



## **I. RODO**

RODO (ogólne rozporządzenie o ochronie danych osobowych) oznacza 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 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych).

Jednym z celów ogólnego rozporządzenia o ochronie danych osobowych jest ujednolicenie przepisów regulujących ochronę danych osobowych w krajach UE, a także ujednolicenie sposobu przepływu danych pomiędzy tymi krajami.

RODO chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.

RODO kompleksowo reguluje kwestie ochrony danych osobowych i obowiązuje od 25 maja 2018 roku we wszystkich państwach członkowskich UE.

Pełny tekst RODO dostępny jest na stronie Urzędu Ochrony Danych Osobowych pod adresem: <https://uodo.gov.pl/pl/404/539>.

Polskim aktem prawnym uzupełniającym przepisy o ochronie danych osobowych jest ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Ustawa nie powiela przepisów RODO, a jedynie uzupełnia RODO w takim zakresie, w jakim prawodawca unijny dopuścił doprecyzowanie niektórych kwestii na gruncie prawa krajowego. Tekst ustawy o ochronie danych osobowych dostępny jest na stronie Urzędu Ochrony Danych Osobowych pod adresem: <https://uodo.gov.pl/pl/395/1192>.

## **II. Dane osobowe**

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoba, 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 (adres IP, adres e-mail), jeden lub kilka szczególnych czynników na określenie fizycznej, fizjologicznej, genetycznej, psychicznej, ekonomicznej, kulturowej lub społecznej tożsamości osoby fizycznej. Podmiot danych – osoba fizyczna, którą można zidentyfikować na podstawie określonych danych osobowych. Osoba niezidentyfikowana to taka, której tożsamości nie znamy, ale możemy ją poznać za pomocą posiadanych przez nas środków (danych).

### Przykłady:

- a. **osoba zidentyfikowana:** pacjent, którego dane są przetwarzane przez Szpital; pracownik, którego dane osobowe są przetwarzane przez pracodawcę; student, którego dane są przetwarzane przez uczelnię.
- b. **osoba możliwa do zidentyfikowania:** lekarz/pielęgniarka z numerem licencji znamy zawód; student, którego numer albumu i nazwa uczelni są znane.

### Wyróżniamy następujące rodzaje/kategorie danych osobowych:

- a. szczególne kategorie danych osobowych:
  - dane ujawniające pochodzenie rasowe lub etniczne,
  - poglądy polityczne,
  - przekonania religijne lub światopoglądowe,



- przynależność do związków zawodowych,
  - dane genetyczne,
  - dane biometryczne,
  - dane dotyczące zdrowia,
  - orientacja seksualna,
- b. tzw. zwykłe dane osobowe, np.:
- imię i nazwisko,
  - PESEL,
  - adres zamieszkania, -
  - data urodzenia,
  - płeć,
  - imiona rodziców,
  - wykształcenie,
  - adres e-mail,
  - numer telefonu,
  - numer i seria dowodu osobistego,
  - login.

### **III. Dane dotyczące zdrowia**

Dane dotyczące zdrowia to wszystkie dane o stanie zdrowia osoby, której dane dotyczą. Dane dotyczące zdrowia oznaczają dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym świadczenia usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia. Dane osobowe dotyczące zdrowia powinny obejmować wszelkie dane dotyczące stanu zdrowia osoby fizycznej, które ujawniają informacje o przeszłym, obecnym lub przyszłym stanie zdrowia fizycznego lub psychicznego osoby, której dane dotyczą.

#### Do takich danych należą:

- a. informacje o danej osobie fizycznej zebrane podczas jej rejestracji do świadczeń opieki zdrowotnej lub w trakcie udzielania jej świadczeń opieki zdrowotnej, - numer, symbol lub oznaczenie nadawane danej osobie fizycznej w celu jednoznacznej identyfikacji tej osoby dla celów zdrowotnych;
- b. informacje z badań laboratoryjnych lub medycznych części ciała lub płynów, w tym dane genetyczne i próbki biologiczne;
- c. wszelkie informacje np. o chorobie, historii choroby, 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.

Dane dotyczące zdrowia pacjentów Szpitala, w tym dane zawarte w dokumentacji medycznej, należą do szczególnej kategorii danych osobowych i podlegają szczególnej ochronie prawnej.

### **IV. Na czym polega przetwarzanie danych osobowych**

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



- a. zbieranie,
- b. utrwalanie,
- c. organizowanie,
- d. przechowywanie,
- e. adaptowanie lub modyfikowanie,
- f. pobieranie,
- g. przeglądanie,
- h. wykorzystywanie,
- i. ujawnienie lub przesłanie,
- j. rozpowszechnianie lub udostępnianie w jakikolwiek inny sposób,
- k. dopasowanie lub łączenie,
- l. ograniczenie,
- m. usuwanie lub zniszczenie.

Przetwarzaniem danych osobowych jest każda czynność, którą wykonujemy z wykorzystaniem danych osobowych (wszystkie operacje dokonywane na danych osobowych) w celu osiągnięcia określonego celu przetwarzania.

**Zapoznanie (przeglądanie, czytanie) przez Stażystów/ Studentów /Praktykantów/ Wolontariuszy danych zawartych w dokumentacji medycznej pacjenta w celach dydaktycznych jest również przetwarzaniem danych osobowych.**

## **V. Sposoby przetwarzania danych osobowych w Szpitalu**

Szpital przetwarza dane osobowe:

- a. tradycyjnie (dokumentacja papierowa),
- b. elektronicznie.

Przykładowe czynności przetwarzania: wprowadzanie danych do systemu, zapisywanie, wyszukiwanie, kopiowanie, modyfikowanie, pobieranie, zapisywanie, porządkowanie, usuwanie. Dane osobowe są chronione niezależnie od sposobu ich przetwarzania.

Nie ma znaczenia, w jaki sposób dane osobowe są wykorzystywane czy przechowywane czy korzystamy z najnowszego systemu informatycznego czy dokumentów papierowych w segregatorach/teczkach, księgach, wykazach, ewidencjach w każdym z tych przypadków przetwarzanie danych podlega wymogom RODO.

## **VI. Administrator Danych Osobowych**

Pojęcie „Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych.

Administradora Danych Osobowych- reprezentowany jest przez Dyrektora Szpitala.

Administrator określa cele i sposoby przetwarzania danych osobowych, a także jest do tego zobowiązany uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze ryzyko do wdrożenia odpowiednich środków organizacyjno-technicznych, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO.



## **VII. Inspektor Ochrony Danych**

Zadania IOD to przede wszystkim:

- doradzanie organizacji i personelowi w zakresie ochrony danych osobowych;
- monitorowanie przestrzegania przepisów RODO w organizacji;
- podnoszenie świadomości personelu na temat ochrony danych osobowych;
- współpraca z organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego i osób, których dane dotyczą.

## **VIII. Administrator Systemu Informatycznego**

Administrator Systemu Informatycznego jest odpowiedzialny m.in. za:

- obsługę techniczną i organizacyjną systemu informatycznego,
- administrację systemem informatycznym,
- administrowanie bazą danych w systemie,
- ocenę i zarządzanie procesem zapewnienia bezpieczeństwa systemu oraz przetwarzanych w nim danych, w tym danych osobowych,
- administrację serwerami i urządzeniami zabezpieczającymi,
- zarządzanie uprawnieniami użytkowników.

## **IX. Zasady przetwarzania danych osobowych**

Jeśli przetwarzasz dane osobowe, musisz to robić zgodnie z poniższymi zasadami:

- Zgodność z prawem, uczciwość i przejrzystość**- przetwarzanie musi być zgodne z prawem, rzetelne i przejrzyste dla osoby, której dane dotyczą.
- Ograniczenie celu**- musisz przetwarzać dane w prawnie uzasadnionych celach, wyraźnie określonych dla osoby, której dane dotyczą, podczas ich zbierania.
- Minimalizacja danych**- należy zbierać i przetwarzać tylko tyle danych, ile jest absolutnie niezbędne do określonych celów.
- Dokładność**- musisz dbać o dokładność i aktualność danych osobowych.
- Ograniczenie przechowywania**- możesz przechowywać dane osobowe tylko tak długo, jak jest to konieczne do określonego celu.
- Integralność i poufność**- przetwarzanie musi odbywać się w taki sposób, aby zapewnić odpowiednie bezpieczeństwo, integralność i poufność (np. za pomocą szyfrowania).
- Odpowiedzialność**- Administrator danych jest odpowiedzialny za wykazanie zgodności RODO ze wszystkimi tymi zasadami.

Artykuł 6 RODO wymienia przypadki, w których przetwarzanie danych osobowych jest zgodne z prawem. Jeżeli chcemy przetwarzać dane osobowe musimy to uzasadnić jednym z poniższych:

- Osoba, której dane dotyczą wyraziła konkretną, jednoznaczną zgodę na przetwarzanie jej danych.
- Przetwarzanie jest niezbędne do wykonania lub przygotowania do zawarcia umowy, której stroną jest osoba, której dane dotyczą.
- Musisz te dane przetworzyć, aby spełnić Twoje zobowiązanie prawne.
- Musisz przetworzyć dane, aby uratować komuś życie.
- Przetwarzanie jest niezbędne do wykonania zadania w interesie publicznym lub do pełnienia funkcji urzędowych.



- f. Masz uzasadniony interes w przetwarzaniu czyichś danych osobowych. Jest to najbardziej elastyczna podstawa prawna, chociaż „podstawowe prawa wolności osoby, której dane dotyczą” zawsze są nadrzędne w stosunku do Twoich interesów, zwłaszcza jeśli są to dane dziecka.

Po ustaleniu zgodnej z prawem podstawy przetwarzania danych należy udokumentować tę podstawę i powiadomić osobę, której dane dotyczą. A jeśli później zdecydujesz się zmienić uzasadnienie, musisz mieć dobry powód, udokumentować ten powód i powiadomić osobę, której dane dotyczą.

Podstawą prawną przetwarzania danych osobowych pacjentów w celach zdrowotnych przez Szpital jest wprost art. 9 sek. 2 lit. h) RODO w związku z przepisami prawa krajowego.

Brzmienie art. 9 sek. 2 lit. h) RODO: „Przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego.”

## **X. Zasady bezpieczeństwa ochrony danych osobowych**

Zasady bezpieczeństwa ochrony danych osobowych w Szpitalu:

### **a. Zasada zamkniętego pomieszczenia**

Opuszczając miejsce stażu, praktyk, zajęć, itp., należy upewnić się, że sala jest zamknięta, jeśli jesteśmy ostatnią osobą, która opuszcza pomieszczenie. W przypadku nieobecności pracowników drzwi do pokoi są zawsze zamykane na klucz, który pozostaje pod nadzorem pracownika. Niedopuszczalne jest pozostawianie pokoi bez nadzoru oraz użyczanie kluczy do pokoi osobom nieupoważnionym.

### **b. Zasada czystego biurka**

Na biurku powinny znajdować się tylko dokumenty lub inne nośniki danych, które są niezbędne do bieżącej pracy w danym momencie. Dokumentację i nośniki danych, które nie są wykorzystywane do bieżącej pracy należy zabezpieczyć przed dostępem osób niepowołanych.

### **c. Zasada czystego ekranu**

Przed wyjściem z miejsca pracy należy zablokować dostęp do komputera, a po zakończeniu pracy wyłączyć komputer. Podczas pracy monitor komputera powinien być ustawiony tak, aby nie umożliwiał oglądania wyświetlanych treści przez osoby nieuprawnione.

### **d. Zasada czystego kosza**

Zabronione jest wyrzucanie do śmieci papierowych dokumentów lub innych nośników zawierających dane osobowe. Wszystkie niepotrzebne dokumenty (wydruki, kopie, szkice itp.) należy natychmiast zniszczyć w niszczarce w sposób uniemożliwiający ich odczytanie.

### **e. Zasada czystej tablicy**

Po zakończeniu zajęć lub spotkań należy wyczyścić/zabezpieczyć wszystkie materiały i wyczyścić tablice.



## **XI. Naruszenie ochrony danych osobowych, co to oznacza**

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Naruszenie poufności polega na udostępnieniu danych osobowych osobie nieuprawnionej.

Naruszenie dostępności polega na czasowej lub trwałej utracie lub zniszczeniu danych osobowych.

Naruszenie integralności polega na zmianie treści danych osobowych w sposób nieuprawniony.

Przykłady naruszeń obejmują m.in.:

a. Udostępnianie dokumentacji medycznej osobom nieuprawnionym

Zabroniony jest dostęp do dokumentacji medycznej pacjentów Szpitala przez osoby, które nie są do tego uprawnione na mocy obowiązujących przepisów prawa.

b. Udostępnianie informacji o stanie zdrowia osobom nieuprawnionym

Zabronione jest udostępnianie dokumentacji medycznej i informacji o stanie zdrowia pacjenta (danych osobowych pacjentów) osobom i podmiotom nieuprawnionym, wbrew ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta.

c. Pozostawianie dokumentów zawierających dane osobowe, w tym dokumentację medyczną, w miejscach bez nadzoru

Dokumenty zawierające dane osobowe pacjentów powinny być zabezpieczone w sposób uniemożliwiający dostęp do tych danych osobom nieuprawnionym. Dokumenty, których aktualnie nie używamy, należy przechowywać w zamkniętych szafach, biurkach itp., obowiązuje zasada „czystego biurka”.

d. Wyrzucanie dokumentów zawierających dane osobowe do kosza

Zabrania się usuwania papierowych dokumentów zawierających dane osobowe poprzez wyrzucanie tych dokumentów do kosza. Wszelkie niepotrzebne dokumenty (wydruki, kopie, szkice itp.) należy niezwłocznie zniszczyć w sposób uniemożliwiający ich odczytanie.

e. Udostępnienie innej osobie identyfikatora i hasła do systemu informatycznego

Nie wolno udostępniać identyfikatorów i haseł do systemu informatycznego innym osobom, w tym innym pracownikom lub studentom/praktykantom. Zabronione jest korzystanie z systemu informatycznego Szpitala, jeżeli nie posiadamy do tego odpowiednich uprawnień. Zabronione jest korzystanie z kont należących do innych użytkowników.

f. Wynoszenie dokumentacji medycznej przez Studenta / Praktykanta poza Szpitalem Studentom/ Praktykantom

Zabronione jest usuwanie dokumentów należących do Szpitala, w tym dokumentacji medycznej/dokumentów zawierających dane osobowe (oryginały, kopie, wersje elektroniczne) lub ich przesyłania drogą elektroniczną.

g. Używanie identyfikatora i hasła do systemu informacyjnego innej osoby

Zabronione jest korzystanie z systemu informatycznego Szpitala, jeżeli nie posiadamy do tego odpowiednich uprawnień. Zabronione jest korzystanie z kont należących do innych użytkowników.

h. Zapisywanie danych na prywatnych nośnikach

Zabronione jest zapisywanie i przechowywanie danych osobowych pacjentów na nośnikach prywatnych (np. pendrive, smartfony, płyty CD, dyski zewnętrzne).



- i. Kradzież dokumentów, nośników, sprzętu komputerowego, urządzeń
- j. Robienie zdjęć na terenie Szpitala, zwłaszcza utrwalanie wizerunków pacjentów.

## **XII. Podejrzenie naruszenia ochrony danych osobowych**

W przypadku podejrzenia naruszenia ochrony danych osobowych należy:

- a. niezwłocznie zgłosić ten fakt do Biura Dyrekcji Szpitala lub Inspektora Ochrony Danych lub wszelkie podejrzenia naruszenia ochrony danych osobowych.  
Dane kontaktowe:
  - Biuro Dyrekcji Szpitala:  
telefon 61 8491 275  
e-mail [szpital@skp.ump.edu.pl](mailto:szpital@skp.ump.edu.pl)  
lokalizacja Budynek Administracji
  - Inspektor Ochrony Danych:  
mgr Edyta Puzicka  
telefon 61 8491 203  
e-mail [iodo@skp.ump.edu.pl](mailto:iodo@skp.ump.edu.pl)  
lokalizacja Budynek E1, piętro I.
- b. również natychmiast powiadomić opiekuna: stażu, praktyk lub wolontariatu,
- c. powstrzymać się od jakichkolwiek działań mogących utrudnić ustalenie okoliczności naruszenia, jednakże np. w przypadku znalezienia na terenie Szpitala niezabezpieczonych dokumentów, zawierających dane osobowe, w tym dokumentację medyczną, a także jej kopie, wydruki, itp., powinny być zabezpieczone tak, aby informacje zawarte w dokumentacji nie zostały ujawnione osobom nieuprawnionym
- d. współpracować z ADO, ASI i IOD w celu wyjaśnienia wszelkich okoliczności naruszenia danych osobowych.

## **XIII. Odpowiedzialność karna za naruszenie przepisów o ochronie danych osobowych**

Przepisy o odpowiedzialności karnej za naruszenie przepisów o ochronie danych osobowych mają zastosowanie do wszystkich osób zaangażowanych w przetwarzanie danych osobowych (nielegalne przetwarzanie danych osobowych).

- a. Brzmienie art. 107 ust. 1 i 2 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych:
  - „1. Kto przetwarza dane osobowe, mimo że ich przetwarzanie jest niedozwolone lub nie jest upoważnione do ich przetwarzania, podlega 14 grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
  - 2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.”.



Osoby naruszające zasady bezpieczeństwa danych osobowych, w tym Stażystów/ Studentów /Praktykantów/ Wolontariuszy mogą podlegać sankcjom karnym na podstawie przepisów o ochronie danych osobowych.

Osoby niebędące pracownikami Szpitala, w tym Stażyści/ Studenci/ Praktykanci/ Wolontariusze, ponoszą odpowiedzialność odszkodowawczą wobec Szpitala na podstawie przepisów Kodeksu Cywilnego.

#### **XIV. Podstawowe obowiązki Stażystów/ Studentów /Praktykantów/ Wolontariuszy**

Powyższe osoby zobowiązane są do:

- a. noszenia w widocznym miejscu identyfikatorów,
- b. przebywania w pomieszczeniach, w których przetwarzane są dane osobowe, wyłącznie w obecności personelu Szpitala,
- c. odbyć szkolenie z zakresu ochrony danych osobowych organizowane przez Szpital.

Stażysci/ Studenci /Praktykanci/ Wolontariusze zobowiązani są w szczególności do zapoznania się z:

- a. powszechnie obowiązującymi przepisami prawa dotyczącymi ochrony danych osobowych, w szczególności z Rozporządzeniem 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 przepływu takich danych oraz uchylenia dyrektywy 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych) oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
- b. wewnętrznymi przepisami Szpitala wskazanymi przez opiekuna grupy, w szczególności w zakresie ochrony danych osobowych, dokumentacji medycznej oraz bezpieczeństwa informacji.

Stażysci/ Studenci /Praktykanci/ Wolontariusze zobowiązani są w szczególności do przestrzegania zasad ochrony danych osobowych obowiązujących w Szpitalu, wynikających z przepisów prawa oraz regulacji wewnętrznych, w tym:

- a. dochowania należytej staranności w celu ochrony danych osobowych;
- b. zapewnienia bezpieczeństwa przetwarzania danych osobowych, w szczególności poprzez ich ochronę przed nieuprawnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, bezprawnym ujawnieniem lub pozyskaniem, w tym stosowaniem wymaganych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych;
- c. zachowania w poufności danych osobowych uzyskanych w związku z uczestnictwem w zajęciach w Szpitalu (niezależnie od sposobu ich pozyskania- pisemny, elektroniczny, ustny), zarówno w trakcie zajęć, jak i po ich zakończeniu. Obowiązek zachowania w tajemnicy danych pacjenta obowiązuje również po śmierci pacjenta;
- d. przeciwdziałania naruszeniom ochrony danych osobowych oraz zgłaszanie naruszeń lub podejrzenia naruszeń ochrony danych. Stażyści/ Studenci /Praktykanci/ Wolontariusze zobowiązani są do przestrzegania przepisów prawa, regulacji wewnętrznych oraz zarządzeń i komunikatów wydawanych przez Dyrektora Szpitala w zakresie ochrony danych osobowych, w tym danych zawartych w dokumentacji medycznej.



## **XV. Komu można udostępniać dokumentację medyczną**

Dokumentację medyczną udostępnia podmiot udzielający świadczeń zdrowotnych:

- e. pacjentowi;
- f. przedstawicielowi ustawowemu pacjenta
- g. osobie upoważnionej przez pacjenta. Poza pacjentem i osobami posiadającymi jego upoważnienie prawo dostępu do dokumentacji mogą uzyskać także inne osoby lub podmioty, jeżeli ich upoważnienie wynika bezpośrednio z przepisów prawa.

Artykuł 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta wskazuje osoby uprawnione, którym podmiot udzielający świadczeń zdrowotnych może udostępnić dokumentację medyczną. Dokumentacja medyczna pod szczególnymi warunkami może, zostać udostępniona na:

- cele dydaktyczne;
- cele naukowe.

## **XVI. Udostępnianie dokumentacji medycznej do celów dydaktycznych**

Dokumentacja medyczna podmiotów udzielających świadczeń zdrowotnych uczestniczących w przygotowaniu osób do wykonywania zawodu lekarza oraz w szkoleniu osób wykonujących zawód medyczny jest udostępniana tym osobom wyłącznie w zakresie niezbędnym do realizacji celów dydaktycznych. (Podstawa prawna – art. 26 sek. 3a ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta).

Osoby te zobowiązane są do zachowania w tajemnicy informacji zawartych w dokumentacji medycznej, również po śmierci pacjenta.

## **XVII. Udostępnianie dokumentacji medycznej do celów badawczych**

Dokumentacja medyczna do celów naukowych jest udostępniana uczelniom lub instytutom badawczym, na ich wniosek, za zgodą Dyrektora Szpitala. Dokumentację można udostępnić bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której ona dotyczy. (Podstawa prawna – art. 26 sek. 4 ustawy z dnia 6 listopada 2008 r. o pacjentach prawa i prawa Pacjenta Rzecznik Praw Obywatelskich)

Studenci/Praktykanci nie są upoważnieni (uprawnieni) do udzielania informacji o stanie zdrowia pacjentów oraz udostępniania dokumentacji medycznej.

## **XVIII. Podstawa prawna**

- 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 95/45/WE (ogólne rozporządzenie o ochronie danych osobowych).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).
- Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (t.j. Dz. U. z 2025 r. poz. 450).



**SZPITAL KLINICZNY**  
**IM. KAROLA JONSCHERA**  
**Uniwersytetu Medycznego**  
**im. Karola Marcinkowskiego**  
W POZNANIU

## OCHRONA DANYCH OSOBOWYCH

### MATERIAŁ DLA STAŻYSTÓW, STUDENTÓW, PRAKTYKANTÓW I WOŁONTARIUSZY

Wydanie 1 z dnia 23.05.2025 r.

- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581).
- Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej (t.j. Dz. U. z 2025 r. poz. 515).
- Dokumenty wewnętrzne z zakresu ochrony danych osobowych.

Opracował: *Inspektor Ochrony Danych*