SZPITAL POWIATOWY W RADOMSKU

OCHRONA DANYCH OSOBOWYCH

REGULACJE PRAWNE DOTYCZĄCE DANYCH OSOBOWYCH

- 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 95/46/WE (ogólne rozporządzenie o ochronie danych) zwane „RODO”.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.

POLITYKA OCHRONY DANYCH OSOBOWYCH

- W celu zapewnienia, że dane osobowe w Szpitalu Powiatowym w Radomsku są przetwarzane zgodnie z obowiązującymi przepisami prawa, wprowadzona została polityka ochrony danych osobowych.
- Zarządzenie nr 51/2025 Dyrektora Szpitala Powiatowego w Radomsku z dnia 02.04.2025 roku w sprawie wdrożenia Polityki Ochrony Danych Osobowych w Szpitalu Powiatowym w Radomsku.
- Każdy pracownik bez względu na formę zatrudnienia zobowiązany jest zapoznać się z Polityką Ochrony Danych Osobowych.

DANE OSOBOWE

to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną.

Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak:

- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji,
- identyfikator internetowy lub
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Dane osobowe stanowią informacje w formie komunikatów, niezależnie od sposobu ich utrwalenia i zawsze podlegają ochronie.

Forma papierowa	Forma elektroniczna	Zapisy rejestratorów
• akta osobowe • teczki • dokumenty • wydruki	• programy • systemy informatyczne • pliki • foldery	• monitoring • centrala telefoniczna (nagrywanie rozmów telefonicznych)

DANE OSOBOWE DZIELĄ SIĘ GŁÓWNIE NA:

Dane tzw. zwykłe

- imię, nazwisko,
- adres zamieszkania,
- data i miejsce urodzenia,
- numer telefonu,
- wykonywany zawód,
- wizerunek,
- adres e-mail i inne dane identyfikujące.

PESEL* - podlega szczególnej ochronie na podstawie komunikatu prezesa UODO.

Dane szczególnej kategorii wymienione w art. 9 RODO ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczące zdrowia,
- seksualności lub orientacji seksualnej tej osoby.

Dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa wymienione w art. 10 rozporządzenia np. informacja z rejestru o skazaniu kandydata do pracy za przestępstwa na tle seksualnym, informacja z Krajowego Rejestru Karnego.

PRZETWARZANIE DANYCH ZWYKŁYCH

Art. 6 ust. 1 RODO: Przetwarzanie tzw. „zwykłych" danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:

- osoba której dane dotyczą **wyraziła zgodę** na przetwarzanie;
- przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego** ciążącego na administratorze;
- przetwarzanie jest **niezbędne do ochrony żywotnych interesów** osoby, której dane dotyczą lub innej osoby fizycznej;
- przetwarzanie jest **niezbędne do wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych interesów** realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba której dane dotyczą jest dzieckiem.

PRZETWARZANIE DANYCH SZCZEGÓLNEJ KATEGORII

Art. 9 ust. 1 RODO [mówiący o zakazie przetwarzania danych szczególnej kategorii] nie ma zastosowania, jeśli:

1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych, chyba że prawo UE lub krajowe wyklucza możliwość cofnięcia zgody,;
2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą w dziedzinie prawa pracy i zabezpieczenia społecznego oraz ochrony socjalnej, w zakresie dozwolonym prawem UE lub państwa członkowskiego;
3. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
4. przetwarzanie jest dokonywane przez fundację, stowarzyszenie lub inny podmiot non-profit, o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem, że przetwarzanie dotyczy wyłącznie członków tego podmiotu lub osób regularnie utrzymujących z nim kontakt w związku z jego celami i że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
5. przetwarzanie dotyczy danych osobowych, które osoba, której dane dotyczą, sama upubliczniła;
6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

PRZETWARZANIE DANYCH SZCZEGÓLNEJ KATEGORII (c.d.)

Art. 9 ust. 1 RODO [mówiący o zakazie przetwarzania danych szczególnej kategorii] nie ma zastosowania, jeśli:

7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
8. przetwarzanie jest **niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy**, oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub leczenia, lub zarządzania systemami i usługami opieki zdrowotnej i pomocy społecznej na podstawie prawa UE lub państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;
9. przetwarzanie jest **niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego**, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO.

Szpital, reprezentowany przez swojego dyrektora, przetwarza dane osobowe na podstawie przepisów odnoszących do funkcjonowania jednostek ochrony zdrowia i dedykowanych aktów prawnych.

Przede wszystkim są to m.in.:

- Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta;
- Ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej;
- Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych;
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia;
- Ustawa z dnia 27 października 2017 r. o podstawowej opiece zdrowotnej;
- Ustawa z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty.

Podstawowe zasady ochrony danych osobowych opierają się na Rozporządzeniu Rady Europejskiej (RODO), jednak szczegółowe zasady określają ustawy dotyczące konkretnej dziedziny, np. dane, które pracodawca może zebrać od pracownika wskazuje dokładnie Kodeks Pracy.

PRZETWARZANIE DANYCH OSOBOWYCH

oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany

PRZETWARZANIE	ZBIERANIE	UTRWALANIE	ORGANIOWANIE
PORZĄDKOWANIE	ADAPTOWANIE LUB MODYFIKOWANIE	POBIERANIE	UJAWNIANIE POPRZEZ PRZESŁANIE
PRZEGLĄDANIE	PRZECHOWYWANIE	DOPASOWYWANIE LUB ŁĄCZENIE	ROZPOWSZECHNIANIE LUB INNEGO RODZAJU UDOSTĘPNIANIE
WYKORZYSTYWANIE	OGRANICZANIE	ARCHIWIZOWANIE	USUWANIE LUB NISZCZENIE

ADMINISTRATOR DANYCH

Administratorem może być osoba fizyczna, osoba prawna, organ publiczny, jednostka organizacyjna i inne podmioty, które decydują o celach i sposobach przetwarzania danych.

Administratorem danych osobowych pacjentów, pracowników, kontrahentów, stażystów w Szpitalu Powiatowym w Radomsku jest **dyrektor szpitala**.

Administrator:

- decyduje, jakie dane pacjentów i pracowników są przetwarzane,
- określa cele przetwarzania (np. leczenie, prowadzenie dokumentacji medycznej, pracowniczej, rozliczenia z NFZ),
- zapewnia zgodność z przepisami o ochronie danych,
- powołuje Inspektora Ochrony Danych (IOD), który nadzoruje przestrzeganie RODO.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Administrator jest odpowiedzialny za przestrzeganie zasad i musi być w stanie wykazać ich przestrzeganie

(„rozliczalność”)

1. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ***(„zgodność z prawem, rzetelność i przejrzystość”)***
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami ***(„ograniczenie celu”)***
3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ***(„minimalizacja danych”)***
4. prawidłowe i w razie potrzeby uaktualniane **(„prawidłowość”)**
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane **(„ograniczenie przechowywania”)**
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych **(„integralność i poufność”)**

Szpital zobowiązany jest do przestrzegania zasad ochrony danych osobowych, w tym m.in. do:

- Spełnienia względem osób, których dane dotyczą, obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO (tzw. klauzule informacyjne o przetwarzaniu danych osobowych).
- Respektowania prawa osób, których dane są przetwarzane.
- Zabezpieczenia danych osobowych przez zastosowanie odpowiednich środków technicznych i organizacyjnych, tak aby dane te nie były udostępniane osobom nieupoważnionym oraz aby dane te były chronione przed zniszczeniem albo utratą.

OBOWIĄZEK INFORMACYJNY

prawny wymóg nałożony na administratora danych osobowych, zobowiązujący do poinformowania osób, których dane dotyczą, o sposobie przetwarzania ich danych.

Obowiązek informacyjny spełniany jest w momencie pozyskania danych osobowych poprzez przekazanie klauzuli informacyjnej – na papierze, tablicy informacyjnej lub elektronicznie.

- Art. 13 RODO: dotyczy sytuacji, w których administrator danych osobowych pozyskuje te dane od osoby, której dane osobowe dotyczą;
- Art. 14 RODO: dotyczy sytuacji, w których administrator danych osobowych pozyskuje te dane z innego źródła niż bezpośrednio od osoby, której one dotyczą.

Klauzule informacyjne o przetwarzaniu danych osobowych są dostępne w siedzibie Szpitala oraz na stronie **https://radomsko.bip.gov.pl/rodo/rodo.html**

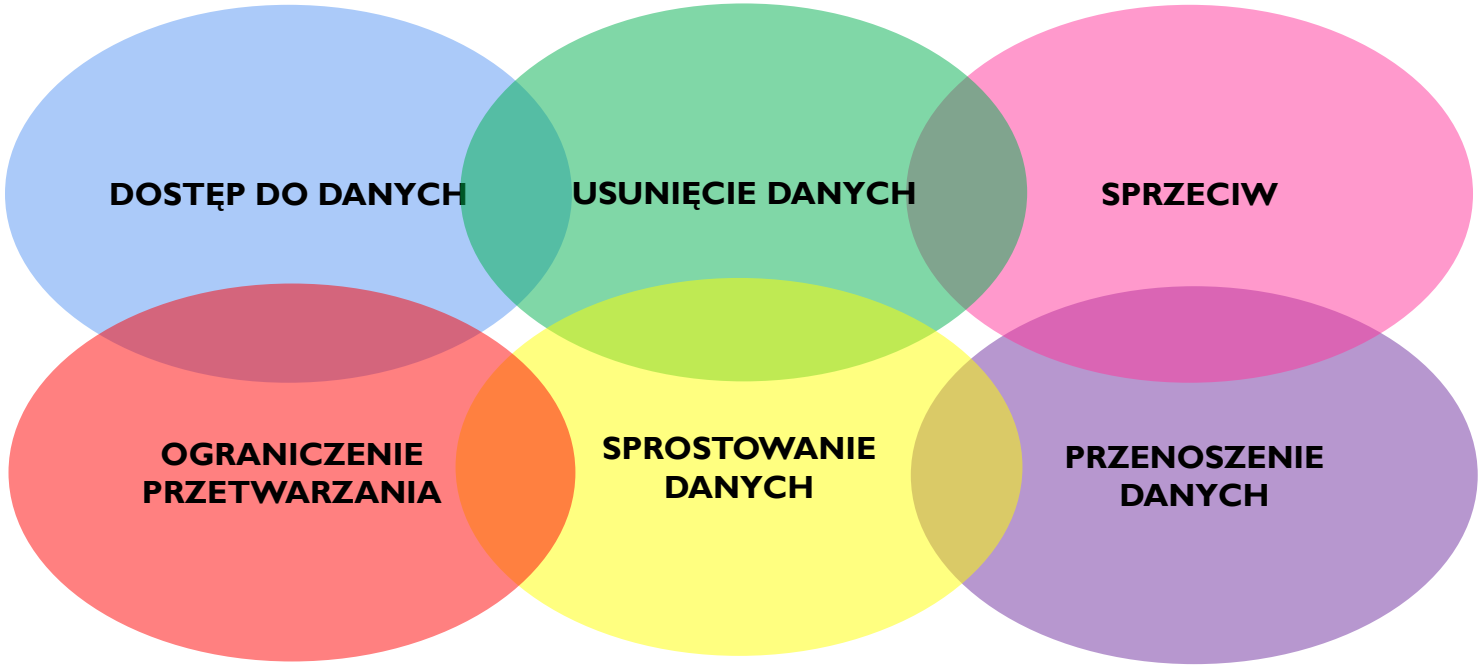
ŚRODKI TECHNICZNE I ORGANIZACYJNE

zabezpieczające dane osobowe przetwarzane przez Szpital.

Środki techniczne	Środki organizacyjne
Szyfrowanie danych	Wdrożona polityka bezpieczeństwa informacji
Pseudonimizacja danych	Wyznaczono IOD
Backup danych	Okresowe szkolenia dla pracowników
Kontrola dostępu do pomieszczeń, systemów informatycznych	Polityka kluczy
Zabezpieczenia fizyczne i logiczne sieci oraz systemu informatycznego	Zarządzanie upoważnieniami do danych
Zabezpieczenia obszaru przetwarzania danych (np. alarm, monitoring wizyjny, zamykane drzwi)	Zasada czystego biurka i ekranu

PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Według RODO każdy ma prawo do:



Niektóre prawa mogą być ograniczone na podstawie przepisów prawnych.

Na przykład: pracownik żąda aby pracodawca usunął jego dane osobowe. Nie jest możliwa realizacja żądania, ponieważ prawo zobowiązuje pracodawcę do przechowywania teczek osobowych przez np. 50 lat od zakończenia stosunku pracy.

ORGAN NADZORCZY

Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza przepisy RODO.

Właściwym organem nadzorczym jest Prezes Urzędu Ochrony Danych Osobowych.

URZĄD OCHRONY DANYCH OSOBOWYCH

NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

to 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.

Rodzaje naruszeń ochrony danych osobowych:

- ***Utrata danych*** – przypadkowa utrata lub usunięcie danych osobowych, które mogą uniemożliwić ich odzyskanie (np. przypadkowe usunięcie plików, zagubienie lub kradzież nośnika z danymi),
- ***Nieuprawniony dostęp do danych*** – osoba nieuprawniona (np. pracownik bez odpowiednich uprawnień) uzyskuje dostęp do danych osobowych.
- ***Nieuprawnione ujawnienie danych*** – dane osobowe zostają ujawnione osobom lub podmiotom, które nie mają prawa do ich przetwarzania (np. przez wysyłanie e-maila do niewłaściwej osoby, udostępnienie dokumentacji medycznej osobie nieupoważnionej).
- ***Modyfikacja danych*** – dane osobowe zostają nieautoryzowanie zmienione lub zmodyfikowane, np. przez edytowanie ważnych informacji osobowych.
- ***Złośliwe oprogramowanie*** – wprowadzenie złośliwego oprogramowania (np. wirusa, ransomware), które powoduje utratę lub kradzież danych osobowych.
- ***Naruszenie systemów informatycznych*** – atak hakerski na systemy komputerowe, w wyniku którego dane osobowe zostają skradzione, zniszczone lub zmienione.

ZGŁASZANIE NARUSZEŃ DANYCH OSOBOWYCH

Kontakt do IOD:
iodo@szpital.biz.pl

Sekcja Informatyki:

tel. 502 021 470

Każdy pracownik, który stwierdzi możliwość wystąpienia naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

Każdy pracownik lub współpracownik, bez względu na to, czy zostało mu wydane upoważnienie do przetwarzania danych osobowych, który podejmie informację lub stwierdzi incydent bezpieczeństwa informacji i/lub naruszenie ochrony danych osobowych i/lub cyberbezpieczeństwa zobowiązany jest do:

1. podjęcia czynności niezbędnych do powstrzymania skutków naruszenia,
2. podjęcia natychmiastowych działań zabezpieczających materiał dowodowy, umożliwiający ustalenie przyczyn oraz skutki naruszenia (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.)
3. zabezpieczenia miejsca zdarzenia w ramach posiadanych kompetencji,
4. natychmiastowego skutecznego zgłoszenia incydentu do bezpośredniego przełożonego, który informuje Inspektora Ochrony Danych, Administratora danych i pracowników sekcji Informatyki (w sytuacji, kiedy incydent dotyczy również systemów informatycznych).

CZAS ZGŁOSZENIA

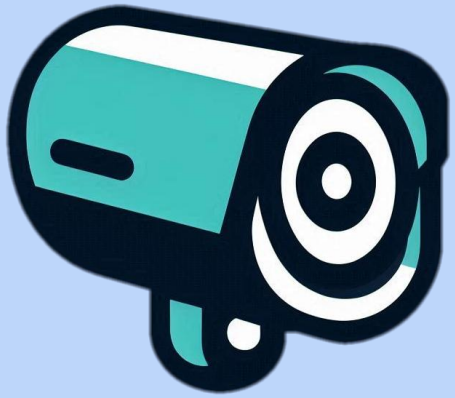
RODO wprowadza obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego w ciągu **72h,** dlatego ważny jest czas.

Administrator danych decyduje o tym, czy zgłosi naruszenie. Zgłasza się tylko te naruszenia, które mogą spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (np. wyciek danych pacjentów).

Dla prawidłowej reakcji na naruszenie, każdorazowo powinno się wezwać do pomocy Inspektora Ochrony Danych.

BEZPIECZEŃSTWO DANYCH W PRAKTYCE

MONITORING



- W Szpitalu Powiatowym w Radomsku prowadzony jest monitoring wizyjny w celu zapewnienia bezpieczeństwa i porządku publicznego, ochrony zdrowia, dóbr i mienia osób przebywających na terenie Szpitala.
- Obszar objęty monitoringiem jest oznaczony.

Regulamin monitoringu wizyjnego w Szpitalu Powiatowym w Radomsku dostępny jest na stronie internetowej Szpitala.

ODPOWIEDZIALNOŚĆ ZA ZASOBY/AKTYWA

- Każdy pracownik odpowiada za powierzone mu zasoby/aktywa (sprzęt informatyczny, oprogramowanie, dokumentację papierową itp.).
- Każdy pracownik zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieuprawnionych oraz przed ich zniszczeniem. Zobowiązany jest do zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośnika informacji.
- Zasoby/aktywa te przeznaczone są wyłącznie do realizacji celów służbowych. Wykorzystanie ich do celów prywatnych jest zabronione.

UPOWAŻNIENIE I UPRAWNIENIE DO PRZETWARZANIA DANYCH

- Każdy pracownik, który przetwarza dane osobowe musi posiadać imienne upoważnienie nadane przez Administratora do przetwarzania danych osobowych.
- Dostęp do systemu informatycznego służącego do przetwarzania informacji, w tym danych osobowych może uzyskać wyłącznie osoba pisemnie upoważniona do przetwarzania danych przez Administratora.
- Każdy pracownik zobowiązany jest do pracy w systemach teleinformatycznych na przypisanych jemu kontach. Zabronione jest udostępnianie dostępu do konta osobom trzecim.

Procedura nadawania uprawnień do przetwarzania danych osobowych w systemie informatycznym - BI-2-1-U

ZASADA POUFNOŚĆ

Każda pracownik dopuszczony do przetwarzania danych osobowych jest zobowiązany do:

- przestrzegania zasad i procedur bezpieczeństwa informacji oraz danych osobowych w Szpitalu,
- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych zadaniach przez Administratora,
- zachowania w tajemnicy danych osobowych, do których ma lub będzie mieć dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- zgłaszania wszelkich podejrzeń o naruszeniu bezpieczeństwa danych osobowych przełożonemu lub IOD,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

TAJEMNICA ZAWODOWA

art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta;

art. 40 ustawy o zawodzie lekarza i lekarza dentysty;

art.. 21 ustawy o zawodach pielęgniarki i położnej;

art. 10 ust. 1 ustawy o Państwowym Ratownictwie Medycznym;

art. 2 ustawy o zawodzie fizjoterapeuty;

art. 35 ust. 1 ustawy o zawodzie farmaceuty;

art. 16 ust. 1 ustawy o medycynie laboratoryjnej;

art. 14 ust. 1ustawy o zawodzie psychologa i samorządzie zawodowym psychologów

Tajemnica zawodowa w zawodach medycznych to obowiązek zachowania w poufności informacji uzyskanych od pacjenta w związku z wykonywaniem zawodu.

Obejmuje ona zarówno dane dotyczące stanu zdrowia, jak i inne, osobiste informacje, które pracownik medyczny pozyskał podczas udzielania świadczeń.

- Zachowuj poufność nawet po ustaniu zatrudnienia.
- Nie rozmawiaj o pacjentach w miejscach publicznych (np. korytarz, stołówka).
- Zabezpieczaj dokumentację medyczną (fizyczną i elektroniczną).
- Zgłaszaj naruszenia bezpieczeństwa danych przełożonemu lub Inspektorowi Ochrony Danych.

Złamanie tajemnicy zawodowej może skutkować odpowiedzialnością dyscyplinarną, cywilną, a nawet karną.

ZASADA CZYSTEGO BIURKA

- Dokumenty przechowuj poza zasięgiem wzroku i dłoni osób postronnych w trakcie pracy, jak i po jej zakończeniu.
- Nie pozostawiaj dokumentów i nośników elektronicznych bez nadzoru.
- Pamiętaj! Aby w momencie przyjmowania interesanta, Twoje biurko było czyste od dokumentów. Będzie to zabezpieczenie przed celowym lub nieumyślnym np. zabraniem dokumentów wraz z tymi, po które przyszedł interesariusz.
- Na koniec dnia pracy chowaj wszystkie dokumenty i nośniki danych do szafek lub szuflad zamykanych na klucz.
- Nie pozostawiaj urządzeń bez nadzoru w stanie umożliwiającym korzystanie z nich.

„Czyste biurko” to nie tylko biurko, ale także szafki, tablice i półki w obrębie stanowiska pracy.

ZASADA CZYSTEGO EKRANU

- Ustawienie monitora nie może pozwalać na dostęp do informacji osobom do tego nieupoważnionych – sprawdź czy Twoje biurko stoi w odpowiedniej pozycji.
- Nie umożliwiaj dostępu osobom nieupoważnionym do informacji wyświetlanych na ekranie Twojego komputera służbowego.
- Przed odejściem od komputera, pamiętaj o zablokowaniu dostępu do urządzenia (np. klawisz funkcyjny + L).
- Wyłącz powiadomienia na ekranie (np. e-mail, komunikatory) podczas udostępniania ekranu innym użytkownikom (np. prezentacje, wspólna praca).

ZASADA CZYSTEGO KOSZA

- Dokumenty i nośniki zawierające dane chronione należy niszczyć w sposób uniemożliwiający ich odczytanie.
- Dokumenty zawierające dane osobowe i informacje poufne zawsze niszcz za pomocą niszczarek biurowych.
- Nigdy nie wyrzucaj dokumentów lub nośników danych do zwykłych koszy na śmieci przed ich odpowiednim zniszczeniem.

NISZCZENIA DANYCH

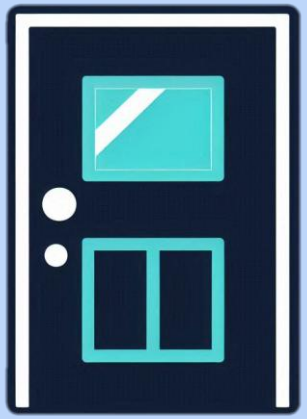
- Nośniki danych (np. dyski twarde, płyty CD/DVD) należy zniszczyć fizycznie lub wymazać dane przy użyciu specjalistycznego oprogramowania, aby uniemożliwić ich odzyskanie.
- Podczas procesu niszczenia danych upewnij się, że osoby nieupoważnione nie będą miały dostępu do niszczonych dokumentów ani nośników.

ZASADA CZYSTEGO DRUKU

- Nie pozostawiaj wydruku bez nadzoru na drukarce, ksero czy skanerze.
- Nie rób tzw. brudnopisu z wydruku z danymi osobowymi.
- Po użyciu skanera pamiętaj, aby usunąć plik z folderu sieciowego, aby uniknąć jego przypadkowego udostępnienia.
- Z urządzeń drukujących mogą korzystać tylko osoby upoważnione.
- Zwróć szczególną uwagę na drukowanie na urządzeniach sieciowych.

W przypadku problemów z drukowaniem skontaktuj się z sekcją Informatyki.

ZASADA ZAMKNIĘTEGO POMIESZCZENIA



- Nie zostawiaj niezabezpieczonego pomieszczenia bez obecności osoby uprawnionej.
- Nie zostawiaj klucza w drzwiach.
- Nie zostawiaj interesanta samego w pomieszczeniu, w którym przetwarzane są dane osobowe.
- Ostatnia wychodząca osoba z pomieszczenia zamyka okna i drzwi.
- Klucze do pomieszczeń należy zabezpieczyć zgodnie z obowiązującymi zasadami.

Uwaga!

Zasada nie dotyczą pomieszczeń ogólnodostępnych (np. rejestracja, recepcje, korytarze).

ZASADA BEZPIECZNEGO UŻYTKOWANIA HASEŁ

- Zachowaj hasło w tajemnicy – nie udostępniaj go osobom nieuprawnionym.
- Nie zapisuj haseł ani loginu i nie pozostawiaj ich w miejscu ogólnie dostępnym np. nie przyklejaj kartki z zapisanym hasłem na monitorze komputera.
- Wpisuj lub zmieniaj hasło bez obecności osób trzecich.
- Zachowaj hasło w tajemnicy także po utracie jego ważności.

Tworzenie hasła

- Min. 12 znaków – unikaj imion, nazwisk, dat urodzenia itp.
- Hasło nie może być identyczne z identyfikatorem użytkownika.

ZASADY KORZYSTANIA Z INTERNETU

- Unikaj odwiedzania nieznanych lub niezaufanych stron internetowych. Może to prowadzić do zainfekowania urządzenia złośliwym oprogramowaniem lub wycieku danych.
- Nie klikaj w podejrzane linki w wiadomościach e-mail, SMS-ach czy komunikatorach. Mogą one prowadzić do stron phishingowych lub złośliwego oprogramowania.
- Nie pobieraj nieznanych plików lub oprogramowania z Internetu, szczególnie z nieoficjalnych źródeł.
- Nie korzystaj ze służbowego Internetu do celów niezwiązanych z pracą, w tym do serfowania po mediach społecznościowych, grania w gry lub korzystania z serwisów streamingowych.
- Nie udostępniaj danych logowania ani nie wysyłaj informacji wrażliwych przez niezabezpieczone strony internetowe (np. bez protokołu HTTPS).
- W przypadku pracy zdalnej, zawsze używaj VPN do bezpiecznego łączenia się ze służbową siecią.
- Regularnie aktualizuj system operacyjny i oprogramowanie, w tym programy antywirusowe, aby chronić urządzenie przed zagrożeniami z sieci.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

- Zawsze sprawdzaj poprawność adresu e-mail, na który wysyłasz wiadomość.
- Sprawdzaj nadawcę wiadomości. Przyjrzyj się adresowi e-mail, z którego przyszła wiadomość.
- Wysyłasz wiadomości do wielu odbiorców? Użyj opcji „UDW" – do ukrytej wiadomości.
- Jeżeli przesyłasz pliki zawierające dane osobowe lub informacje poufne za pomocą poczty elektronicznej, używaj do tego bezpiecznego oprogramowania, pliki zabezpiecz hasłem, które podasz adresatowi w inny sposób – sprawdzając jego tożsamość.
- Nie korzystaj z firmowej poczty do wysyłania wiadomości niezwiązanych z pracą, w tym do działań reklamowych, prywatnych rozmów itp.
- Nie otwieraj podejrzanych załączników. Zachowaj ostrożność w otwieraniu załączników lub klikaniu w linki, szczególnie jeśli wiadomość pochodzi z nieznanych źródeł (może to być próba phishingu).
- Regularnie usuwaj niepotrzebne wiadomości i załączniki, aby uniknąć przeciążenia skrzynki i zapewnić jej bezpieczeństwo.

ZASADY KORZYSTANIA Z NOŚNIKÓW I URZĄDZEŃ MOBILNYCH

- Jeżeli korzystasz z nośników typu np. pendrive pamiętaj, aby korzystać tylko z urządzeń szyfrowanych.
- Zawsze przechowuj urządzenie w bezpiecznym miejscu.
- Jeżeli jesteś użytkownikiem urządzenia mobilnego, dbaj o jego bezpieczeństwo, zapewnij bezpieczny transport i przechowanie – nigdy nie udostępniaj go osobom nieupoważnionym.

ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

- Zawsze weryfikuj podstawę prawną udostępnianych danych.
- Przed udostępnieniem danych zawsze weryfikuj tożsamość osoby, której dane udostępniasz oraz jej uprawnienie do otrzymania żądanych danych.
- Udostępniaj dane z zachowaniem zasad RODO oraz przez bezpieczne kanały.
- Każde udostępnienie należy udokumentować.

Zasady udostępniania dokumentacji medycznej – procedura akredytacyjna PP 4.

ODPOWIEDZIALNOŚĆ ZA PRZETWARZANIE DANYCH OSOBOWYCH NIEZGODNIE Z PRAWEM

Pracownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami o ochronie danych osobowych oraz regulacjami wewnętrznymi obowiązującymi w Szpitalu, a także o zobowiązaniu się do ich przestrzegania oraz zachowania w tajemnicy danych pozyskanych w trakcie wykonywania obowiązków służbowych/zleceniobiorcy.

Nieuzasadnione zaniechanie obowiązków związanych z ochroną danych osobowych przez osobę zatrudnioną:

- na podstawie umowy o pracę traktowane będzie jako naruszenie obowiązków pracowniczych,
- na podstawie umowy zlecenia może zostać uznane za nienależyte wykonanie zlecenia.

W obu przypadkach może to skutkować wyciągnięciem konsekwencji służbowych lub rozwiązaniem współpracy.

ODPOWIEDZIALNOŚĆ

- Karna:

art. 107 Ustawy o ochronie danych osobowych - ten kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega: grzywnie, karze ograniczenia wolności, karze pozbawienia wolności do lat dwóch, w przypadkach szczególnych kategorii danych osobowych, do lat trzech.

- Cywilnoprawna:

art. 79 i art. 82 RODO w związku z rozdziałem 10 nowej ustawy o ochronie danych osobowych osoba, której prawa zostały naruszone będzie mogła żądać zaniechania naruszenia swych praw lub dopełnienia czynności niezbędnych do usunięcia jego skutków itd. oraz osoba która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, będzie miała prawo uzyskać, od administratora lub podmiotu przetwarzającego, odszkodowanie lub zadośćuczynienie za poniesioną szkodę.

- Administracyjna:

za nie przestrzeganie przepisów RODO Prezes UODO może nałożyć na jednostki administracji publicznej karę pieniężną do 100 000 złotych.

DANE INSPEKTORA OCHRONY DANYCH

Ewelina Garwolska

Inspektor Ochrony Danych

Szpital Powiatowy w Radomsku

e-mail: iodo@szpital.biz.pl

tel. 504 220 585