# KOMPENDIUM WIEDZY

## DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI I FUNKCJONOWANIA WOJEWÓDZKIEGO SZPITALA SPECJALISTYCZNEGO NR 2 W JASTRZĘBIU-ZDROJU

| STANOWISKO/KOMÓRK ORGANIZACYJNA | | Data |
|---|---|---|
| Opracował: | **INSPEKTOR OCHRONY DANYCH OSOBOWYCH**<br>**RZECZNIK PRASOWY**<br>inż. Marcelina Twardowska | **10.05.2024 r.** |
| Zatwierdził: | **DYREKTOR**<br>mgr Robert Rychel | **10.05.2024 r.** |

## I. CO TO JEST KOMPENDIUM WIEDZY I JAKIE MA ZASTOSOWANIE

Kompendium Wiedzy dotyczące bezpieczeństwa informacji i funkcjonowania Wojewódzkiego Szpitala Specjalistycznego Nr 2 w Jastrzębiu-Zdroju jest dokumentem obowiązującym wszystkich pracowników i jest częścią Systemu Zarzadzania Bezpieczeństwem Informacji oraz Ciągłości Działania. Ma na celu wskazanie pracownikom WSS Nr 2 w jaki sposób bezpiecznie przetwarzać dane osobowe oraz inne informacje, niezależnie od formy ich przetwarzania (systemy informatyczne, informacje zgromadzone w formie tradycyjnej- papierowej, kontakt osobisty).

## II. ODPOWIEDZIALNOŚĆ

Każdy pracownik, szczególnie nowo zatrudniony jest zobowiązany do zapoznania się poniższymi dokumentami:

Lokalizacja → Dysk wspólny o nazwie Zasoby publiczne → folder WAŻNE DOKUMENTY

| Nazwa dokumentu | Jednostka Odpowiedzialna / kontakt |
|---|---|
| Kompendium Wiedzy Dotyczące Bezpieczeństwa Informacji | Marcelina Twardowska – Inspektor Ochrony Danych<br>32 47 84 536 mtwardowska@wss2.pl<br>Zbigniew Trzcionkowski<br>- Pełnomocnik ds. Cyberbezpieczeństwa<br>32 47 84 510 ztrzcionkowski@wss2.pl |
| Regulamin Organizacyjny | Biuro Organizacji i Audytu Wewnętrznego<br>Bogusława Kacprzyk – kierownik działu<br>32 47 84 533, bkacprzyk@wss2.pl |
| Regulamin Pracy | Dział Kadr<br>32 47 84 520, 521, 522 |
| Polityka Antymobbingowa | Dział Kadr<br>32 47 84 520, 521, 522 |
| Regulamin Wynagradzania | Dział Kadr<br>32 47 84 520, 521, 522 |
| Procedury Szpitalne odpowiednio dla jednostki organizacyjnej | Bezpośredni przełożony,<br>Agnieszka Gilga - Pełnomocnik ds. Jakości |

Nieprzestrzeganie postanowień dotyczących bezpieczeństwa informacji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej przepisami Kodeksu Pracy i w wewnętrznych regulacjach WSS Nr 2. Jeżeli skutkiem zamierzonego działania osób uprawnionych do dostępu do informacji jest ujawnienie informacji osobie nieuprawnionej, osoby te mogą być pociągnięte do odpowiedzialności karnej określonej przepisami Kodeksu Karnego.

1. **Odpowiedzialność porządkowa i dyscyplinarna** – upomnienie ustne, upomnienie pisemne, nagana. W przypadku ciężkiego naruszenia podstawowych obowiązków pracowniczych, skutkiem może być rozwiązanie stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. **Odpowiedzialność materialna** - w przypadku, gdy nieprawidłowe, niezgodne z prawem przetwarzanie danych przez pracownika narazi Szpital na szkodę np. wypłatę odszkodowania na rzecz osoby fizycznej, której prawa i wolności zostały naruszone, wówczas, jeśli bezprawność zachowania (wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych) i wina pracownika zostaną należycie wykazane, **pracownik może zostać pociągnięty do odpowiedzialności materialnej**.
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

## ZASADY BEZPIECZNEGO PRZETWARZANIA INFORMACJI

II. IDENTYFIKATORY

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

III. KORZYSTANIE Z KLUCZY DO POMIESZCZEŃ

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 do pomieszczenia najszybciej jak to możliwe)
   a) 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".
   b) Bezpośredni nadzór nad gospodarką kluczami Oddziałów Szpitala, Zakładu Diagnostyki Obrazowej i Izby Przyjęć sprawują sekretariaty.

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

2. Rozpoczynając pracę, osoba odpowiedzialna za nadzór kluczami powinna sprawdzić czy w przeznaczonej do tego szafie znajdują się wszystkie klucze zgodnie z wykazem. Na klucze brakujące w szafie, dyżurujący portier winien mieć pokwitowanie pobrania w „Książce wydawanych kluczy".
3. 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.
4. Klucze zapasowe przechowywane są w dziale technicznym 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.
5. **Zabrania się odtwarzania kluczy przez osoby do tego nieuprawnione.**

## III. BEZPIECZNE PRZETWARZANIE INFORMACJI – STANOWISKO PRACY

1. Przy pierwszym wejściu do obszaru przetwarzania (dyżurka, 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.
2. Informacje, w tym dane osobowe, przetwarzane tradycyjnie (papierowo) po godzinach pracy mają być przechowywane w zamykanych szafkach. W przypadku przetwarzania takich danych w pomieszczeniu, w którym przebywać mogą osoby nieupoważnione do ich przetwarzania (np. interesanci, pacjenci albo inni pracownicy) powinny być przetwarzane w taki sposób, aby osoby nieupoważnione nie miały wglądu do tych danych.
3. Należy przechowywać dokumenty papierowe i wymienne nośniki komputerowe w odpowiednio zabezpieczonych meblach biurowych – szafy i pomieszczenia zamykane na klucz.
4. Nie wolno pozostawiać dokumentacji papierowej, stacji roboczych i komputerów przenośnych bez nadzoru w stanie aktywnej sesji dostępu do sieci- należy się wylogować lub zablokować ekran przed opuszczeniem stanowiska pracy, nawet na krótki czas oraz nie zostawiać pomieszczenia bez nadzoru osoby upoważnionej.
5. Należy przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien podczas nieobecności w pomieszczeniu.
6. Monitory komputerów muszą być ustawione w taki sposób, żeby uniemożliwić osobom nieupoważnionym wgląd w zawartość ekranu.

7. Nie wolno pozostawiać wymiennych nośników komputerowych w napędach, bądź ogólnie dostępnych miejscach.
8. Należy niszczyć niepotrzebne nośniki papierowe w niszczarkach, szczególnie te zawierające informacje szczególnej kategorii (dane wrażliwe), których sposób niszczenia powinien uniemożliwić ich odtworzenie w przyszłości.
9. Należy dbać o prawidłową wentylację komputerów (nie można zasłaniać kratek wentylatorów, lub stawiać komputerów tuż przy ścianie);
10. Po zakończeniu pracy trzeba uporządkować swoje stanowisko pracy, uniemożliwiając dostęp osób nieupoważnionych do dokumentów (w szczególności zawierających dane osobowe) - szafy i pomieszczenia zamykane na klucz, przestrzegać zasady niepozostawiania otwartych i niezabezpieczonych drzwi i/lub okien.

## IV. PRACA W SYSTEMACH INFORMATYCZNYCH

### Ogólne zasady bezpiecznego użytkowania systemów informatycznych –systemu szpitalnego, poczty elektronicznej itp.

1. Środki do przetwarzania informacji wykorzystywane w WSS Nr 2 są przeznaczone wyłącznie do wykonywania zadań służbowych. Użytkownik ponosi odpowiedzialność za powierzony sprzęt i oprogramowanie oraz sposób jego eksploatacji.
2. Każdy użytkownik ma w systemie, w którym pracuje ( np. KS-MEDIS ) unikalny identyfikator zatem ponosi odpowiedzialność za wszelkie czynności wykonane z użyciem jego identyfikatora i hasła.
3. Niedopuszczalne jest, aby dwóch lub większa ilość użytkowników wykorzystywała wspólnie jedno konto użytkownika w Zintegrowanym Systemie Informatycznym (HIS i ERP).
4. Zabronione jest:
   a) udzielanie informacji osobom postronnym o zasadach ochrony systemów teleinformatycznych Szpitala, w tym o identyfikatorach używanych w tych systemach,
   b) umożliwianie dostępu do systemów teleinformatycznych osobom nieupoważnionym,
   c) udostępnianie danych osobom nieupoważnionym,
   d) rejestrowanie się w systemie na identyfikatorze innego użytkownika,
   e) przenoszenie informacji również uzyskanych w związku z wykonywanymi zadaniami służbowymi na/ i z prywatnych nośników informacji, w szczególności pamięci typu pendrive i inne pamięci zewnętrzne (chyba, że jest na to zgoda, a nośnik jest szyfrowany),
   f) samowolne modyfikowanie ustawień związanych z bezpieczeństwem w systemach

teleinformatycznych,

g) świadome usuwanie danych mających znaczenie archiwalne gromadzonych w systemie,

h) świadome wprowadzanie błędnych danych do systemu,

i) włączanie urządzeń elektrycznych do wydzielonej instalacji elektrycznej przeznaczonej dla systemów teleinformatycznych,

j) pobieranie z Internetu, kopiowanie, instalowanie, przechowywanie lub rozpowszechnianie nieautoryzowanego oprogramowania i danych,

k) korzystanie ze stron internetowych, forów dyskusyjnych, gier internetowych oraz innych usług, nie mających związku z wykonywaną pracą (związane z ryzykiem prób włamania do systemu szpitalnego).

5. W przypadku bardzo ważnych dokumentów, których utrata może spowodować zakłócenie ciągłości pracy lub funkcjonowania szpitala konieczne jest wykonywanie kopii zapasowych na dysk wspólny, do odpowiednio przygotowanego folderu. Pracownik może zwrócić się do Działu Informatyki o utworzenie lub wskazanie takiego miejsca.

**Polityka haseł**

1. Hasło do stacji roboczej, poczty elektronicznej, szyfrowanych plików oraz systemu muszą mieć odpowiednie cechy:
   a) minimalna długości hasła to 15 znaków,
   b) duże litery alfabetu, (A-Z),
   c) małe litery alfabetu, (a-z),
   d) cyfry, (0-9),
   e) znaki specjalne (!, @, #, $, %,. ,).
2. Zabronione jest zapisywanie haseł w sposób jawny i umieszczania ich w miejscach dostępnych dla innych osób oraz przekazywanie ich innym osobom.
3. Zabrania się tworzenia haseł na podstawie:
   a) cech i numerów osobistych (np. dat urodzenia, imion itp.),
   b) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx, 1q2w3e4r5t, itp.),
   c) identyfikatora użytkownika (loginu),
   d) innych haseł łatwych do odgadnięcia.
4. Użytkownik powinien zabezpieczyć dostęp do służbowej poczty elektronicznej, służbowego adresu e-mail poprzez nadanie indywidualnego hasła, przy czym pierwsze hasło jest nadawane Użytkownikowi przez Dział Informatyki,
5. Użytkownik powinien chronić hasło przed dostępem osób trzecich, w każdym przypadku, gdy hasło zostało ujawnione innej osobie, Użytkownik jest zobowiązany do jego zmiany.
6. W przypadku domniemania lub faktu poznania przez osobę nieuprawnioną hasła należy

niezwłocznie poinformować ASI o zdarzeniu/problemie i zmienić hasło.

7. W przypadku braku dostępu do konta chronionego hasłem (np. z powodu zapomnienia/zagubienia hasła, zablokowania konta), w którego posiadaniu się znajduje, Użytkownik zobowiązany jest wystąpić osobiście, w dowolny sposób, do Działu Informatyki o zmianę hasła w sytuacji:

**Poczta elektroniczna – e-mail**

Zabrania się logowania do systemów poczty elektronicznej z urządzeń dostępnych poza siedzibą szpitala za wyjątkiem pracowników posiadających na to zgodę.

1. Służbową pocztę elektroniczną należy przeglądać minimum raz w tygodniu.
2. Wewnętrzna poczta elektroniczna służy wyłącznie do celów służbowych.
3. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Szpitala nie stanowi własności prywatnej użytkownika podlega rejestrowaniu i może być monitorowana. Korespondencja i dane przechowywane w elektronicznym systemie pocztowym stanowią własność WSS Nr 2. ASI może na polecenie Dyrektora lub IOD weryfikować zawartości wiadomości pocztowych, co może mieć miejsce w następujących przypadkach:
   a) uzasadnionego podejrzenia naruszenia przez Użytkownika postanowień procedury lub przepisów powszechnie obowiązujących,
   b) gdy dostęp jest niezbędny ze względu na uzasadniony interes WSS Nr 2,
   c) na wezwanie uprawnionego organu państwowego, jeżeli obowiązek taki wynika z przepisów powszechnie obowiązujących.
4. Korespondencja i dane zawarte w elektronicznym systemie pocztowym, mogą zostać udostępnione innemu użytkownikowi. Czynności tej dokonać można na wniosek kierowany do Dyrektora, IODO lub ASI. We wniosku wskazuje się powód udostępnienia oraz osobę, której udostępnia się wskazane zasoby. Udostępnienia dokonuje się w obecności pracownika IT, który dokonuje logowania i po zakończonej pracy – wylogowania.
5. Użytkownik powinien zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
6. Niedopuszczalne jest odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki, rejestrowanie się na stronach handlowych, informacyjnych, chatach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy.
7. 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.
8. Zabronione jest:
   a) Wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu).

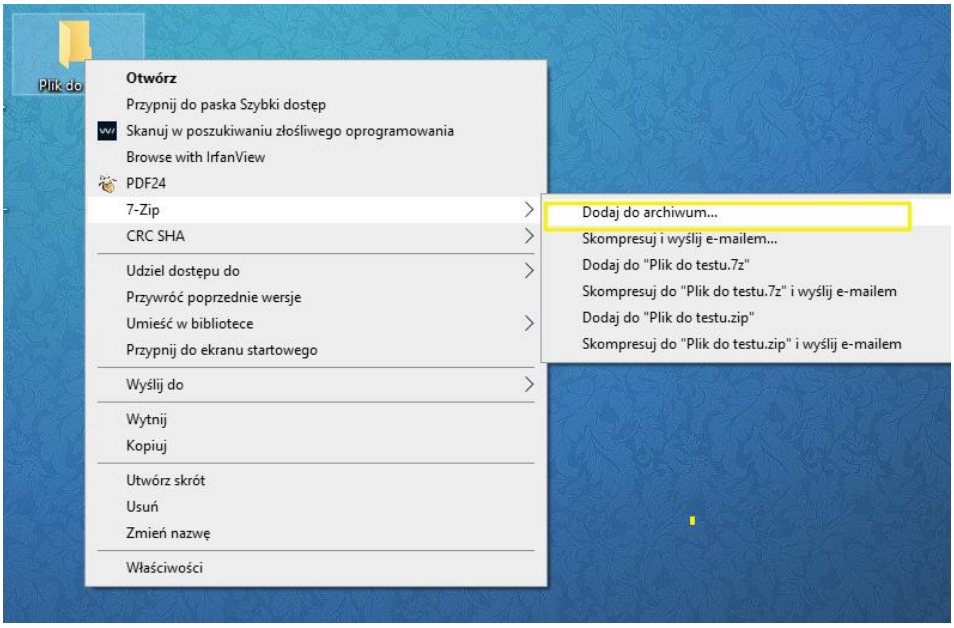
b) Otwieranie załączników nieznanego pochodzenia np. (faktura, której się nie spodziewamy itp.).

c) Otwieranie linków oraz załączników w korespondencji elektronicznej nadesłanej przez nieznanego nadawcę lub podejrzanych załączników nadanych przez znanego nadawcę.

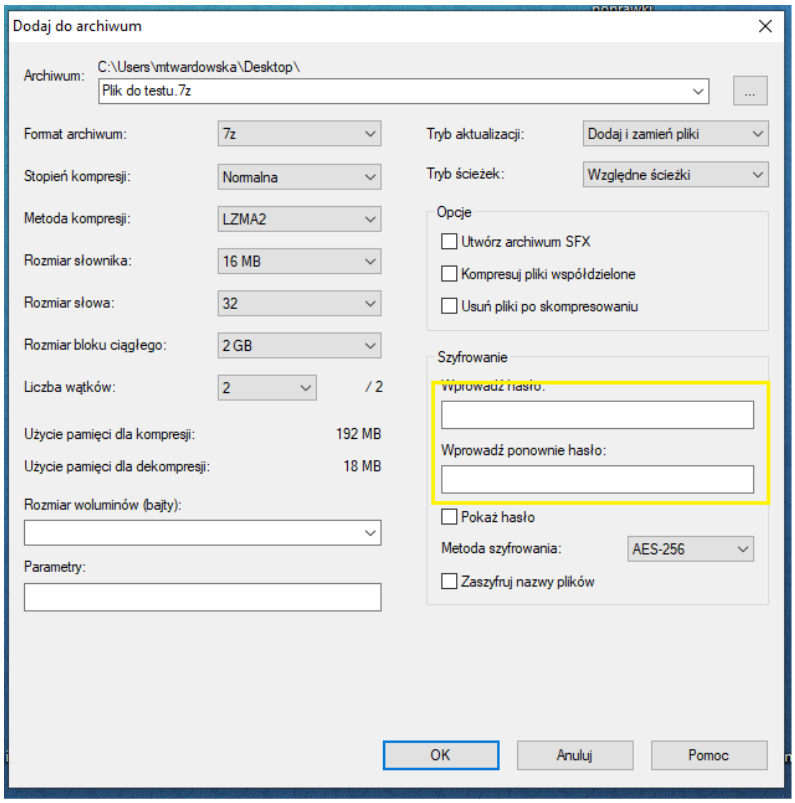
d) Ukrywanie lub dokonywanie zmian tożsamości nadawcy.

9. W przypadku dostępu do szpitalnej poczty elektronicznej z sieci Internet należy uważnie przeczytać pojawiające się w przeglądarce komunikaty o alertach bezpieczeństwa i nigdy nie ignorować ostrzeżeń.
10. WSS Nr 2 zastrzega sobie prawo zablokowania konta poczty elektronicznej w przypadkach jego wykorzystania w sposób niezgodny z powyższymi zasadami.
11. <u>Wysyłanie za pośrednictwem poczty elektronicznej plików zawierających dane szczególnej kategorii należy odpowiednio chronić! Sposób postępowania:</u>

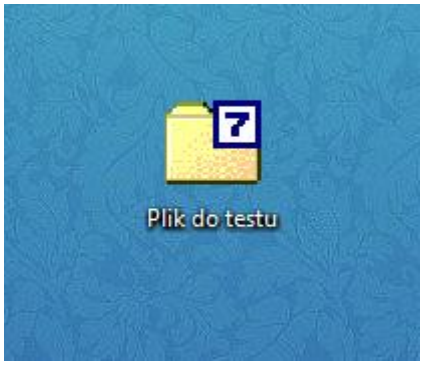
a) Klikając prawym przyciskiem myszy na plik przeznaczony do szyfrowania należy wybrać z listy 7-zip, a następnie - opcję „dodaj do archiwum”.




b) Po pojawieniu się okna, w sekcji szyfrowanie należy wprowadzić wymyślone przez siebie hasło zgodne z polityką haseł ( min15. znaków ….)




c) Po wykonaniu tych czynności na pulpicie pojawi się plik o tej samej nazwie, ale innym rozwinięciu (ikonka żółty folder z „7”). Zabezpieczony plik należy wysłać mailem, natomiast hasło należy przekazać telefonicznie (lub innym źródłem). Pomoc przy dokonaniu zabezpieczenia można uzyskać u IODO lub w DI. Niedopuszczalne jest wysyłanie pliku wraz z hasłem do zabezpieczenia w jednej lub kilku wiadomościach mailowych.



**Zasady użytkowania komputerów i urządzeń przenośnych (laptopy, dyski zewnętrzne, pen drive itp.)**

1. Komputery i urządzenia przenośne podlegają szczególnej ochronie polegającej na zabezpieczaniu dostępu. Ich używanie poza strefą administracyjną Szpitala musi mieć uzasadnienie w realizowanych przez pracownika zadaniach. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem pracy poza strefą administracyjną WSS Nr 2, obowiązany jest do wystąpienia do ASI z wnioskiem o zapewnienie środków technicznych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się zabezpieczenia dostępu do komputera hasłem, szyfrowanie dysku/ów, zabezpieczenia kryptograficzne oraz ochronę antywirusową.
2. Na użytkowniku urządzenia przenośnego spoczywa obowiązek jego ochrony, w szczególności zabrania się pozostawiania bez opieki tego typu urządzenia w samochodach, przedziałach wagonów oraz innych miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
3. W przypadku utraty powierzonego urządzenia przenośnego używanego poza WSS 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 użytkowanie sprzętu poza siedzibą pracodawcy.

## IV. 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. <u>Udostępnianie dokumentacji medycznej</u>

Dostęp do dokumentacji medycznej jest jednym z podstawowych praw pacjenta. Udostępnienia dokonuje się na wniosek (w dowolnej formie, również ustnej), poprzez wgląd lub wydanie kopii (w formie elektronicznej lub papierowej).

Udostępnianie dokumentacji medycznej do wglądu pacjentowi (również w trakcie hospitalizacji) odbywa się z wyłączeniem dokumentacji dotyczącej medycznych czynności ratunkowych, z zapewnieniem pacjentowi lub instytucjom uprawnionym z <u>możliwości sporządzenia notatek lub zdjęć.</u>

W przypadku, gdy na terenie Szpitala dochodzi do zdarzenia niepożądanego, w wyniku którego nastąpi zgon pacjenta (np. samobójstwo), skutkującego koniecznością poinformowania Prokuratury o zajściu, istnieje wysokie prawdopodobieństwo konieczności zabezpieczenia przez prokuraturę oryginałów dokumentacji medycznej poszkodowanego pacjenta. Wówczas należy niezwłocznie

wykonać kopię.

Szczegółowy opis wraz ze sposobem przekazania dokumentacji znajduje się w procedurze **QP-PP 4-01** Zasady udostępniania dokumentacji medycznej
(lokalizacja – dysk wspólny zasoby publiczne → procedury szpitalne → Procedury szpitalne nowe 21-22 → zarzadzanie informacją).

2. Udzielanie informacji na temat stanu zdrowia pacjenta:

a) Jeżeli pacjent nie ukończył 16 lat lub jest nieprzytomny bądź niezdolny do zrozumienia znaczenia informacji, lekarz udziela informacji osobie bliskiej tzn.
   - małżonkowi,
   - krewnemu do drugiego stopnia (rodzice, dziadkowie, dzieci, wnuki, rodzeństwo),
   - powinowatemu do drugiego stopnia w linii prostej (teściowie pacjenta, zięć, synowa),
   - osobie pozostającej we wspólnym pożyciu (w takim przypadku można pobrać pisemne oświadczenie od osoby domagającej się informacji, że jest osobą bliską i załączyć do dokumentacji pacjenta),
   - osobie wyznaczonej przez pacjenta.

b) 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.

c) 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.

d) 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.

e) 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.

f) Prokuratura i sądy są instytucjami uprawnionymi do uzyskiwania na pisemny wniosek informacji o stanie zdrowia pacjenta.

3. **Telefonicznie udzielanie informacji o stanie zdrowia pacjenta:**
   a) 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.
   b) W celu telefonicznego udzielania informacji na temat stanu zdrowia pacjenta niezbędne jest podjęcie 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).
   c) Przy udzielaniu informacji należy kierować się zasadą minimalizacji i przekazywać telefonicznie jedynie te informacje, które są niezbędne do działania w stanie wyższej konieczności
   d) 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**
   a) Dążyć należy do minimalizacji ryzyka ujawnienia informacji osobom postronnym, w szczególności danych o stanie zdrowia.
   b) 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.
   c) 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. **Wywoływanie pacjentów do gabinetów lekarskich, do wykonania badania itp.**
   Nie należy wzywać pacjentów na wizytę w poradni/ do wykonania badania imieniem i nazwiskiem. **Możliwe przykładowe sposoby wywoływania Pacjenta:**
   a) 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)

b) Wezwanie po imieniu oraz godzinie np. „Pan Michał zapisany na godzinę 11.00”

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

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

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

7. Obchód i przekazywanie informacji pacjentowi:

a) 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.

b) 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.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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. planowanych badaniach a wynik tego badania powinien być omawiany z pacjentem tak jak w przypadku poprzedniego punktu).

h) 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.

i) 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.

j) 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.

**Opis łóżek, karty przyłóżkowe (gorączkowe)**

8. W związku z tym, że istotą działania Szpitala jest ochrona życia i zdrowia pacjenta, w wielu przypadkach nagłe pogorszenie się stanu zdrowia pacjenta może wymagać natychmiastowego dostępu do jego danych identyfikacyjnych. Możliwe jest zatem opisywanie łóżek oraz zastosowanie kart przyłóżkowych. W przypadku, gdy Lekarz Zarządzający Oddziałem uzna, że zastosowanie kart jest konieczne, należy dokonać ich zabezpieczenia poprzez:
   a) zastosowanie ramek na kartę przyłóżkowe chroniących dane osobowe zawarte w kartach- konstrukcja ramki powinna uniemożliwiać odczytanie danych.
   b) zastosowanie nakładki zabezpieczającej dane pacjenta na karcie przyłóżkowej,
   c) odwrócenie kart przyłóżkowych.

## V. POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA INCYDENTÓW ZWIĄZANYCH Z NARUSZENIEM OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI

1. Incydent naruszenia ochrony danych - 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. W przypadku podejrzenia zidentyfikowania incydentu należy niezwłocznie powiadomić o tym IOD lub Dział IT, Kierownika IT.

   Można również zgłosić ten fakt do Działu Organizacji, Sekretariatu Dyrektora.

   a) Marcelina Twardowska – inspektor ochrony danych
      32 47 84 536 mtwardowska@wss2.pl
   b) Sebastian Spandel – główny specjalista ds. informatyki i administrator systemów informatycznych
      32 47 84 510 SebastianSpandel@wss2.pl
   c) Zbigniew Trzcionkowski - pełnomocnik ds. cyberbezpieczeństwa
      32 47 84 509 ztrzcionkowski@wss2.pl
   d) Bogusława Kacprzyk – kierownik biura organizacji i audytu wewnętrznego
      32 47 84 533, bkacprzyk@wss2.pl
   e) Sekretariat Dyrektora - 32 47 84 500
   f) Dział Informatyki – 32 47 84 509, inf@wss2.pl
3. 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 (lokalizacja – dysk wspólny zasoby publiczne → WAŻNE DOKUMENTY)

## VI. MONITOROWANIE STACJI ROBOCZYCH.

1. Program Axence nVision jest instalowany na wszystkich komputerach i służy do:
   a) udzielania pomocy użytkownikom komputerów (łączenie się z użytkownikami poprzez zdalny pulpit, które jest realizowane na prośbę użytkowników),
   b) lepszej komunikacji pomiędzy pracownikami poprzez czat ( możliwość pisania każdy z każdym, dodawania załączników oraz prowadzenie czatów grupowych dla danych oddziałów lub konkretnych grup osób pracujących nad wspólnym projektem),
   c) zgłaszania próśb do Działu IT o pomoc poprzez system helpdesk,
   d) monitorowania sieci LAN,WAN w celu ich prawidłowego działania,

e) instalacji i monitorowania aplikacji oraz wykrywania błędów w ich działaniu,

f) inwentaryzacji sprzętu i oprogramowania (drukarki, monitory, komputery, dyski twarde, pendrive, pamięci RAM i inne podzespoły),

g) zabezpieczenia sieci i komputerów przed włamaniami i wyciekiem danych,

h) planowania zakupów nowego sprzętu komputerowego lub wymianie podzespołów w obecnie użytkowanym sprzęcie.

## VII. INFORMOWANIE MEDIÓW I PRZEPŁYW INFORMACJI

Osobą reprezentującą Szpital w przestrzeni publicznej jest Dyrektor, Rzecznik Prasowy oraz osoby upoważnione przez Dyrekcję. Dotyczy to zarówno środków masowego przekazu takich jak telewizja, prasa, radio, portale informacyjne, jak i mediów społecznościowych m. in. portal Facebook, Instagram. W związku z tym udostępnianie nieautoryzowanych przez w/w osoby zdjęć, postów, informacji dotyczących szpitala i jego funkcjonowania jest zabronione. Nieakceptowalne jest również udzielanie informacji przedstawicielom mediów.

## VIII. POSZANOWANIE DLA WSPÓŁPRACOWNIKÓW

Zachowanie tajemnicy służbowej ma zastosowanie również w stosunku do naszych współpracowników. Mając na uwadze, że każdy pracownik szpitala może stać się również jego pacjentem lub potrzebować innej pomocy, dbajmy o wspólne poszanowanie godności, prawa do intymności naszych kolegów i koleżanek. Używanie programu szpitalnego w celu dowiadywania się szczegółów dotyczących przebiegu leczenia, kariery czy innych informacji niezwiązanych z wykonywanymi obowiązkami służbowymi jest rażącym naruszeniem ochrony danych osobowych oraz poszanowania godności osób, których to dotyczy. Również powtarzanie plotek lub innych informacji stwarza obszar do nieetycznych zachowań prowadzących do naruszenia przepisów.

PAMIĘTAJ O NAJWAŻNIEJSZYCH ZASADACH

Zapoznaj się z dokumentami, w przypadku jakichkolwiek pytań osoby odpowiedzialne chętnie odpowiedzą.

Nie przetwarzaj nadmiarowo danych osobowych, niszcz wszystkie dodatkowe notatki, notatniki, pomoce i wszystko to, co nie podlega archiwizacji.

Jesteś odpowiedzialny za swoje stanowisko pracy, biuro, gabinet i powierzony sprzęt, sprawdzaj czy „wszystko" działa prawidłowo, wątpliwości zgłaszaj przełożonym.

Zamykaj drzwi biura, gabinetu jak wychodzisz, nawet na chwilę. W pomieszczeniach wieloosobowych dokonaj wylogowania przed odejściem ze swojego stanowiska.

W systemach informatycznych pracuj wyłącznie na swoim loginie i haśle, nie udostępniaj tych informacji innej osobie, gdyż jesteś odpowiedzialny za to, jakie zmiany zostaną wprowadzone „na twoje konto"

Chroń loginy i hasła, nikomu ich nie ujawniaj, nie zapisuj w widocznych miejscach.

Poczta służbowa e-mail służy do zadań służbowych! Nie jest Twoją prywatną pocztą, może być ona udostępniana innym osobom.

Przeglądarka internetowa i poczta mogą być oknem dla cyberprzestępców, odwiedzaj tylko zaufane strony internetowe, potrzebne do zadań służbowych

Chroń prywatność pacjentów – tam gdzie tylko się da, zorganizuj pracę tak, żeby nie ujawniać osobom postronnym szeroko rozumianych danych osobowych. Dbaj o godność osób powierzonych Twojej opiece.

Chroń prywatność i godność współpracowników.

Zwracaj uwagę na to, co mówisz przy osobach postronnych (np. w windzie czy na korytarzu), wiele rzeczy można się w ten sposób dowiedzieć.

Zgłaszaj incydenty związane z bezpieczeństwem informacji.

Nie upubliczniaj informacji o funkcjonowaniu szpitala, to zadanie dyrektora, rzecznika prasowego lub osób wyznaczonych.