SZKOLENIE
RODO

Czym jest RODO?

RODO chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
RODO w sposób kompleksowy reguluje kwestie ochrony danych osobowych i jest stosowane od 25 maja 2018 r. we wszystkich państwach członkowskich UE.

PODSTAWA PRAWNA

RODO oznacza:
Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).
Aktem prawnym, który uzupełnia regulacje w zakresie ochrony danych osobowych, jest ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (tekst jednolity Dz.U.2019.1781 z dnia 2019.09.19). Ustawa nie powiela przepisów RODO, a stanowi jedynie dopełnienie RODO, w zakresie w jakim ustawodawca unijny dopuścił doprecyzowanie pewnych zagadnień na gruncie prawa krajowego.

Dane osobowe

co to znaczy?

Dane osobowe to wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. 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) lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
Definicja – art. 4 pkt 1 RODO

rodzaje danych osobowych

DANE OSOBOWE ZWYKŁE

- imię i nazwisko
- wykształcenie
- nr i seria dowodu osobistego
- PESEL
- płeć
- adres e-mail
- adres zamieszkania
- nr telefonu
- login internetowy

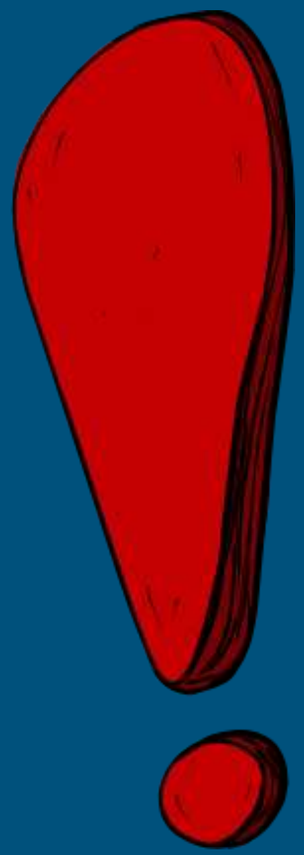
DANE OSOBOWE WRAŻLIWE

- przynależność do związków zawodowych
- przekonania religijne lub światopoglądowe
- dane ujawniające pochodzenie rasowe lub etniczne
- poglądy polityczne
- seksualności lub orientacji seksualnej
- dane genetyczne
- dane dotyczące zdrowia
- dane biometryczne

Co oznacza przetwarzanie danych osobowych?

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

- zbieranie,
- utrwalanie,
- organizowanie
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie,
- pobieranie,
- przeglądanie,
- wykorzystywanie,
- ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie,
- dopasowywanie lub łączenie,
- ograniczanie,
- usuwanie lub niszczenie.



Katalog czynności, które mogą składać się na przetwarzanie danych osobowych, ma charakter przykładowy, jest katalogiem otwartym – należy przyjąć, iż przetwarzanie danych osobowych to każda czynność, którą wykonujemy z wykorzystaniem danych osobowych (wszelkie operacje wykonywane na danych osobowych) w celu osiągnięcia określonego celu przetwarzania.

W jaki sposób IMW przetwarza dane osobowe?

TRADYCYJNIE
(dokumentacja papierowa)
zalicza się do niej:

- dokumentację medyczną,
- wyniki badań,
- akta osobowe pracowników,
- dokumenty wydrukowane zawierające dane osobowe.

Przykładowe czynności przetwarzania dokumentacji papierowej:

- wypełnienie ,
- przechowywanie,
- przeglądanie,
- kopiowanie,
- organizowanie,
- udostępnianie,
- niszczenie.

W jaki sposób IMW przetwarza dane osobowe?

ELEKTRONICZNIE
(w systemach informatycznych)

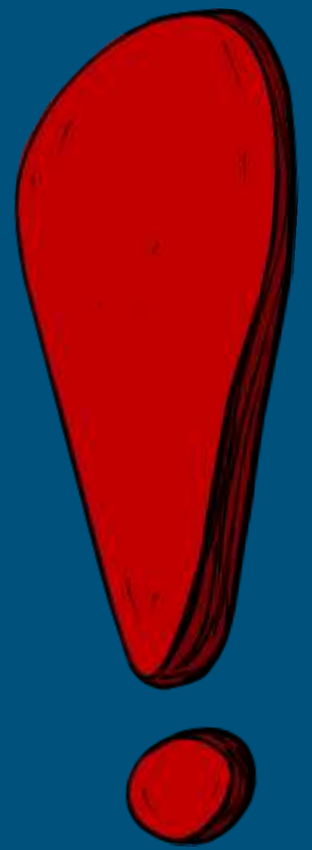
- dane pacjentów w systemie Ks-Medis, Ks-Somed (elektroniczna dokumentacja medyczna),
- dane pacjentów zapisane w pamięci urządzeń/aparatury medycznej.
- dane pracowników oraz zleceniobiorców w systemie Ks-ZZL
- dane kontrahentów, współpracowników w systemie Ks- FK

Przykładowe czynności przetwarzania dokumentacji elektronicznej :

- wypełnienie,
- przechowywanie,
- przeglądanie,
- kopiowanie,
- organizowanie,
- udostępnianie,
- niszczenie.

DANE OSOBOWE SĄ OBJĘTE OCHRONĄ BEZ WZGLĘDU NA TO, W JAKI SPOSÓB SĄ PRZETWARZANE.

Nie ma znaczenia w jaki sposób są używane lub przechowywane – czy wykorzystujemy najnowszy system informatyczny czy dokumenty papierowe w segregatorach/teczkach, kartoteki, księgi, wykazy, ewidencje - w każdym z tych przypadków przetwarzanie danych podlega wymogom RODO.



Kto jest Administratorem danych przetwarzanych w IMW?

Pojęcie „Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.
[Definicja – art. 4 pkt 7 RODO]

Kto jest Administratorem danych przetwarzanych w IMW?

Administratorem danych przetwarzanych w IMW jest:
INSTYTUT MEDYCYNY WSI im. W. Chodźki ul. Jaczewskiego 2, 20-090 Lublin
Administratora danych reprezentuje Dyrektor Instytutu dr Jerzy Kuliński.
Administrator danych ustala cele i sposoby przetwarzania danych osobowych, a także zobowiązany jest – uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia – wdrożyć odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych odbywało się zgodnie z RODO.

INSTYTUT
MEDYCYNY
WSI

Kto to jest Inspektor Ochrony Danych (IOD)?

Inspektor Ochrony Danych (IOD) to wyznaczona przez Dyrektora osoba, która nadzoruje przestrzeganie zasad ochrony danych osobowych w IMW.

W IMW na Inspektora Ochrony Danych została wyznaczona

Pani Małgorzata Chudaś (od 03.03.2025).

Dane kontaktowe IOD: adres e-mail: iod@imw.lublin.pl, bezpośredni nr telefonu 81 7184461, wewnętrzny nr telefonu 461, miejsce pracy: Dział Kadr i Płac.

Inspektor Ochrony Danych

Osoby, których dane są przetwarzane w IMW, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego. Inspektor Ochrony Danych nie może otrzymywać instrukcji dotyczących wykonywania przez niego zadań określonych w art. 39 RODO.
[Podstawa prawna – art. 37 i 38 RODO]

Jak należy zabezpieczać dane osobowe?

RODO nie wskazuje konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający lecz wprowadza tzw. podejście oparte na ryzyku.

Przykładowe środki zabezpieczenia danych osobowych to:

- pseudonimizacja i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

ŚRODKI OCHRONY DANYCH OSOBOWYCH STOSOWANE W IMW

TECHNICZNE

ORGANIZACYJNE

ŚRODKI OCHRONY DANYCH OSOBOWYCH STOSOWANE W IMW

Techniczne i organizacyjne środki ochrony danych osobowych, to środki, które administrator lub podmiot przetwarzający dane stosuje w celu zapewnienia bezpieczeństwa danych osobowych, adekwatne do przeprowadzonej oceny ryzyka przetwarzania danych osobowych.

Przykładowe środki organizacyjne i techniczne stosowane w IMW

wdrożone polityki ochrony danych	regulaminy	instrukcje	procedury
upoważnienia do przetwarzania danych osobowych	stosowanie urządzeń zabezpieczających sieć typu firewall	stosowanie systemu kopii zapasowych	umowy o zachowaniu poufności
stosowanie oprogramowania antywirusowego	szkolenia dla osób przetwarzających dane osobowe	stosowanie loginu i hasła (systemu uwierzytelniania	pseudonimizacja

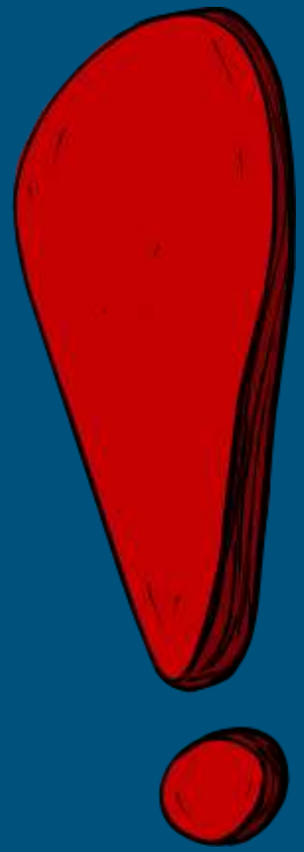
Jakie dane IMW przetwarza ?

Dane osobowe zwykłe – niezbędne w procesie rekrutacji, zatrudnienia, zawierania wszelkich rodzajów umów oraz kontraktów.

Dane dotyczące zdrowia- wrażliwe to wszystkie dane o stanie zdrowia osoby, której dane dotyczą. Dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej. Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane osoby fizycznej, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą.

Jakie dane IMW przetwarza ?

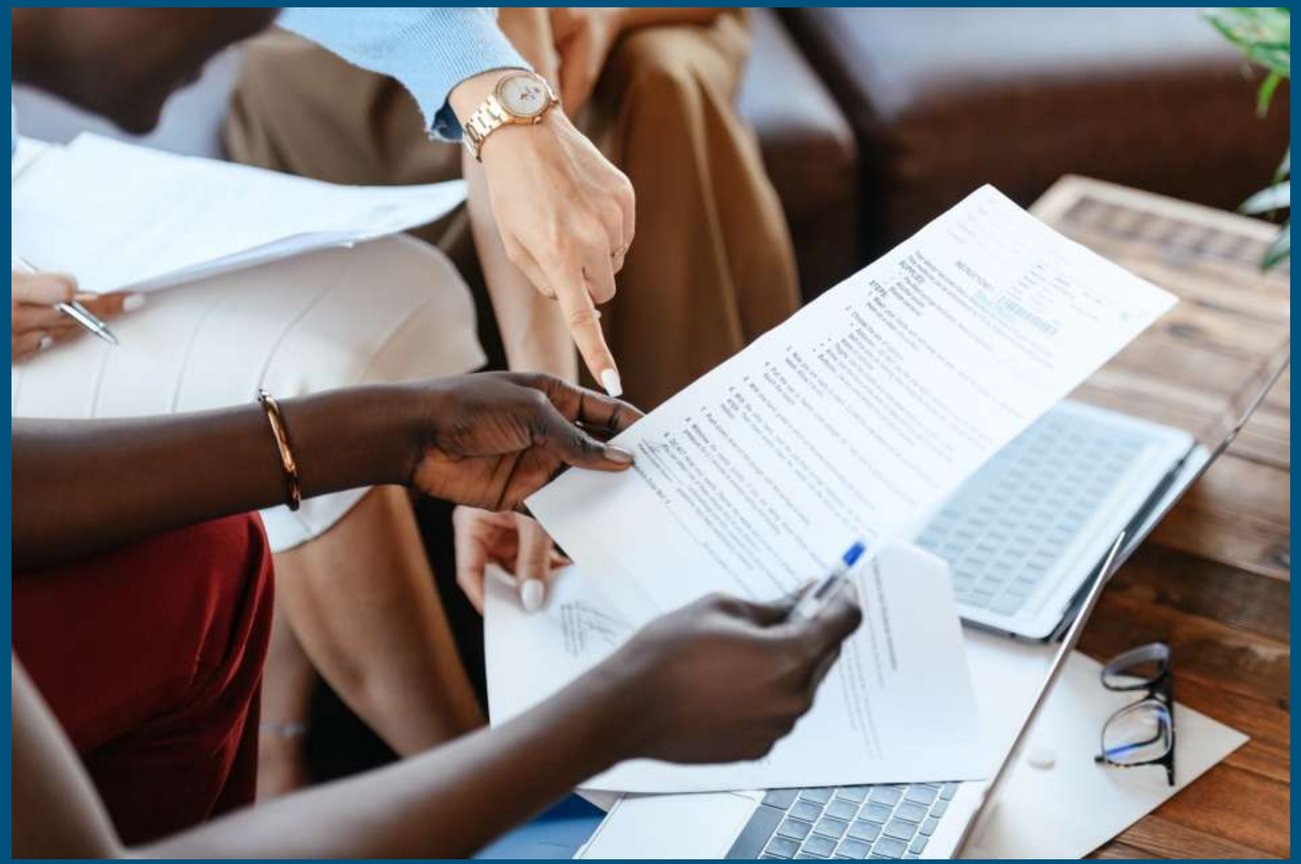
- **Dane dotyczące zdrowia pacjentów IMW, w tym dane zawarte w dokumentacji medycznej, należą do szczególnych kategorii danych osobowych i podlegają szczególnej ochronie prawnej.**



Udostępnianie danych osobowych

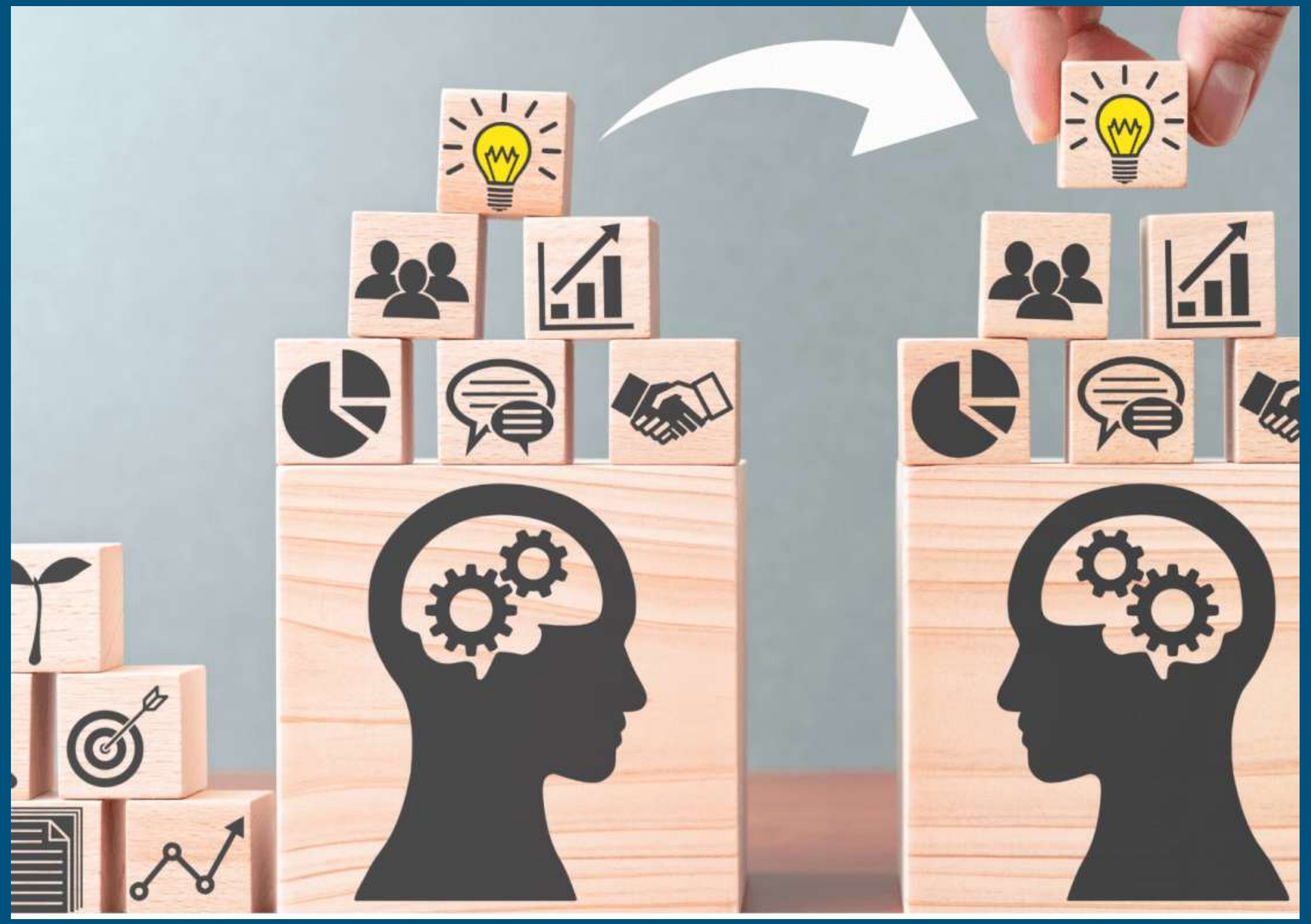
Dokumentację medyczną podmiot udzielający świadczeń zdrowotnych udostępnia:

- pacjentowi;
- przedstawicielowi ustawowemu pacjenta;
- osobie upoważnionej przez pacjenta.



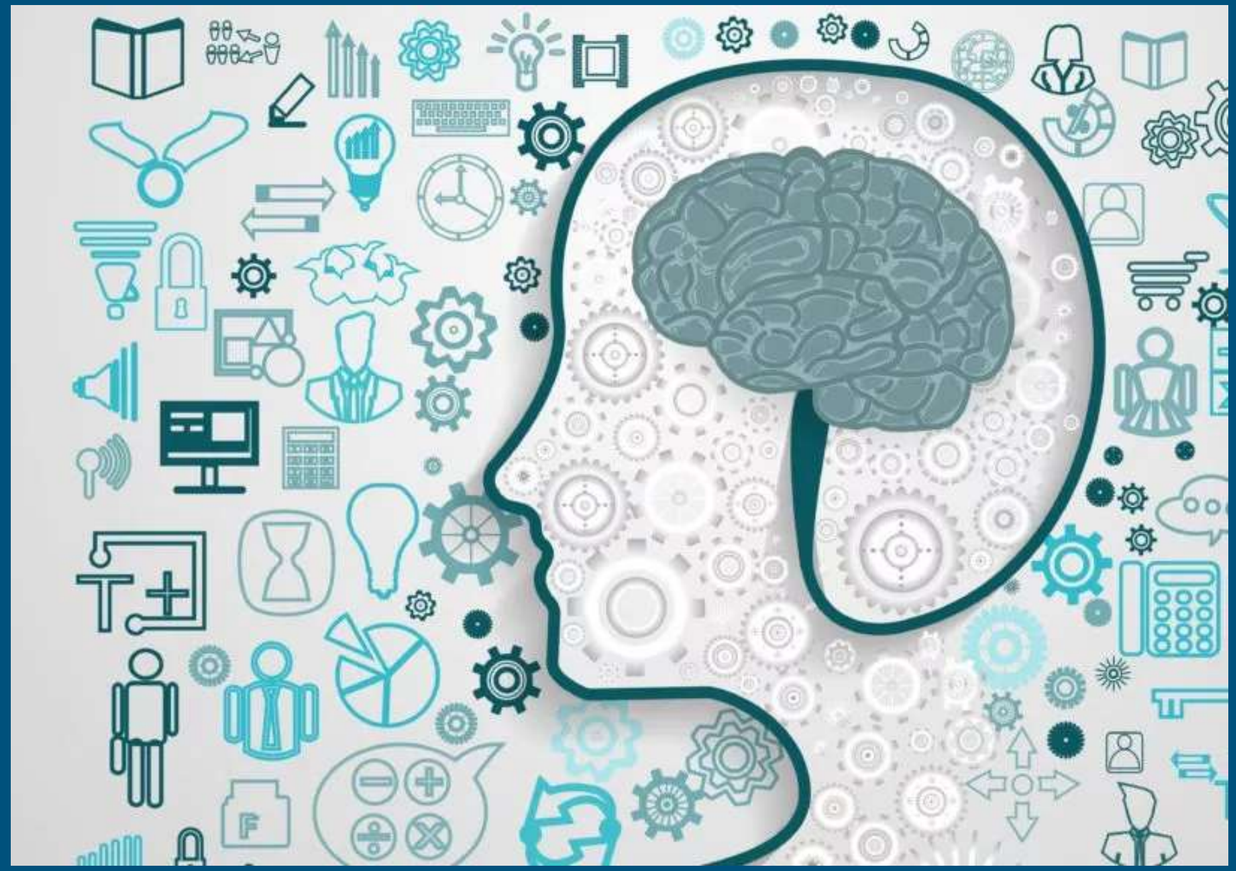
Udostępnianie danych osobowych

Poza pacjentem oraz osobami mającymi jego upoważnienie, prawo dostępu do dokumentacji mogą uzyskać także inne osoby lub podmioty, jeżeli ich uprawnienie wynika wprost z przepisów prawa. Art. 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta enumeratywnie wskazuje krąg uprawnionych, którym podmiot udzielający świadczeń zdrowotnych może udostępnić dokumentację medyczną pacjenta.



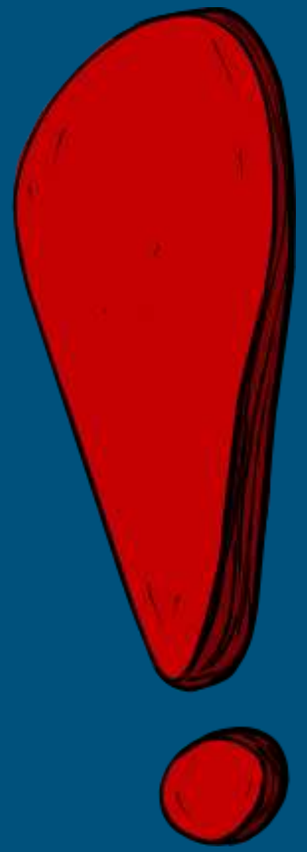
Dokumentacja medyczna może być (pod szczególnymi warunkami) udostępniana do:

- celów dydaktycznych;
- celów naukowych.



Naruszenie ochrony danych osobowych, co to znaczy?

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
[Definicja – art. 4 pkt 12 RODO]



Rodzaje naruszeń

Naruszenie poufności polega na ujawnieniu danych osobowej nieuprawnionej osobie.

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

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

Przykładami naruszeń mogą być:

Udostępnienie dokumentacji medycznej lub informacji o stanie zdrowia osobom nieuprawnionym.

Umożliwienie wglądu do dokumentacji medycznej osobom nieuprawnionym.

Pozostawienie dokumentów zawierających dane osobowe, w tym dokumentacji medycznej w miejscach bez nadzoru.

Wyrzucenie dokumentów zawierających dane osobowe do kosza. Wszystkie zbędne dokumenty muszą być niezwłocznie niszczone w niszczarkach w sposób uniemożliwiający ich odczytanie.

Udostępnienie identyfikatora i hasła do systemu informatycznego innej osobie.

Kradzież dokumentów, nośników, sprzętu komputerowego, urządzeń.

Zniszczenia fizyczne (pożar, zalanie, zniszczenie dokumentów/nośników lub urządzeń)

Zapisywanie danych na prywatnych nośnikach

Wyniesienie dokumentacji medycznej przez pracownika/zleceniobiorcę poza IMW.

Co zrobić w przypadku podejrzenia/stwierdzenia naruszenia ochrony danych osobowych?

- niezwłocznie zgłosić IOD podejrzenie/stwierdzenie naruszenia ochrony danych osobowych.
- powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia, jednakże np. w przypadku znalezienia na terenie Szpitala niezabezpieczonych dokumentów zawierających dane osobowe, w tym dokumentacji medycznej, jak również jej kopii, wydruków, itp., należy je zabezpieczyć, aby informacje zawarte w dokumentacji nie zostały ujawnione osobom nieuprawnionym.
- współpracować z IOD w celu wyjaśnienia wszystkich okoliczności naruszenia ochrony danych osobowych.

Pamiętaj o 4 zasadach !!!

ZASADA CZYSTEGO BIURKA

Polega na przechowywaniu dokumentów poza zasięgiem wzroku i dłoni osób postronnych oraz niepozostawianiu ich bez nadzoru.

Pamiętaj o 4 zasadach !!!

ZASADA CZYSTEGO EKRANU

Zasada czystego ekranu polega
na uniemożliwieniu osobom
nieupoważnionym dostępu
do wyświetlanych na monitorze informacji.

Pamiętaj o 4 zasadach !!!

ZASADA CZYSTEGO KOSZA

Zasada czystego kosza polega
na niszczeniu dokumentów,
na których znajdują się poufne informacje,
w taki sposób, aby ich odczytanie było
niemożliwe

Pamiętaj o 4 zasadach !!!

ZASADA CZYSTEGO WYDRUKU

Zasada czystego wydruku polega na zabieraniu z urządzeń drukujących dokumentów zaraz po ich wydrukowaniu / skserowaniu / zeskanowaniu.

STOSUJ ZASADY CYBERBEZPIECZEŃSTWA

Chroń dane osobowe pracowników i pacjentów

Chroń swoje dane osobowe

Zawsze ustawiaj silne hasła

Nie zapominaj o wylogowaniu się

Nie odwiedzaj podejrzanych stron

Uważaj na wiadomości i linki nieznanego pochodzenia

ODPOWIEDZIALNOŚĆ KARNA

Pracownicy/Zleceniobiorcy naruszający zasady bezpieczeństwa danych osobowych mogą ponosić sankcje karne na podstawie przepisów o ochronie danych osobowych.

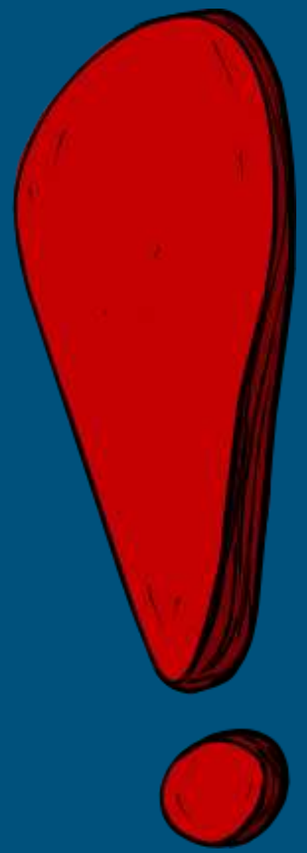
Osoby niebędące pracownikami IMW, ponoszą wobec IMW odpowiedzialność odszkodowawczą na zasadach określonych w kodeksie cywilnym.

Pracownicy/Zleceniobiorcy są zobowiązani w szczególności do przestrzegania zasad ochrony danych osobowych obowiązujących w IMW wynikających z przepisów prawa i regulacji wewnętrznych, w tym:

- zachowania należytej staranności w celu ochrony danych osobowych;
- zapewnienia bezpieczeństwa przetwarzania danych osobowych, w szczególności poprzez ich ochronę przed nieuprawnionym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem, w tym stosowanie wymaganych środków technicznych i organizacyjnych zapewniających ochronę danych osobowych;
- zachowania w tajemnicy danych osobowych uzyskanych w związku z procesem leczenia na terenie IMW (bez względu na sposób ich uzyskania – pisemny, elektroniczny, ustny), zarówno w trakcie leczenia jak również po jego zakończeniu. Zobowiązanie do zachowania tajemnicy danych dotyczących pacjenta ma zastosowanie również po śmierci pacjenta;
- przeciwdziałania naruszeniom ochrony danych osobowych oraz zgłaszanie przypadków naruszenia lub podejrzenia naruszenia ochrony danych.

PRAWA I OBOWIĄZKI

Pracownicy oraz Zleceniobiorcy są zobowiązani do przestrzegania przepisów prawa, regulacji wewnętrznych oraz zarządzeń i komunikatów wydanych przez Dyrektora IMW dotyczących zabezpieczenia danych osobowych, w tym danych zawartych w dokumentacji medycznej.



Niniejszy materiał szkoleniowy został przygotowany w związku z realizacją zadań Inspektora Ochrony Danych wynikających z zapisów art. 39 ust. 1 pkt b) RODO – szkolenia osób uczestniczących w operacjach przetwarzania danych osobowych.

Materiał szkoleniowy nie stanowi wykładni prawa w zakresie ochrony danych osobowych, a posiada wyłącznie charakter informacyjno-szkoleniowy.

Małgorzata Chudaś – Inspektor Ochrony Danych

Dziękuję za uwagę