# POLITYKA BEZPIECZEŃSTWA INFORMACJI

## I OCHRONY DANYCH OSOBOWYCH

## QP-ZI-2

w Wojewódzkim Szpitalu Specjalistycznym Nr 2 w Jastrzębiu-Zdroju



WYDANIE: **3**

| STANOWISKO/KOMÓRKA ORGANIZACYJNA | | Data |
|---|---|---|
| Opracował: | **INSPEKTOR OCHRONY DANYCH OSOBOWYCH**<br>inż. Marcelina Twardowska | **01.02.2019** |
| Sprawdził: | **RADCA PRAWNY**<br>mgr Katarzyna Ferenc | **04.02.2019** |
| Zapoznał: | **ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH**<br>inż. Szymon Jurkiewicz | **04.02.2019** |
| Zapoznał | **PEŁNOMOCNIK DS. JAKOŚCI**<br>mgr Agnieszka Gilga | **04.02.2019** |
| Zatwierdził: | **DYREKTOR**<br>mgr Robert Rychel | **05.02.2019** |

**JASTRZĘBIE-ZDRÓJ luty 2019**

## SPIS TREŚCI

## I. WSTĘP

1. Wojewódzki Szpital Specjalistyczny w Jastrzębiu-Zdroju jest Administratorem Danych Osobowych w rozumieniu przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 94/46/WE (ogólne rozporządzenie o ochronie danych). Dyrektor Naczelny jest zobowiązany do podejmowania wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom związanym z przetwarzaniem danych osobowych wdrażając odpowiednie środki techniczne i organizacyjne, aby zapewnić:

1.1 Zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.

1.2 Zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.

1.3 Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

1.4 Pseudonimizację i szyfrowanie danych osobowych.

## II. POSTANOWIENIA OGÓLNE

### 1. Cel i zakres wdrożenia polityki bezpieczeństwa

1.1. Wdrożenie polityki bezpieczeństwa ma na celu wskazanie pracownikom WSS Nr 2 w jaki sposób bezpiecznie przetwarzać dane osobowe oraz usystematyzowanie zabezpieczeń przetwarzanych przez Wojewódzki Szpital Specjalistyczny Nr 2 danych osobowych.

1.2. Cele polityki bezpieczeństwa realizowane są poprzez zapewnienie danym osobowym następujących cech:

1) Poufności - właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom;
2) Integralności - właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) Rozliczalności - właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi

1.3. Szpital realizuje cele poprzez zabezpieczenia i ochronę danych dzięki zapewnieniu bezpieczeństwa fizycznego, tworzeniu procedur organizacyjnych, zagwarantowaniu oprogramowania systemowego oraz utrzymywaniu świadomości jego użytkowników.

1.4. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w WSzS Nr 2, niezależnie od formy ich przetwarzania (zbiory danych, systemy informatyczne, informacje zgromadzone w formie tradycyjnej-papierowej)

1.5. Polityka ma zastosowanie wobec wszystkich komórek organizacyjnych WSzS Nr 2.

1.6. Zasady określone przez niniejszy dokument mają zastosowanie do całego systemu przetwarzania danych, w tym do systemu informatycznego, a w szczególności do:

1) Wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz tradycyjnych, w których przetwarzane są lub będą informacje podlegające ochronie;
2) Informacji, których administratorem jest Szpital lub jednostki obsługiwane, o ile zostały przekazane do WSzS Nr 2 na podstawie umów lub porozumień;
3) Wszystkich nośników papierowych, magnetycznych lub optycznych, na których są lub będą znajdować się informacje podlegające ochronie;
4) Wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
5) Wszystkich osób upoważnionych do przetwarzania danych osobowych w Szpitalu.

1.7. Do spraw nieuregulowanych w Polityce stosuje się przepisy RODO oraz ustawy o ochronie danych osobowych.

1.8. Integralną częścią niniejszej polityki jest **Instrukcja Zarządzania Systemem Informatycznym**, która określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, podkreślający istotę zapewnienia ich bezpieczeństwa.

2. **Podstawowe Pojęcia**

2.1. Przez użyte w tym dokumencie określenia należy rozumieć:

1) **WSS Nr 2/ Szpital-** Wojewódzki Szpital Specjalistyczny w Jastrzębiu-Zdroju
2) **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Ochrony Danych Osobowych w Szpitalu;
3) **Instrukcja** – rozumie się przez to Instrukcję Zarządzania Systemem Informatycznym w Szpitalu;
4) **Administrator Danych Osobowych (ADO)** – Wojewódzki Szpital Specjalistyczny w Jastrzębiu-Zdroju reprezentowany przez Dyrektora Naczelnego Szpitala, decydujący o celach i środkach przetwarzania danych osobowych;
5) **Inspektor Ochrony Danych Osobowych (IODO)–** osoba wyznaczona przez Dyrektora Szpitala, odpowiedzialna za organizację i bezpieczeństwo danych osobowych;
6) **Administrator Systemu Informatycznego** (**ASI**) – osoba zatrudniona przez Dyrektora WSzS Nr 2, upoważniona do realizacji zadań związanych z zarządzaniem systemem informatycznym;
7) **Organ nadzorczy/ UODO –** Urząd Ochrony Danych Osobowych
8) **RODO-** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 94/46/WE (ogólne rozporządzenie o ochronie danych).
9) **Rozporządzenie** – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 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);
10) **Dane osobowe (dane)** – wszelkie informacje dotyczące zidentyfikowanej bądź możliwej do zidentyfikowania osoby fizycznej;
11) **Dane szczególnej kategorii**– rozumie się dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także informacje o innych orzeczeniach wydanych
12) **Użytkownik** – osoba posiadająca uprawnienia do pracy w systemie informatycznym oraz obsługi sprzętu wchodzącego w jego skład zgodnie z zakresem obowiązków służbowych;

13) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym;

14) **Pracownik** – osoba pozostająca w stosunku pracy z pracodawcą lub zatrudniona umowę cywilnoprawną na świadczenie usług;

15) **Naruszenie bezpieczeństwa systemu informatycznego** – jakiekolwiek naruszenie poufności, integralności, dostępności do systemu informatycznego spowodowane przez ludzi, jak też naruszenia powstałe na skutek oddziaływania sił przyrody, katastrof cywilizacyjnych itp.;

a) poufność danych- , informacja jest dostępna jedynie dla podmiotów do tego upoważnionych

b) integralności danych - wszelkie nieuprawnione modyfikacje informacji są niedozwolone;

c) dostępności danych - do informacji można uzyskać dostęp w każdych okolicznościach, które są dopuszczone przez politykę bezpieczeństwa informacji.

16) **Integralność danych –**właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

17) **Rozliczność** – właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

18) **Przetwarzanie danych** – wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, udostępnianie, opracowywanie, zmienianie, usuwanie;

19) **System informatyczny (system**) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

20) **Stacja robocza** – stacjonarne lub przenośne urządzenie wchodzące w skład systemu informatycznego umożliwiające użytkownikom systemu dostęp do danych osobowych znajdujących się w systemie;

21) **Osoba upoważniona** –osoba posiadająca podstawy prawne do przetwarzania danych osobowych (przede wszystkim osoby wykonujące zawód medyczny lub osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych i dopuszczona do przetwarzania danych w systemie informatycznym, zbiorach papierowych i/lub elektronicznych w zakresie niezbędnym do realizacji zadań.

## III. ORGANIZACJA – ROLE I ODPOWIEDZIALNOSCI

1. Za bezpieczeństwo informacji w zakresie przetwarzania danych osobowych odpowiedzialny jest **każdy pracownik pracujący w Szpitalu** w zakresie zajmowanego stanowiska i posiadanych informacji.

2. **Do obowiązków Kierowników komórek organizacyjnych** należy bezpośredni nadzór nad przetwarzaniem danych osobowych oraz:

2.1. Występowanie z wnioskiem do IODO i ASI o nadawanie upoważnień dotyczących dostępu do zasobu danych osobowych podległym pracownikom,

2.2. Dopilnowanie aby pracownicy w podległej komórce mający dostęp do danych osobowych postępowali zgodnie z przepisami dotyczącymi ochrony danych osobowych, polityką,

3. Obowiązkiem Kierownika komórki organizacyjnej jest dopilnowanie aby wszyscy jemu podlegli pracownicy mający dostęp do danych osobowych zostali przeszkoleni z tego zakresu oraz aby aktualizowali swoją wiedzę wykorzystując materiały dostarczane przez IODO

4. Kierownik komórki organizacyjnej może zwrócić się z wnioskiem o przeprowadzenie szkolenia podając ilość osób do przeszkolenia oraz ustalając wspólnie formę i termin przeprowadzenia szkolenia.

5. **Dyrektor** (**ADO**) decyduje o celach i środkach przetwarzania danych osobowych. Do obowiązków administratora należy:

5.1. Zrozumienie oraz zapewnienie świadomości bezpieczeństwa przetwarzania danych osobowych

5.2. Podział zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznaczenie IODO

5.3. Utworzenie oraz cykliczna aktualizacja rejestru czynności przetwarzania,

5.4. Dokonania oceny skutków dla ochrony danych.

5.5. Wprowadzenie do stosowania procedury zgłaszania incydentu naruszenia ochrony danych osobowych oraz prowadzenie rejestru incydentów

5.6. Zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu oraz osobie, której dane dotyczą

5.7. Poddawanie przeglądom skuteczności Polityki Bezpieczeństwa przetwarzania danych osobowych.

5.8. Przeprowadzanie audytów zewnętrznych z częstotliwością co najmniej raz na 2 lata.

5.9. Zapewnienie niezbędnych środków potrzebnych dla zapewnienia bezpieczeństwa przetwarzania danych osobowych.

5.10. Wprowadzenie do stosowania procedur zapewniających prawidłowe przetwarzanie danych osobowych.

6. Do **obowiązków IODO** należy nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej. Do obowiązków należy również:

6.1. Informowanie ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i doradzanie im w tej sprawie;

6.2. Monitorowanie przestrzegania RODO oraz niniejszej polityki

6.3. Zapoznawanie pracowników mających dostęp do danych osobowych z przepisami dotyczącymi ochrony danych osobowych.

6.4. Podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania.

6.5. Przeprowadzanie wewnętrznych audytów przestrzegania zasad ochrony danych osobowych.

6.6. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania.

6.7. Współpraca z organem nadzorczym w tym pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach prowadzenie konsultacji ( art. 36 RODO) we wszelkich sprawach.

6.8. IODO przeprowadza szkolenia dla każdej osoby, która w ramach wykonywania obowiązków służbowych przetwarza dane osobowe (szczególnie dla osoby nowo zatrudnionej)

6.9. IODO przynajmniej raz w roku przeprowadza lub zleca przeprowadzenie szkolenie z zakresu ochrony danych osobowych dla całego personelu.

7. **Obowiązki ASI** zostały określone w Instrukcji Zarządzania Systemami Informatycznymi.

8. Do **obowiązków każdego pracownika** przetwarzającego dane osobowe należy przestrzeganie zasad określonych w niniejszej polityce oraz stosowanie procedur zapewniających prawidłowe przetwarzanie danych osobowych.

## IV. NOWO ZATRUDNIONY PRACOWNIK – SPOSÓB POSTĘPOWANIA

1. Dane osobowe kandydatów na pracowników WSS Nr 2 na etapie rekrutacji pozyskiwane są za pośrednictwem dokumentów aplikacyjnych, w treści których znajduje się klauzula zgody na przetwarzanie danych osobowych na potrzeby bieżącej jak również i przyszłych rekrutacji.

2. Historię kandydatów do pracy należy zweryfikować zgodnie z odpowiednimi przepisami prawnymi, regulacjami i zasadami etycznymi. Niezbędna jest weryfikacja tożsamości, wykształcenia, referencji itp.

3. Nowo zatrudniony pracownik jest zobowiązany do uzupełnienia karty obiegowej.

4. W przypadku, gdy do realizacji wykonywanych przez pracownika obowiązków niezbędne jest przetwarzanie danych osobowych, konieczne jest:

4.1 Zapoznanie przez IODO z przepisami dotyczącymi ochrony danych osobowych. Weryfikacja wiedzy może odbyć się na podstawie testu.

4.2 Nadanie uprawnień w określonym zakresie na podstawie wniosku przełożonego skierowanego do IODO i ASI. Wniosek można pobrać w Dziale Personalnym lub w Dziale Informatyki.

4.3 Nadanie upoważnienia w przypadku osoby nie wykonującej czynności medycznych (wykonujące czynności pomocnicze np. pracownicy sekretariatów, rejestracji lub wykonujący czynności związane z utrzymaniem systemu informatycznego). Upoważnienie nadaje ADO.

4.4 Poinformowanie o postępowaniu dyscyplinarnym.

**5. Postępowanie dyscyplinarne może obejmować:**

5.1 **Odpowiedzialność porządkowa i dyscyplinarna** – upomnienie, nagana. W przypadku poważnego naruszenia podstawowych obowiązków pracowniczych, skutkiem może być rozwiązanie stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

5.2 **Odpowiedzialność materialna** - w przypadku, gdy nieprawidłowe przetwarzanie danych przez pracownika narazi ADO na szkodę np. wypłatę odszkodowania na rzecz osoby fizycznej, której prawa i wolności zostały naruszone właśnie na skutek niezgodnego z prawem i procedurami działania pracownika. Wówczas, jeśli bezprawność zachowania (wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych) i wina pracownika zostaną należycie wykazane, **pracownik może zostać pociągnięty do odpowiedzialności materialnej**.

5.3 **Odpowiedzialność karna** - w przypadku, gdy naruszenie miałoby charakter **umyślnego przestępstwa**, wówczas zastosowanie znajdują **przepisy karne** - art. 107 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (przykład: umyślne i celowe ujawnienie danych szczególnej kategorii)

6. Kierownik Działu Personalnego przekazuje ASI lub IODO raport dotyczący zmian personalnych (zatrudnienia, zakończenie pracy, przesunięcia na inne stanowisko) w celu umożliwienia kontroli nadanych uprawnień do systemu informatycznego.

# V. ZASADY BEZPIECZNEGO PRZETWARZANIA DANYCH OSOBOWYCH

## 1. OGÓLNE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

**1.1.** Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Oznacza to, że niedopuszczalne jest zbieranie danych „za zapas", przechowywanie ich dłużej niż to konieczne.

1.2. Przy pierwszym wejściu do obszaru przetwarzania (biuro, pomieszczenie archiwum, serwerownia, magazyn itp.) w danym dniu należy upewnić, się czy nie są widoczne ślady ingerencji osób trzecich, pożaru, zalania lub innego uszkodzenia (szczególnie Pracownik Archiwum)

1.3. Dokumentacja medyczna pacjentów jest oddawana do archiwum do 2 tygodni od wypisu pacjenta z oddziału. Dokumenty przekazywane są zgodnie z przepisami jakie dotyczą dokumentacji archiwalnej.

1.4. Dokumenty zawierające dane osobowe po ustaniu przydatności są deponowane w dedykowanych pojemnikach przeznaczonych do utylizacji dokumentów obsługiwanych przez firmę specjalizującą się w utylizacji dokumentów papierowych/nośników danych.

**1.5.** Wszyscy pracownicy WSS Nr 2 zobowiązani są do zachowania w tajemnicy informacji na temat danych osobowych pacjentów, współpracowników, zdarzeń niepożądanych oraz sposobów zabezpieczania informacji, systemów informatycznych. Zachowanie tajemnicy służbowej obowiązuje również wobec najbliższych. Obowiązek trwa także po ustaniu stosunku pracy. Nie przewiduje się czasowego ograniczenia tego obowiązku.

1.6. Wszelkiego typu dane osobowe (również dane medyczne) w formie papierowej oraz elektronicznej powinny być zabezpieczone przed utratą, kradzieżą lub nieuprawnionym dostępem. Dane osobowe zawarte w dokumentacji przetwarzane są przez osoby upoważnione zgodnie z zasadami niniejszej polityki

1.7. Niedopuszczalne jest powierzanie dokumentacji (w tym dokumentacji medycznej) osobie nieuprawnionej do tego (np. przekazywanie pacjentowi jego kartoteki, zobowiązanie nieuprawnionej osoby do dostarczenia dokumentów do innego pomieszczenia itp.). Należy się kierować regułą ograniczonego zaufania.

1.8. Zabezpieczenia opisane w polityce są informacją przeznaczoną wyłącznie dla pracowników Szpitala.

## 2. ZASADY BEZPIECZNEGO UŻYTKOWANIA SYSTEMÓW INFORMATY CZNYCH

2.1. Środki do przetwarzania informacji wykorzystywane w WSzS Nr 2 są przeznaczone wyłącznie do wykonywania zadań służbowych. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.

2.2. Każdy użytkownik ma w systemie unikalny identyfikator zatem ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła

2.3. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika.

2.4. Zabronione jest:

1) Udzielanie informacji o zasadach ochrony systemów teleinformatycznych Szpitala, w tym o identyfikatorach używanych w tych systemach,
2) Umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
3) Udostępnianie danych osobom nieupoważnionym,
4) Rejestrowanie się w systemie na identyfikatorze innego użytkownika,
5) Przenoszenie informacji uzyskanych w związku z wykonywanymi zadaniami służbowymi na prywatne nośniki informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne (chyba, że jest na to zgoda, a nośnik jest szyfrowany)
6) Samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach teleinformatycznych,
7) Świadome niszczenie danych mających znaczenie archiwalne gromadzonych w systemie,
8) Świadome wprowadzanie błędnych danych do systemu,
9) Włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,
10) Przeglądanie stron internetowych o treściach pornograficznych, erotycznych, rasistowskich, użytkowanych przez grupy przestępcze i terrorystyczne
11) Pobieranie z internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania i danych,
12) Korzystanie z list i forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą.

## 3. ZASADY UŻYTKOWANIA KOMPUTERÓW I URZĄDZEŃ PRZENOŚNYCH (LAPTOPY, DYSKI ZEWNĘTRZNE, PEN DRIVE)

3.1. Podlegają one szczególnej ochronie polegającej na zabezpieczaniu dostępu do komputera. Ich używanie poza strefą administracyjną Szpitala musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.

3.2. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza strefą administracyjną WSzS Nr 2, obowiązany jest do wystąpienia do ASI z wnioskiem o zapewnienie środków techniczno-organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia dostępu do komputera hasłem, szyfrowanie dysku/ów, zabezpieczenia kryptograficzne oraz ochronę antywirusową.

3.3. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzeniaw samochodach, przedziałach wagonów oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.

3.4. W przypadku utraty powierzonego urządzenia przenośnego używanego poza WSzS Nr 2 użytkownik niezwłocznie powiadamia o tym fakcie ASI oraz bezpośredniego przełożonego, a w przypadku kradzieży niezwłocznie zgłasza ten fakt na policję. Ponadto o kradzieży informuje osobę wydającą zgodę na wyniesienie sprzętu.

## 4. ZARZĄDZANIE HASŁAMI

4.1. Hasło do stacji roboczej, poczty elektronicznej oraz systemu mają odpowiednie cechy: minimalna długości hasła to 8 znaków, zawierających kombinację dużych i małych liter alfabetu oraz z cyfr lub znaków specjalnych:

1) (A-Z) - duże litery alfabetu,

2) (a-z) - małe litery alfabetu,

3) (0-9) – cyfry,

4) (!, @, #, $, %,...,) - znaki specjalne.

4.2. Hasła muszą składać się przynajmniej z 3 spośród 4 powyższych grup znaków. Ponadto co 30 dni następuje zmiana hasła. Zabronione jest zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób,

4.3. Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:

1) Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła).

2) W przypadku ujawnienia lub podejrzenia ujawnienia hasła.

4.4. Zmiana haseł użytkowników jest wymuszana przez system co 30 dni. W przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła nie rzadziej niż co 30 dni.

4.5. Hasła nie mogą się powtarzać względem 7 poprzednio wprowadzonych haseł;

4.6. Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy wykorzystywać: dat, imion, nazwisk, numerów telefonów itp.

4.7. Użytkownik zobowiązuje się do zachowania hasła w poufności Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

4.8. W przypadku domniemania lub faktu poznania przez osobę nieuprawnioną hasła należy niezwłocznie zmienić hasło i poinformować o zdarzeniu/problemie IODO.

4.9. W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, Użytkownik zobowiązany jest wystąpić osobiście do ASI o zmianę hasła w sytuacji:

1) Zapomnienia/zgubienia hasła;

2) Wygaśnięcia ważności hasła;

3) Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła;

4) Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

## 5. ZARZĄDZANIE POCZTĄ ELEKTRONICZNĄ:

5.1. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Szpitala nie stanowi własności prywatnej użytkownika podlega rejestrowaniu i może być monitorowana,

5.2. Wewnętrzna poczta elektroniczna służy wyłącznie do celów służbowych. Niedopuszczalne jest odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki, rejestrowanie się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy itp.

5.3. Wysyłanie za pośrednictwem poczty elektronicznej plików zawierających dane szczególnej kategorii należy dodać wybrany folder do archiwum za pomocą programu 7-Zip i zabezpieczyć go hasłem. Pomoc przy dokonaniu zabezpieczenia można uzyskać u IODO, ASI lub pracownika działu informatyki. Odbiorca zabezpieczonego pliku otrzymuje hasło za pośrednictwem innej formy kontaktu (np. telefonicznie). Niedopuszczalne jest wysyłanie pliku wraz z hasłem do zabezpieczenia w wiadomości mailowej.

5.4. Użytkownicy obowiązani są do okresowego porządkowania i usuwania wiadomości zbędnych z folderów programu pocztowego tak, aby nie dopuścić do jego zablokowania z powodu przekroczenia dopuszczalnej pojemności skrzynki.

5.5. Zabronione jest:

1) Wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu).

2) Otwieranie załączników nieznanego pochodzenia np. (faktura, której się nie spodziewamy itp.)

3) Ukrywanie lub dokonywanie zmian tożsamości nadawcy.

6. POSTĘPOWANIE W PRZYPADKU WYKRYCIA WIRUSA

6.1. W przypadku wykrycia wirusa, na ekranie wyświetlony zostanie komunikat programu antywirusowego. Użytkownik ma obowiązek niezwłocznie powiadomić ASI i postępować zgodnie z jego instrukcjami. Ponadto należy zapoznać się treścią komunikatu programu antywirusowego o wykrytym wirusie. Nie wolno natomiast kasować, kopiować, przenosić plików danych i nie niszczyć nośników danych (zachować dowody).

## 7. PROCEDURA WYREJESTROWANIA UŻYTKOWNIKA

7.1. Użytkownicy systemu informatycznego są niezwłocznie wyrejestrowywani przez ASI, gdy tracą prawo dostępu do systemu.

7.2. Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez ASI

7.3. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie.

7.4. ASI dokonuje cyklicznej weryfikacji dostępu do systemu informatycznego na podstawie raportu dotyczącego zmian personalnych (zatrudnienia, zakończenie pracy, przesunięcia na inne stanowisko) przekazywanego przez Kierownika Działu Personalnego.

## 8. STANOWISKO PRACY

8.1. Użytkownik rozpoczyna prace z systemem informatycznym przetwarzającym dane osobowe z użyciem nadanego mu identyfikatora i hasła.

8.2. Zmiana użytkownika stacji roboczej każdorazowo poprzedza wylogowanie się poprzedniego użytkownika. W uzasadnionych przypadkach dopuszczona jest możliwość przełączenia konta użytkownika za pomocą opcji „przełącz użytkownika", bez konieczności wylogowania wcześniej zalogowanej osoby.

8.3. W celu ograniczenia ryzyka nieuprawnionego dostępu, utraty lub uszkodzenia informacji w czasie godzin pracy i poza nimi użytkownik jest zobowiązany:

1) Przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych – szafy i pomieszczenia zamykane na klucz.

2) Nie pozostawiać stacji roboczych i komputerów przenośnych i bez nadzoru w stanie aktywnej sesji dostępu do sieci- należy się wylogować przed opuszczeniem stanowiska pracy nawet na krótki czas.

3) Podczas nieobecności przy stanowisku komputerowym należy wylogować się z systemu.

8.4. Po zakończeniu pracy wylogować się z systemu i wyłączyć komputer, niedopuszczalne jest zakończenie pracy bez wykonania pełnej i poprawnej procedury zamknięci.

8.5. Po zakończeniu pracy uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów (w szczególności zawierających dane osobowe) - szafy i pomieszczenia zamykane na klucz.

8.6. Przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu.

8.7. Ustawiać monitory komputerów w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu.

8.8. Zwracać szczególną uwagą na pracujące drukarki pozostawione bez nadzoru.

8.9. Nie pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach.

8.10. Niszczyć niepotrzebne nośniki papierowe w niszczarkach szczególnie nośników zawierających informacje szczególnej kategorii, których sposób niszczenia powinien uniemożliwić ich odtworzenie w przyszłości.

8.11. Pracownik jest zobowiązany do

1) Dbania o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów meblami, zasłonami lub stawiać komputerów tuż przy ścianie);

2) Niepodłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. Grzejniki, czajniki, wentylatory);

3) Kasowania po wykorzystaniu danych na pamięciach przenośnych;

4) Nieużywania powtórnie dokumentów zadrukowanych jednostronnie;

5) Niezapisywania hasła wymaganego do uwierzytelnienia się w systemie na papierze lub innym nośniku;

6) Bezpiecznej utylizacji wszelkich nośników (tradycyjnych oraz elektronicznych) zawierających dane osobowe po ustaniu ich przydatności;

7) Niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych;

8) Niedopuszczalne jest sporządzanie wydruków dokumentów zawierających dane osobowe za pomocą drukarek sieciowych w innym pomieszczeniu niż zostały one sporządzone z wyjątkiem systemów gdzie wydruk znajduje się pod kontrolą osoby z ciągu aprobującego dany dokument i to ona nanosi swój podpis, pieczątkę i datę wytworzenia na dokumencie, bądź niszczy w wypadku pomyłki.

## 9. KORZYSTANIE Z KLUCZY DO POMIESZCZEŃ

9.1. Klucze do wszystkich pomieszczeń na terenie Szpitala muszą być dostępne w każdej chwili (np. w przypadku awarii, pożaru, zalania, gdy istnieje konieczność dostania się się do pomieszczenia najszybciej jak to możliwe)

9.2. Bezpośredni nadzór nad gospodarką kluczami Administracji i Działu Technicznego sprawują portierzy zgodnie z grafikiem służby. Pracownicy tych komórek administracyjnych zobowiązani są do ewidencjonowania pobierania oraz oddawania kluczy. Fakt ten kwitują w „Książce wydawanych kluczy".

9.3. Bezpośredni nadzór nad gospodarką kluczami Oddziałów Szpitala, Zakładu Diagnostyki Obrazowej i Izby Przyjęć sprawują sekretariaty.

9.4. Nadzór nad gospodarką kluczami Poradni Przyszpitalnych sprawują portierzy zgodnie z grafikiem służby. W przypadku braku klucza fakt ten zgłaszają Pielęgniarce Koordynującej Poradni Przyszpitalnych.

9.5. Rozpoczynając pracę, osoba odpowiedzialna za nadzór kluczami powinna sprawdzić czy w przeznaczonej do tego szafie znajdują się wszystkie klucze zgodnie z wykazem.

9.6. Na klucze brakujące w szafie, dyżurujący portier winien mieć pokwitowanie pobrania w „Książce wydawanych kluczy"

9.7. W przypadku Oddziałów Szpitala, Poradni Przyszpitalnych, Zakładu Diagnostyki Obrazowej i Izby Przyjęć - każdy pracownik jest odpowiedzialny za swoje miejsce pracy i za klucze do danego pomieszczenia.

9.8. Klucze zapasowe przechowywane są przez Dyrektora ds. Technicznych i w razie potrzeby (uszkodzenia, zgubienia klucza głównego) mogą być wydane do użytku uprawnionym osobom na czas odtworzenia klucza głównego. Klucze zapasowe po wykorzystaniu należy niezwłocznie zwrócić do depozytu.

## 10. IDENTYFIKATORY

10.1. Pracownicy Szpitala, maja obowiązek nosić w widocznym miejscu identyfikator zawierający imię i nazwisko oraz funkcję tej osoby.

## 11. TELEFONICZNE INFORMOWANIE O DYŻURACH LEKARSKICH:

11.1. Przetwarzanie danych osobowych ma miejsce wyłącznie w określonym celu oraz wynika z prawnie uzasadnionego obowiązku. O tym czy należy informować pacjentów o obecności danego lekarza w pracy decyduje Lekarz Zarządzający Oddziałem.

## VI. KOMÓRKI ORGANIZACYJNE WYKONUJĄCE DZIAŁALNOŚĆ MEDYCZNĄ – OCHRONA DANYCH OSOBOWYCH

**Najważniejszą zasadą współpracy na linii personel medyczny-pacjent jest ochrona zdrowia i życia pacjenta a następnie poszanowanie jego godności i ochrona danych osobowych.**

1. **UDOSTĘPNIANIE DOKUMENTACJI MEDYCZNEJ** – Ze względu na szeroki zakres zagadnień, sposób postępowania został opisany w osobnym dokumencie.

Należy się zapoznać z procedurą QP-PP 4-01 Zasady udostępniania dokumentacji medycznej.

**2. UDZIELANIE INFORMACJI NA TEMAT STANU ZDROWIA PACJENTA:**

2.1 Jeżeli pacjent **nie ukończył 16 lat lub jest nieprzytomny bądź niezdolny do zrozumienia** znaczenia informacji, lekarz udziela **informacji osobie bliskiej tzn:**

1) małżonkowi,

2) krewnemu lub powinowatemu do drugiego stopnia w linii prostej (rodzice i dziadkowie, teściowie pacjenta, jego dzieci i wnuki),

3) osobie pozostającej we wspólnym pożyciu ( w takim przypadku należy pobrać pisemne oświadczenie od osoby domagającej się informacji, że jest osobą bliską i załączyć do dokumentacji pacjenta)

4) osobie wyznaczonej przez pacjenta.

2.2 Pacjentowi, który nie ukończył 16 lat, lekarz udziela informacji w zakresie i formie potrzebnej do prawidłowego przebiegu procesu diagnostycznego lub terapeutycznego i wysłuchuje jego zdania.

2.3 W przypadku gdy pacjent jest przytomny i zdolny do wyznaczenia osoby upoważnionej do uzyskiwania informacji na temat jego stanu zdrowia, lekarz ma **zakaz udzielenia informacji** nawet osobie najbliższej, w tym rodzinie, jeśli pacjent nie wyrazi na to jednoznacznej zgody.

2.4 Lekarz ma obowiązek udzielać pacjentowi lub jego ustawowemu przedstawicielowi lub osobie upoważnionej przystępnej informacji o jego stanie zdrowia, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych, leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu.

2.5 Policja może otrzymać informację o stanie zdrowia pacjenta, gdy pacjent zwolni lekarza z zachowania tajemnicy oraz na polecenie prokuratury lub sądu. Udostępnianie danych osobowych na podstawie ustnego wniosku zawierającego wszystkie powyższe cztery elementy wniosku pisemnego może nastąpić tylko wtedy, gdy zachodzi konieczność niezwłocznego działania, np. w trakcie pościgu za osobą podejrzaną o popełnienie czynu zabronionego albo podczas wykonywania czynności mających na celu ratowanie życia i zdrowia ludzkiego lub mienia.

2.6 Prokuratura i sądy są instytucjami uprawnionymi do uzyskiwania informacji o stanie zdrowia pacjenta.

**3. TELEFONICZNIE UDZIELANIE INFORMACJI O STANIE ZDROWIA PACJENTA:**

3.1 W wyjątkowych przypadkach możliwe jest telefoniczne poinformowanie osoby bliskiej o stanie zdrowia pacjenta. Ważne jest odwołanie się do zdrowego rozsądku i doświadczenia życiowego. W przypadku, kiedy odmowa udzielenia informacji o pobycie Pacjenta w szpitalu może uniemożliwiać realizację prawa osób bliskich do informacji o stanie zdrowia pacjenta, lekarz lub osoba wyznaczona przez lekarza powinna udzielić takiej informacji, w sytuacjach nagłych (np. wypadek drogowy klęska żywiołowa) oraz stanach zagrożenia dla życia Pacjenta.

3.2 W celu telefonicznego udzielania informacji na temat stanu zdrowia pacjenta niezbędne jest podjecie próby weryfikacji tożsamości rozmówcy. Możliwe jest uprawdopodobnienie, że rozmówca jest osobą uprawnioną do uzyskania tej informacji poprzez zadanie pytań kontrolnych (np. zapytanie o PESEL pacjenta).

3.3 Przy udzielaniu informacji należy kierować się zasadą minimalizacji i przekazywać telefonicznie jedynie te informacje, które są niezbędne do działania w stanie wyższej konieczności

3.4 W celu telefonicznego udzielania informacji na temat stanu zdrowia pacjenta osobom upoważnionym w przypadkach innych niż nagłe (np. pacjenci długotrwale hospitalizowani) można ustalić inne zasady zapewniające jednoznaczną weryfikację tożsamości osoby upoważnionej. Może to być np. ustalenie hasła.

**4. ZAPEWNIENIE ANONIMOWOŚCI PACJENTA PODCZAS REJESTRACJI I WIZYTY NP. W PORADNI lub POZ**

5. Dążyć należy do minimalizacji ryzyka ujawnienia informacji osobom postronnym, w szczególności danych o stanie zdrowia.

5.1 Należy ustalić tożsamość osoby ubiegającej się o udzielenie świadczenia w sposób nieutrudniający dostępu do jego uzyskania, z ograniczeniem ryzyka uzyskania danych osobowych przez osobę trzecią, poprzez okazanie dokumentu weryfikującego tożsamość. Jeżeli Pacjent odmawia okazania dokument weryfikującego tożsamość można poprosić go o podanie danych identyfikacyjnych tj. PESEL.

5.2 Przy okienku rejestracji (w sekretariacie itp.) powinien znajdować się wyłącznie obsługiwany pacjent, ewentualnie osoba towarzysząca (bliska). Pozostałe osoby takie jak inni pacjenci, osoby towarzyszące tym pacjentom, powinny pozostawać poza tym obszarem.

5.3 **Wywoływanie pacjentów do gabinetów lekarskich, do wykonania badania itp**. Możliwe przykładowe sposoby wywoływania Pacjenta:

1) Wezwanie po numerze nadanym podczas rejestracji. Takie rozwiązanie wiąże się z nadawaniem unikalnego numeru podczas rejestracji w sposób, zapewniający przekazanie numeru lekarzowi w gabinecie oraz Pacjentowi (dopięty do karty, przekazany Pacjentowi).

2) Wezwanie po imieniu oraz godzinie np. Pan Michał z godziny 11:30

3) Dodanie numeru gabinetu, np. Pan Jan z godziny X proszony do gabinetu Y.

4) Gdy jest kilka kategorii Pacjentów lub rodzajów poradni możliwe jest przydzielanie numerów w różnych kolorach (np. czerwona jedynka, żółta trójka itp.).

5.4 **Wywoływanie pacjentów – IZBA PRZYJĘĆ**- powołując się na ochronę żywotnych interesów pacjenta możliwe jest zwracanie się po imieniu i nazwisku.

## 6. OBCHÓD I PRZEKAZYWANIE INFORMACJI PACJENTOWI:

6.1 Co do zasady, przekazywanie przez personel medyczny Pacjentowi informacji ujawniających dane o stanie jego zdrowia, na sali wieloosobowej, powinny być ograniczone do minimum niezbędnego do realizacji celu.

6.2 Osoby nieuprawnione, tj. osoby odwiedzające innych pacjentów, powinny w czasie obchodu opuścić salę chorych, a drzwi od sali, jeżeli to możliwe powinny zostać zamknięte tak, aby osoby nieuprawnione nie mogły usłyszeć informacji przekazywanych podczas wizyty.

6.3 Jeżeli u Pacjenta, któremu przekazujemy informacje, są osoby odwiedzające, to także powinny opuścić salę chorych chyba, że są to osoby bliskie lub upoważnione a pacjent wyrazi zgodę na ich obecność.

6.4 Osoby biorące udział w obchodzie inne niż udzielające świadczeń zdrowotnych np. inni lekarze, pielęgniarki, fizjoterapeuci, biorą udział w obchodzie bez zgody Pacjenta, jeżeli są osobami wykonującymi zawód medyczny i tylko wtedy, gdy jest to niezbędne ze względu na rodzaj świadczenia. Jeżeli nie spełniają tego wymogu, to mogą brać udział w obchodzie wyłącznie za zgodą Pacjenta.

6.5 Jeżeli podczas obchodu lekarze zamierzają dokonać obserwacji miejsc intymnych Pacjenta, wyniki obserwacji nie powinny być wypowiadane na głos na sali wieloosobowej, a jedynie wpisywane do dokumentacji medycznej.

6.6 Komunikacja z pacjentem np. informowanie o pobieraniu świadomej zgody na procedury medyczne, informacja o diagnozie i sposobie leczenia, wynikach itp., jeżeli stan zdrowia pacjenta na to pozwala, przekazanie takich informacji ustronnym miejscu, tj. w takim, w którym nie przebywają inne nieuprawnione osoby, np. inni pacjenci (dotyczy to zarówno sali chorych, jak i np.

korytarza szpitalnego). Przy rozmowie może być obecna, za zgodą pacjenta, np. osoba bliska/członek rodziny.

6.7 Komunikacja z pacjentem związana bezpośrednio z realizacją bieżącego monitorowania stanu zdrowia, w tym pytanie o samopoczucie, uzyskanie i przekazanie podstawowych informacji związanych z procesem leczenia, w tym również czynności w ramach obchodu lekarskiego może odbywać się na salach wieloosobowych. Możliwe jest przekazanie informacji o zmianie leków, o planowanych badaniach, na sali chorych (różnica polega na tym, że przekazujemy informację np. o planowanych badaniach a wynik tego badania powinien być omawiany z pacjentem tak jak w przypadku poprzedniego punktu).

6.8 W trakcie wykonywania bieżących czynności medycznych, w tym w trakcie obchodu lekarskiego, na sali mogą przebywać wyłącznie osoby uprawnione, tj. personel medyczny, opiekun faktyczny, opiekunowie ustawowi pacjenta małoletniego, całkowicie ubezwłasnowolnionego lub niezdolnego do świadomego wyrażenia zgody. Na życzenie pacjenta w trakcie udzielania świadczenia może być obecna osoba bliska z zastrzeżeniem, że w przypadku obchodu opuszcza salę chorych, jeżeli omawiany jest stan zdrowia innego Pacjenta.

6.9 W przypadku, gdy rozmowa o stanie zdrowia pacjenta związana jest bezpośrednio z ratowaniem życia bądź zdrowia i nie przeprowadzenie rozmowy w trybie natychmiastowym mogłoby narazić Pacjenta na uszczerbek, możliwe jest przeprowadzenie rozmowy w każdym miejscu.

6.10 Lekarz nie powinien na sali chorych zwracać się po imieniu i nazwisku do pacjenta (zwłaszcza w obecności osób postronnych). Można natomiast zwracać się do pacjenta używając chociażby zwrotu „Pan/Pani”wraz z dodaniem imienia, co jednocześnie zagwarantuje poszanowanie godności pacjenta. Wyjątkiem są przypadki, gdy lekarz nie może zidentyfikować pacjenta w inny sposób niż poprzez użycie jego nazwiska, bądź gdy jest to konieczne dla podejmowania nagłych czynności ratowania życia bądź zdrowia. Najważniejsze jest ochrona zdrowia i życia pacjenta a w następnej kolejności ochrona jego danych osobowych i poszanowanie godności.

## 7. OPIS ŁÓŻEK, KARTY PRZYŁÓŻKOWE (GORĄCZKOWE)

7.1 W związku z tym, że istotą działania Szpitala jest ochrona życia bądź zdrowia pacjenta, a w bardzo wielu przypadkach nagłe pogorszenie się stanu zdrowia pacjenta może wymagać natychmiastowego dostępu do jego danych identyfikacyjnych, możliwe jest opisywanie łóżek oraz zastosowanie kart przyłożkowych. W przypadku, gdy Lekarz Zarządzający Oddziałem uzna, że zastosowanie kart jest konieczne, należy dokonać ich zabezpieczenia poprzez:

1) Zastosowanie ramek na kartę przyłóżkowe chroniących dane osobowe zawarte w kartach-konstrukcja ramki powinna uniemożliwiać odczytanie danych;

2) zastosowanie nakładki zabezpieczającej dane pacjenta na karcie przyłóżkowej;

3) odwrócenie kart przyłóżkowych.

## VII. POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA INCYDENTÓW ZWIĄZANYCH Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

1. Incydent naruszenia ochrony danych osobowych - 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.
2. Sposób postępowania w przypadku zidentyfikowania incydentu naruszenia ochrony danych osobowych w komórkach organizacyjnych został opisany w Procedurze QP-ZI/2-01 - PROCEDURA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA INCYDENTÓW ZWIĄZANYCH Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH
3. Każdy pracownik Szpitala, a w szczególności osoba, która w ramach wykonywania swoich obowiązków służbowych przetwarza dane osobowe, jest obowiązana niezwłocznie powiadomić o zaistniałym przypadku naruszenia ochrony danych osobowych do IODO pod rygorem postępowania dyscyplinarnego.

## VIII. OGÓLNE ZASADY STOSOWANIA MONITORINGU

1. Monitoring w Szpitalu jest uzasadniony względami bezpieczeństwa pacjentów i pracowników Szpitala.

2. Informacja o tym, że w Szpitalu prowadzony jest monitoring wizyjny znajduje się przy każdym wejściu na teren Szpitala w widocznym miejscu.

3. Zapisy monitoringu wizyjnego traktowane są podobnie jak dane osobowe i podlegają takiej samej ochronie.

4. Sposób udostępnienia zapisów monitoringu

   1. Zapisy monitoringu mogą być udostępnione na płycie CD lub do wglądu na pisemny wniosek.
   2. Instytucje uprawnione do dostępu do nagrań (np. Policja, Prokuratura) oraz osoby, których wizerunek został utrwalony (w uzasadnionych przypadkach) składają wniosek do Sekretariatu Dyrektora, w którym określony jest cel, zakres oraz podstawa prawna (w przypadku instytucji).
   3. Zgoda na udostępnienie materiału jest przedkładana odpowiednio pracownikowi Działu Informatyki i stanowi podstawę do przygotowania przedmiotowego nagrania,
   4. Udostępnienie odbywa się bez zbędnej zwłoki jednak nie później niż do 14 dni od daty otrzymania wniosku.
   5. Pracownik Działu Informatyki po udostępnieniu nagranego materiału sporządza protokół przekazania, który zostaje umieszczony w rejestrze udostępniania zapisów monitoringu wraz z wnioskiem.

5. Szpital nie ingeruje w treść zapisanych danych i nie spełnia żądania korekty lub usunięcia danych wobec osób objętych monitoringiem, a zapisane dane, w przypadku braku incydentów usuwa z systemu po ustalonym w punkcie 10 czasie.

6. System monitoringu nie ma na celu nagrywania (np. poprzez zbliżenie lub ukierunkowanie kamery) lub innego rodzaju przetwarzania (np. indeksowanie, profilowanie) obrazów ujawniających tzw. szczególne kategorie danych: o pochodzeniu rasowym lub etnicznym, poglądach politycznych, religijnych lub filozoficznych, przynależności do związków zawodowych, zdrowiu i życiu seksualnym.

7. Monitoringowi nie podlegają obszary, w których istnieje zwiększone prawdopodobieństwo nagrania obrazów ujawniających szczególne kategorie danych ( przebieralnie, toalety, itp.).

8. Kamery są umieszczane przede wszystkim na korytarzach i w niektórych oddziałach nie są instalowane w salach chorych. Rozmieszczenie kamer jest opisane w załączniku nr ….....

9. Urządzenia do zapisu monitoringu są zabezpieczone przed dostępem oraz zabraniem przez osoby nieupoważnione.

10. Czas przechowywania danych monitoringu nie jest dłuższy niż 30 dni za wyjątkiem zabezpieczenia zapisów na wniosek prokuratury, policji i innych uprawnionych służb.

11. Na stronie internetowej Szpitala umieszczona jest klauzula informacyjna dotycząca przetwarzania danych za pośrednictwem monitoringu.

## IX. NAGRYWANIE ROZMÓW

1. Wszystkie rozmowy przychodzące oraz wychodzące z Poradni Nocnej i Świątecznej Opieki Zdrowotnej Wojewódzkiego Szpitala Specjalistycznego Nr 2 w Jastrzębiu-Zdroju są rejestrowane.

2. Udostępnianie zarejestrowanego materiału, bez względu na sposób organizacji rejestracji i archiwizacji, odbywa się w następujący sposób:

2.1. Złożenie pisemnego wniosku do Dyrekcji Szpitala o udostępnienie nagrania ze szczegółowym wskazaniem uzasadnienia oraz wskazaniem okresu jaki dotyczy nagrania.

2.2. Zgoda na udostępnienie materiału jest przedkładana odpowiednio pracownikowi Działu Informatyki i stanowi podstawę do przygotowania przedmiotowego nagrania,

2.3. Po otrzymaniu zgody, odsłuchanie materiału odbywa się w obecności przedstawiciela Dyrekcji (Zastępca lub inny wskazany pracownik).

2.4. Z przesłuchania sporządza się notatkę służbową, która jest przechowywana w BOK

2.5. Dopuszczalne jest przesłanie nagranego materiału Dyrekcji Szpitala lub innej wskazanej przez Dyrekcję osobie w formie zaszyfrowanego pliku.

2.6. Po wykorzystaniu materiału ulega on zniszczeniu tak, aby nie było możliwości jego odtworzenia.

3. Wszystkie zdarzenia i awarie mające wpływ na zachowanie obowiązku rejestrowania rozmów należy natychmiast zgłaszać Dyrekcji Szpitala oraz do BOK

**4. Klauzula informacyjna**

4.1. Po wykonaniu połączenia odtwarzany jest następujący komunikat:

*Szanowni Państwo, w trosce o bezpieczeństwo świadczonych usług medycznych, rozmowy mogą być rejestrowane. Jeżeli nie wyrażacie Państwo zgody na ich nagrywanie, prosimy o przerwanie połączenia. Informujemy, że Administratorem Państwa danych osobowych jest Wojewódzki Szpital Specjalistyczny Nr 2 w Jastrzębiu-Zdroju. Szczegółowe informacje o danych kontaktowych administratora oraz inspektora ochrony danych a także o celach i podstawach prawnych przetwarzania danych, jak również przysługujących prawach znajdziecie Państwo na stronie www.WSS2.pl.*

## X. OBOWIĄZEK INFORMACYJNY

1. WSzS Nr2 przekazuje pacjentom informacje, o których mowa w art. 13 RODO w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie poprzez:

1.1. Umieszczenie klauzul informacyjnych na stronie internetowej

1.2. Umieszczenie informacji na tablicach informacyjnych w przestrzeniach ogólnodostępnych, najczęściej wykorzystywanych przez Pacjentów (tablice informacyjne na każdym oddziale, okienka rejestracji )

2. WszS Nr2 przekazuje informacje:

2.1. kandydatom do pracy na etapie rekrutacji,

2.2. pracownikom

2.3. kontrahentom

2.4. osobom, których dane osobowe przetwarzane są na nagraniach rozmów przychodzących oraz wychodzących z Poradni Nocnej i Świątecznej Opieki Zdrowotnej

2.5. osobom, których dane osobowe przetwarzane są na nagraniach monitoringu wizyjnego

3. Informacje, o których mowa w art. 13 RODO w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie.

## XI. OPIS TECHNICZNYCH I ORGANIZACYJNYCH ŚRODKÓW OCHRONY DANYCH OSOBOWYC

1. Przypisano role i odpowiedzialności ADO, ASI, IODO, kierowników poszczególnych komórek organizacyjnych oraz każdego pracownika szpitala.

2. Określono sposób postępowania w przypadku osoby nowo zatrudnionej w WSzS Nr 2 oraz dyscyplinarną odpowiedzialność związaną z naruszeniem opisanych w polityce zasad.

3. Określono zasady bezpiecznego przetwarzania danych osobowych oraz bezpiecznego użytkowania powierzonego sprzętu przez pracowników szpitala w poszczególnych obszarach:

3.1. Ogólne zasady przetwarzania danych osobowych

1) Zasady bezpiecznego użytkowania systemów informatycznych

2) Zasady bezpiecznego użytkowania komputerów i urządzeń przenośnych (laptopy, dyski zewnętrzne, pen drive)

3) Zarządzanie hasłami

4) Zarządzanie pocztą elektroniczną

5) Postępowanie w przypadku wykrycia wirusa

6) Procedura wyrejestrowania użytkownika z systemu informatycznego:

7) Zasady dbania o bezpieczeństwo informacji na swoim stanowisku pracy

8) Korzystanie z kluczy do pomieszczeń

3.2. W przypadku komórek organizacyjnych wykonujących działalność medyczną określono zasady:

1) Udostępnianie dokumentacji medycznej

2) Udzielanie informacji na temat stanu zdrowia pacjenta

3) Telefonicznie udzielanie informacji o stanie zdrowia pacjenta:

4) Zapewnienie anonimowości pacjenta podczas rejestracji i wizyty np. W poradni:

5) Obchód lekarski i przekazywanie informacji pacjentowi.

6) Opis łóżek, karty przyłóżkowe (gorączkowe).

4. Monitoring w szpitalu jest uzasadniony względami bezpieczeństwa pacjentów i pracowników szpitala. Ustalono sposób udostępniania oraz okres przechowywania nagrań.

5. Rozmowy przychodzące oraz wychodzące z Poradni Nocnej i Świątecznej Opieki Zdrowotnej Wojewódzkiego Szpitala Specjalistycznego Nr 2 w Jastrzębiu-Zdroju są rejestrowane. Ustalono sposób udostępniania nagrań oraz okres przechowywania nagrań.

6. WSzS Nr 2 przekazuje informacje, o których mowa w art. 13 RODO w zwięzłej, przejrzystej, zrozumiałej oraz łatwo dostępnej formie.

7. Wszyscy pracownicy WSzS nr 2 są zobowiązani do zachowanie poufności oraz przestrzegania zasad bezpiecznego przetwarzania danych osobowych opisanych w niniejszej polityce. Wszyscy użytkownicy systemu muszą stosować się do obowiązujących procedur bezpieczeństwa. Obowiązek trwa także po ustaniu stosunku pracy. Nie przewiduje się czasowego ograniczenia tego obowiązku.

8. Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.

9. Dokumenty i nośniki informacji, zawierające dane osobowe znajdują się w pomieszczeniach zabezpieczonych przed dostępem osób nieupoważnionych do przetwarzania danych. Jeśli nie są aktualnie używane - są przechowywane w szafach lub w innych przeznaczonych do tego celu urządzeniach biurowych, posiadających odpowiednie zabezpieczenia.

10. Pomieszczenia są chronione poprzez ograniczenia dostępu do grona osób upoważnionych za pośrednictwem instrukcji postępowania z kluczami do pomieszczeń. Ponadto dodatkowemu

zabezpieczeniu (poprzez czytnik linii papilarnych bądź kod dostępu) podlegają oddział anestezjologii i intensywnej terapii, izba przyjęć, blok operacyjny.

11. Wprowadzono procedurę QP-ZI/2-01 - procedura postępowania w przypadku wystąpienia incydentów związanych z naruszeniem ochrony danych osobowych.

12. Szkolenia w zakresie ochrony danych osobowych. Przeprowadzane są bieżące szkolenia wewnętrzne i zewnętrzne dla wszystkich osób upoważnionych do przetwarzania danych osobowych również w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych

13. Pomieszczenia, w których przetwarzane są dane osobowe zabezpieczone powinno być przed skutkami pożaru za pomocą gaśnic (miejsce jej przechowywania jest odpowiednio oznaczone) a pracownicy mają wiedzę jak jej użyć.

14. Szczegółowe informacje na temat zasad korzystania z systemów informatycznych zawarte są w „Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w WSzS Nr 2" będącą integralną częścią niniejszej polityki.

„INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM" JEST DOKUMENTEM OBJĘTYM TAJEMNICĄ PRZEDSIĘBIORSTWA. UDOSTĘPNIANA JEST WYŁĄCZNIE OSOBOM UPOWAŻNIONYM PRZEZ ADO, ASI, IODO. W PRZYPADKU KONTROLI ORGANU NADZORCZEGO UDOSTĘPNIANIA JEST DO WGLĄDU WYLEGITYMOWANEMU KONTROLEROWI.

14.1. Zapisy instrukcji obejmują szczegółowe opisy dotyczące:

1) Przetwarzania danych w systemie teleinformatycznym.

2) Nadawanie/cofanie uprawnień do przetwarzania danych osobowych.

3) Zasad przydzielania uprawnień do korzystania z systemów teleinformatycznych.

4) Rejestru uprawnień do przetwarzania danych osobowych.

5) Przeglądu praw dostępu użytkowników.

6) Zarządzania metodami oraz środkami uwierzytelniania.

7) Procedura uwierzytelniania użytkownika w systemie informatycznym.

8) Procedury rejestrowania/wyrejestrowania użytkownika z systemu informatycznego.

9) Korzystania z poczty elektronicznej.

10) Korzystanie z innych usług sieciowych.

11) Rozpoczęcie, zawieszenie i zakończenie pracy w systemie informatyczny.

12) Postępowania z nośnikami wymiennymi.

13) Systemu informatycznego - zabezpieczenie danych i programów.

14) Ochrony przed złośliwym oprogramowaniem.

15) Wykonywania kopii bezpieczeństwa.

16) Zabezpieczeń systemu informatycznego.

17) Zasad udzielania pomocy użytkownikom przez dział IT.

18) Procedury postępowania w przypadku wystąpienia awarii krytycznych lub usterek dla pracownika działu IT.

19) Inwentaryzacji aktywów.

20) Zasad napraw i likwidacji sprzętu komputerowego.

21) Obszarów bezpiecznych.

22) Dokumentowania procedur eksploatacyjnych.

23) Oprogramowania.

24) Zarządzanie oprogramowaniem.

25) Instalacja oprogramowania.

26) Oprogramowanie produkcyjne.

27) Bezpieczeństwo komunikacji.

28) Audytów bezpieczeństwa.

## XII. PODSTAWY PRAWNE

1. Konstytucja Rzeczypospolitej Polskiej (art. 47, 51);
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000)
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 94/46/WE (ogólne rozporządzenie o ochronie danych).
4. Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318, z późn. zm.);
5. Ustawa z dnia 30 czerwca 2011 o działalności leczniczej (Dz. U. 2011 Nr 112 poz.654)
6. Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty (Dz. U. z 2018 r. poz. 617, z późn. zm.);
7. 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)
8. Ustawa z dnia 30 czerwca 2011 o działalności leczniczej (Dz. U. 2011 Nr 112 poz.654)
9. Rozporządzenie Ministra Zdrowia dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (Dz. U. 2010 Nr 252, poz.1697).
10. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 25 października 2007 r. w sprawie rodzaju i zakresu oraz sposobu przetwarzania dokumentacji medycznej w zakładach opieki zdrowotnej utworzonych przez ministra właściwego do spraw wewnętrznych (Dz. U. 2007 nr 217 poz. 1614).

## XIII. TABELA ZMIAN

| WERSJA | DATA PUBLIKACJI | ZAKRES ZMIAN |
|---|---|---|
| **1** | Listopad 2011 | Dokument podstawowy |
| **2** | Lipiec 2015 | Aktualizacja dokumentu podstawowego |
| **3** | Luty 2019 | Aktualizacja dokumentu podstawowego |
| | | |
| | | |
| | | |
| | | |