamieszkania; dane osobowe opiekuna (nazwisko i imię, adres zamieszkania, numer telefonu); grupa krwi; **dane osób upoważnionych do otrzymywania informacji o stanie zdrowia pacjenta** (nazwisko i imię, adres zamieszkania, numer telefonu); **dane osób upoważnionych do uzyskania dokumentacji medycznej** (nazwisko i imię, adres zamieszkania, numer telefonu).

Ponadto, w ramach dokumentacji medycznej gromadzone są następujące dane osobowe (dane medyczne):

dane o hospitalizacjach pacjenta: identyfikator opieki, data przyjęcia, tryb przyjęcia, rok i numer księgi głównej, identyfikator jednostki organizacyjnej, rok i numer księgi wypisu, tryb wypisu, data zakończenia opieki;
dane o pobytach pacjenta: identyfikator pobytu, identyfikator opieki, identyfikator pacjenta, rok i numer księgi głównej, data początku pobytu, data zakończenia pobytu, status pobytu, identyfikator lekarza przyjmującego, identyfikator lekarza dokonującego wypisu, identyfikator jednostki organizacyjnej;
dane o opiekach pacjenta: identyfikator opieki, identyfikator pacjenta, identyfikator jednostki kierującej, identyfikator lekarza kierującego;
dane o rozpoznaniach: identyfikator pobytu, identyfikator opieki, identyfikator pacjenta, rodzaj rozpoznania, data i godzina rozpoznania, identyfikator rozpoznania, lekarz dokonujący rozpoznania;
dane o zleceniach dla pacjenta: identyfikator pobytu, identyfikator opieki, identyfikator pacjenta, identyfikator lekarza zlecającego, data i godzina zlecenia, kod zleconego elementu leczenia/leku;
dane o podanych lekach: identyfikator pobytu, identyfikator opieki, identyfikator pacjenta, identyfikator lekarza zlecającego, identyfikator podanego leku, data i godzina początku podawania leku, data i godzina zakończenia podawania leku, dawka, częstotliwość podawania;
dane o udzielonych procedurach medycznych: identyfikator pobytu, identyfikator opieki, identyfikator pacjenta, data i godzina rozpoczęcia procedury, data i godzina zakończenia procedury, identyfikator lekarza zlecającego, kod procedury, wynik.

10/ Osoby upoważnione do przetwarzania danych osobowych i dostęp do danych osobowych w systemach informatycznych

Do przetwarzania danych osobowych w Szpitalu Specjalistycznym w Brzozowie upoważnione są jedynie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych, wydane przez Administratora Danych – upoważnienia te wydawane są zgodnie z zasadą wiedzy koniecznej.

Inspektor Ochrony Danych prowadzi elektroniczny rejestr upoważnień.

Wzór „Karty szkolenia w zakresie ochrony danych osobowych" – formularz przeznaczony dla osób przetwarzających medyczne dane osobowe

Upoważnienia do przetwarzania danych osobowych wydawane są na okres wykonywania pracy w Szpitalu Specjalistycznym w Brzozowie. W przypadku praktykantów, stażystów i wolontariuszy upoważnienia do przetwarzania danych osobowych wydawane są na okres trwania stażu, praktyki lub wolontariatu. Po zakończeniu okresu, na który zostało wydane upoważnienie, traci ono moc, co jest odnotowane w rejestrze upoważnień.
Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu **identyfikatora (loginu)** i właściwego **hasła**. **Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi, który odpowiedzialny jest za wszystkie czynności wykonane przy użyciu identyfikatora.**

Inspektor Ochrony Danych przydziela każdemu użytkownikowi systemu informatycznego indywidualne hasło dostępu oraz osobisty identyfikator. Hasło dostępu poszczególnego użytkownika podlega zmianie nie rzadziej niż raz na miesiąc. **Zmiana hasła dokonywana jest samodzielnie przez użytkownika systemu, przy czym hasło powinno zapewniać odpowiedni stopień bezpieczeństwa – winno składać się z ośmiu znaków alfanumerycznych oraz znaków specjalnych.** Identyfikator każdego użytkownika zostaje wpisany do ewidencji pracowników upoważnionych do przetwarzania danych osobowych wraz z imieniem i nazwiskiem użytkownika oraz podlega rejestracji w systemie informatycznym. Identyfikator ten nie podlega zmianie, a po wyrejestrowani użytkownika z systemu informatycznego nie może być przydzielony innej osobie.
Użytkownik systemu informatycznego nie może udostępniać innym osobom własnego hasła i identyfikatora w celu uzyskania dostępu do systemu informatycznego – podczas nadawania uprawnień do pracy w systemie informatycznym osoba, której będą nadane stosowne uprawnienia podpisuje klauzulę o następującej treści:

„Zobowiązuję się do zachowania w tajemnicy i nie udostępniania osobom trzecim kodu identyfikacyjnego (loginu) oraz hasła, a także zobowiązuję się do zmiany indywidualnego hasła startowego podczas pierwszego logowania i kolejnych zmian hasła nie rzadziej niż raz w miesiącu.
Równocześnie wyrażam zgodę na to, iż wszystkie działania w systemie informatycznym Szpitala Specjalistycznego w Brzozowie wykonane przez użytkownika o wskazanym kodzie identyfikacyjnym (loginie), będą przypisane mojej osobie ***i w przypadku stwierdzenia udostępnienia tego loginu i hasła osobom trzecim, zostanie mi cofnięte uprawnienie do przetwarzania danych osobowych."***

11/ Procedura niszczenia materiałów zawierających dane osobowe

1/ W przypadku konieczności zniszczenia materiałów zawierających dane osobowe (dokumentacja medyczna, dokumentacja pracownicza, wydruki z systemów informatycznych, wyniki badań, płyty DVD, płyty CD, dokumentacja zbiorcza etc.) każda osoba będąca w posiadaniu takich materiałów zobowiązana jest do ich przekazywania osobie wyznaczonej przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów.

Zabrania się wynoszenia poza teren Szpitala wszelkich materiałów zawierających dane osobowe.

2/ Materiały powyższe muszą być przechowywane w obrębie danej komórki organizacyjnej oraz w odpowiedni sposób zabezpieczone.

3/ Po zebraniu odpowiedniej ilości tych materiałów (stosownie do możliwości przechowywania tych materiałów przez każdą komórkę organizacyjną Szpitala) osoba wyznaczona przez kierownika danej komórki organizacyjnej do zabezpieczania tych materiałów zawiadamia telefonicznie Inspektora Ochrony Danych w Szpitalu Specjalistycznym w Brzozowie o konieczności zniszczenia materiałów zawierających dane osobowe.

4/ Inspektor Ochrony Danych – po konsultacji z Kierownikiem Sekcji Gospodarczej w Szpitalu

Specjalistycznym w Brzozowie – wyznacza termin odbioru materiałów przeznaczonych do zniszczenia.

5/ W przypadku stanowisk samodzielnych lub jednoosobowych stanowisk pracy – osoby zajmujące te stanowiska osobiście przedkładają do zniszczenia zbędne materiały zawierające dane osobowe.

6/ W przypadku fizycznej likwidacji urządzeń przetwarzających dane osobowe proces kasacji zostaje przeprowadzony przez Administratora Systemów Informatycznych w obecności osoby zlecającej kasację.

12/ Wystąpienie zagrożeń bezpieczeństwa danych osobowych oraz incydentów zagrażających bezpieczeństwu danych osobowych oraz procedury zabezpieczające

Zagrożenie bezpieczeństwa danych osobowych i incydenty zagrażające bezpieczeństwu danych

- **zagrożenia bezpieczeństwa danych** oznaczają wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
- **incydent** oznacza takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
- **naruszenie ochrony danych osobowych** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Do **typowych zagrożeń bezpieczeństwa danych** osobowych należy nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

Do **typowych incydentów zagrażających bezpieczeństwu danych** osobowych należą:

zdarzenia losowe:
pożar, zalanie, awarie serwera, awarie
komputerów, twardych dysków, oprogramowania, pomyłki informatyków,
użytkowników systemu informatycznego, utrata lub zagubienie danych;
umyślne incydenty:
włamanie do systemu informatycznego lub pomieszczeń, kradzież danych lub sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wir usów i innego szkodliwego oprogramowania

1/ Każdy osoba biorąca udział w przetwarzaniu danych osobowych jest odpowiedzialna za bezpieczeństwo tych danych. **W szczególności osoba, która zauważyła zdarzenie mogące być przyczyną naruszenia ochrony danych osobowych lub mogące spowodować naruszenie bezpieczeństwa danych, zobowiązana jest do natychmiastowego poinformowania Inspektora Ochrony Danych.**

2/ W przypadku stwierdzenia naruszenia bezpieczeństwa danych, Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające, w toku którego:

- ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
- zabezpiecza ewentualne dowody;
- ustala osoby odpowiedzialne za naruszenie;

- podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
- inicjuje działania dyscyplinarne;
- wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
- dokumentuje czynności podjęte w prowadzonym postępowaniu.

O naruszeniu ochrony danych osobowych w systemach informatycznych Szpitala mogą świadczyć następujące symptomy:

- brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych;
- brak możliwości zalogowania się do tej aplikacji;
- ograniczone, w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (na przykład brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
- wygląd aplikacji inny niż normalnie;
- inny zakres danych niż normalnie dostępny dla użytkownika – dużo więcej lub dużo mniej danych;
- znaczne spowolnienie działania systemu informatycznego;
- pojawienie się niestandardowych komunikatów generowanych przez system informatyczny;
- ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
- ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopii zapasowych;
- włamanie lub próby włamania do szafek, w których przechowywane są – w postaci elektronicznej lub papierowej – nośniki danych osobowych;
- zagubienie bądź kradzież nośnika danych osobowych;
- kradzież sprzętu informatycznego, w którym przechowywane są dane osobowe;
- informacja z systemu antywirusowego o zainfekowaniu systemu;
- fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej;
- podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.

W przypadku wystąpienia powyższych symptomów, jak również innych objawów, które mogą wskazywać na zagrożenie bezpieczeństwa danych osobowych, należy natychmiast powiadomić Inspektora Ochrony Danych.

Informacja o pojawieniu się zagrożenia jest przekazywana przez pracownika osobiście, telefonicznie lub pocztą elektroniczną. Taka informacja powinna zawierać imię i nazwisko osoby zgłaszającej oraz zauważone symptomy zagrożenia. W przypadku, gdy zgłoszenie o podejrzeniu incydentu otrzyma osoba inna niż Inspektor Ochrony Danych, jest ona zobowiązana poinformować o tym fakcie Inspektora Ochrony Danych.

Zasady pracy na służbowym sprzęcie komputerowym oraz zasady dostępu do sieci internetowej zostały określone w Zarządzeniu Nr 54/2011 Dyrektora Szpitala z dnia 10 maja 2011 roku wraz z jego aktualizacją – zgodnie z postanowieniami tego zarządzenia:

1/ na stacjach komputerowych pracują tylko osoby do tego upoważnione;

2/ komputer służbowy wykorzystywany jest tylko do celów służbowych;

3/ użytkownik komputera służbowego ponosi pełną odpowiedzialność za powierzony sprzęt komputerowy i zainstalowane oprogramowanie;

4/ użytkownik komputera służbowego ma obowiązek poinformować pracownika Sekcji Obsługi i Konserwacji Urządzeń o wszystkich uszkodzeniach sprzętu systemu w momencie ich zauważenia, oraz o komunikatach informujących o obecności wirusów;

5/ użytkownikowi komputera służbowego zabrania się:

- pobierania pakietów instalacyjnych oprogramowania oraz instalowania ich na dysku komputera;
- dokonywania zmian w konfiguracji istniejącego oprogramowania;
- łamania zabezpieczeń systemu i łamania haseł;
- udostępniania loginu i hasła osobom trzecim;
- używania stanowisk komputerowych w celach zarobkowych czy komercyjnych;
- wykonywania czynności naruszających prawa autorskie twórców lub dystrybutorów oprogramowania i danych;
- wyszukiwania i prezentowania materiałów o treści obrażającej uczucia innych;
- naruszania praw autorskich i licencyjnych;
- otwierania stron dotyczących przemocy, pornografii itp.;
- korzystania z gier komputerowych, serwerów CHAT, IRC i innych komunikatorów internetowych;
- wchodzenia na strony zawierające pirackie oprogramowanie;
- pobierania plików z sieci i zapisywania ich na nośnikach przenośnych;
- podłączania do szpitalnej sieci internetowej komputerów prywatnych oraz podłączania do komputera nośników prywatnych (pendrivów, płyt CD itp.);
- kopiowania danych osobowych na jakiekolwiek nośniki informacji;
- udostępniania sprzętu komputerowego osobom nieupoważnionym.

Ponadto w obowiązującym w Szpitalu Specjalistycznym w Brzozowie ***„Regulaminie przetwarzania i ochrony danych osobowych"*** zapisano między innymi:

„W przypadku pracowników Szpitala, oraz osób wykonujących na jego rzecz pracę w oparciu o umowy cywilnoprawne i kontraktowe, możliwy jest – ***w wyjątkowych, indywidualnych przypadkach*** *– dostęp do sieci lokalnej LAN oraz do sieci rozległej WAN poprzez prywatny komputer przenośny. W tej sytuacji o dostępie do sieci – w przypadku pracowników Szpitala – decyduje Administrator Danych Osobowych, który, na wniosek bezpośredniego przełożonego pracownika, skierowany do Administratora, udziela – po konsultacji z Inspektorem Ochrony Danych oraz Kierownikiem Sekcji Obsługi i Konserwacji Urządzeń – indywidualnej zgody na dostęp do szpitalnej sieci internetowej. W przypadku osób zajmujących kierownicze stanowiska w Szpitalu (zastępcy dyrektora Szpitala, ordynatorzy, kierownicy komórek organizacyjnych) oraz pracowników zatrudnionych na samodzielnych stanowiskach pracowniczych wniosek do Administratora Danych Osobowych składany jest przez te osoby.*

Przed udzieleniem zgody na podłączenie komputera do sieci musi się odbyć dokładne sprawdzenie czy komputer prywatny spełnia podstawowe wymogi podłączenia do sieci informatycznej, tzn. czy posiada odpowiednie zabezpieczenia antywirusowe i inne.
Minimalne środki ochrony to: zainstalowane systemy typu firewall oraz antywirus, wdrożony system aktualizacji systemu operacyjnego oraz jego składników, wymaganie podania hasła przed uzyskaniem dostępu do pracy na komputerze, niepozostawianie niezablokowanych stacji bez nadzoru, bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

Po pozytywnym rozpatrzeniu wniosku przez Administratora Danych Osobowych, wniosek ten przekazany zostaje Kierownikowi Sekcji Obsługi i Konserwacji Urządzeń, który kontaktuje się z osobą, której dotyczy wniosek i uzyskuje od niej niezbędny do nadania uprawnień adres fizyczny karty sieciowej, zainstalowanej w komputerze przenośnym.

Przetwarzanie danych osobowych na komputerach przenośnych powinno być ograniczone do niezbędnych przypadków. Przetwarzanie tych danych może odbywać się wyłącznie za zgodą Administratora Danych Osobowych oraz za wiedzą Inspektora Ochrony Danych.

Wzór „Karty szkolenia w zakresie ochrony danych osobowych" – formularz przeznaczony dla osób przetwarzających medyczne dane osobowe

Zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzania danych ustala przełożony pracownika, za wiedzą Inspektora Ochrony Danych. W przypadku osób wykonujących pracę na rzecz Szpitala w oparciu o umowę cywilnoprawną lub umowę kontraktową, zakres danych przetwarzanych na komputerze przenośnym oraz zakres uprawnień do przetwarzania danych ustala Administrator Danych Osobowych.

Osoba korzystająca z komputera przenośnego w celu przetwarzania danych osobowych, zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.

Użytkownik komputera przenośnego zobowiązany jest do:

- *transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności: transportowania komputera w bagażu podręcznym, nie pozostawiania komputera w samochodzie, przechowalni bagażu itp.;*

- *korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego;*

- *nie zezwalania osobom nieupoważnionym do korzystania z komputera przenośnego, na którym przetwarzane są dane osobowe;*

- *zabezpieczania komputera przenośnego hasłem;*

- *blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez pracownika;*

- *kopiowania danych osobowych przetwarzanych na komputerze przenośnym do systemu informatycznego w celu umożliwienia wykonania kopii awaryjnej tych danych;*

- *umożliwienia, poprzez podłączenie komputera do sieci informatycznej Szpitala Specjalistycznego w Brzozowie, aktualizacji wzorców wirusów w programie antywirusowym;*

- *utrzymanie konfiguracji oprogramowania systemowego w sposób wymuszający korzystanie z haseł;*

- *wykorzystywanie haseł o odpowiedniej jakości, zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe;*

- *zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe.*

W razie zgubienia lub kradzieży komputera przenośnego pracownik zobowiązany jest do natychmiastowego powiadomienia Administratora Danych Osobowych i Inspektora Ochrony Danych, zgodnie z zasadami informowania o naruszeniu ochrony danych osobowych.

Użytkownicy systemu informatycznego są zobowiązani do bezwzględnego przestrzegania następującej procedury rozpoczęcia, prowadzenia i zakończenia pracy w systemie informatycznym:

- **rozpoczynając pracę przy komputerze użytkownik loguje się do systemu poprzez wprowadzenie wymaganych identyfikatorów i haseł w sposób uniemożliwiający ich ujawnienie osobom trzecim;**

- w przypadku jakiejkolwiek przerwy w pracy w systemie informatycznym i opuszczenia stanowiska pracy użytkownik jest zobowiązany do wylogowania się z systemu bądź

zablokowania stacji roboczej;

- użytkownik jest zobowiązany do korzystania z systemu informatycznego w sposób uniemożliwiający osobom nieuprawnionym zapoznanie się z danymi osobowymi;

- **po zakończeniu pracy w systemie informatycznym użytkownik jest zobowiązany do zamknięcia aplikacji, wylogowania się z systemu oraz wyłączenia komputera;**

- **w celu przesłania w postaci elektronicznej (e-mail) komunikatów służbowych zawierających dane osobowe należy korzystać wyłącznie ze służbowych skrzynek pocztowych; wiadomość zawierającą dane osobowe należy przed wysłaniem zaszyfrować za pomocą programu 7-zip i zaopatrzyć w odpowiedni klucz (hasło); zaszyfrowaną wiadomość można wysłać jedynie za pomocą służbowej skrzynki pocztowej, natomiast klucz do odszyfrowania wiadomości należy przekazać adresatowi wiadomości telefonicznie; z uwagi na wysokie niebezpieczeństwo związane z tego typu operacjami zaleca się aby czynności te wykonywane były pod bezpośrednim nadzorem pracownika Sekcji Obsługi i Konserwacji Urządzeń;**

- **niedozwolone jest – bez powiadomienia o tym fakcie Administratora Danych Osobowych i Inspektora Ochrony Danych – zapisywanie czy kopiowanie na nośniki zewnętrzne informacji zawierających dane osobowe."**

Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia w Szpitalu naruszenia bezpieczeństwa danych osobowych Inspektor Ochrony Danych, we współpracy z Kierownikiem Sekcji Obsługi i Konserwacji Urządzeń, jest zobowiązany do podjęcia kroków w celu:

- wyjaśnienia zdarzenia, a w szczególności czy miało miejsce naruszenie ochrony danych osobowych;
- wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów, a w szczególności, gdy zdarzenie było związane z celowym działaniem pracownika bądź osób trzecich;
- zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia;
- usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu).

Inspektor Ochrony Danych określa w formie raportu, na podstawie zebranych informacji, przyczyny zaistnienia incydentu. Jeżeli incydent był spowodowany celowym działaniem, jest on zobowiązany do pisemnego powiadomienia Administratora Danych, który może poinformować organy uprawnione do ścigania przestępstw o fakcie celowego naruszenia bezpieczeństwa danych osobowych.

Inspektor Ochrony Danych prowadzi ewidencję interwencji związanej z zaistniałymi incydentami w zakresie bezpieczeństwa danych osobowych. Ewidencja taka obejmuje następujące informacje:

- imię i nazwisko osoby zgłaszającej incydent;
- imię i nazwisko osoby przyjmującej zgłoszenie incydentu;
- datę zgłoszenia incydentu;
- przeprowadzone działania wyjaśniające przyczyny zaistnienia incydentu;
- wyniki przeprowadzonych działań;
- podjęte akcje naprawcze i ich skuteczność.

13/ Odpowiedzialność

1. Za przestrzeganie zasad dotyczących bezpieczeństwa przetwarzania danych osobowych, odpowiedzialni są wszyscy pracownicy Szpitala oraz osoby wykonujące na jego rzecz pracę w oparciu o umowy cywilnoprawne oraz umowy kontraktowe.

2. W przypadku pracowników Szpitala, których zakres obowiązków pracowniczych nie obejmuje konieczności przetwarzania danych osobowych, a które z racji tych obowiązków mogą mieć dostęp do pomieszczeń, w których przetwarza się dane osobowe – pracownicy Sekcji Gospodarczej, Sekcji Higieny Szpitalnej, Sekcji Technicznej, Kuchni i Pralni – nałożono obowiązek pisemnego oświadczenia zawierającego klauzulę zobowiązującą do zachowania w tajemnicy, nieujawniania i niewykorzystywania wszelkich informacji, z którymi zapoznali się z racji wykonywanych obowiązków, w szczególności dotyczących danych osobowych.

3. Osoby przetwarzające dane osobowe zobowiązane są do stosowania postanowień dotyczących zasad przetwarzania danych osobowych. **Przypadki, nieuzasadnionego zaniechania obowiązków pracowniczych w powyższym zakresie potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.**

Wobec osoby, która w przypadku naruszenia bezpieczeństwa przetwarzania danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła określonego działania, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi procedurami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

Kara dyscyplinarna nie wyklucza odpowiedzialności karnej tej osoby zgodnie z odpowiednimi przepisami, oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.