Ochrona danych osobowych – wspólna odpowiedzialność całego personelu!

Każdy pracownik szpitala, od rejestracji po lekarzy, jest zobowiązany do ochrony prywatności pacjentów.

Czym są dane osobowe?

Rozpoznawanie danych w codziennej praktyce szpitalnej

Dane identyfikujące bezpośrednio
Imię i nazwisko, PESEL, numer dowodu, adres zamieszkania, numer telefonu – pozwalają wskazać konkretną osobę.

Dane systemowe i kontaktowe
Adres e-mail, ID w systemie HIS, numer karty pacjenta – często niedoceniane jako dane osobowe.

Dane medyczne
Diagnozy, wyniki badań, hospitalizacje, zalecenia lekarskie – podlegają szczególnej ochronie jako dane wrażliwe.

Zasada rozpoznawalności
Jeśli można zidentyfikować osobę bezpośrednio lub pośrednio – mamy do czynienia z daną osobową.

Szczególne kategorie danych

Co chronimy w szpitalu klinicznym w sposób szczególny?

- **Dane dotyczące zdrowia:** Diagnozy, historia leczenia, wyniki badań, zalecenia – to dane wrażliwe podlegające najwyższej ochronie.
- **Dane genetyczne i biometryczne:** DNA, odciski palców, dane z rozpoznawania twarzy – mają potencjał do trwałej identyfikacji osoby.
- **Informacje o przekonaniach i pochodzeniu:** Wyznanie, poglądy polityczne, pochodzenie etniczne – są objęte dodatkowymi ograniczeniami przetwarzania.
- **Ochrona ustawowa:** RODO i przepisy krajowe wymagają szczególnej ochrony danych wrażliwych – w praktyce oznacza to m.in. ograniczony dostęp, specjalne procedury i szyfrowanie.

Photo by Arseny Togulev on Unsplash

Gdzie w szpitalu są dane osobowe?

Mapa ryzyka w szpitalu klinicznym

- **Dokumentacja papierowa:** Historie choroby, książki raportów, listy pacjentów – mogą zostać przypadkowo ujawnione lub zgubione.
- **Systemy informatyczne:** HIS, RIS, LIS, e-recepty – dostęp wymaga uprawnień i zabezpieczeń, ale błędne logowanie może naruszyć prywatność.
- **Nośniki i urządzenia:** Pendrive'y, płyty CD, laptopy, telefony – łatwe do zgubienia, często bez szyfrowania.
- **Usta i uszy:** Rozmowy w korytarzach, windach, dyżurkach – często nieświadomie naruszają poufność danych.

Photo by Sear Greyson on Unsplash

Kiedy „przetwarzasz” dane?

Codzienne sytuacje w pracy personelu szpitala klinicznego

Wgląd do dokumentacji
Otwieranie historii choroby lub sprawdzanie wyników badań pacjenta to przetwarzanie danych.

Tworzenie i aktualizacja wpisów
Dodanie informacji do dokumentacji, wystawienie e-recepty, zmiana zaleceń – wszystko to jest przetwarzaniem.

Udostępnienie informacji
Przekazanie danych koleżance z dyżuru lub innemu lekarzowi – musi być uzasadnione służbowo.

Przekazanie dokumentacji
Wysyłka dokumentacji medycznej do innego podmiotu – np. na konsultację lub do innej placówki – wymaga podstawy prawnej.

Najczęstsze naruszenia danych – przykłady z życia

Jak dochodzi do incydentów w szpitalu klinicznym?

- **Wydanie dokumentacji nie tej osobie:** Najczęstszy incydent – dokumentacja trafia do innego pacjenta lub osoby nieuprawnionej.
- **Pozostawienie dokumentów na ladzie:** Pacjenci mają dostęp wzrokowy do danych innych osób – np. na rejestracji.
- **Błędna wysyłka e-mail:** Załącznik z dokumentacją medyczną wysłany do niewłaściwego adresata bez szyfrowania.
- **Nieuprawniony dostęp do danych:** Przeglądanie historii choroby pacjenta, którym się nie opiekuję – bez potrzeby służbowej.

Photo by National Cancer Institute on Unsplash

Obsługa dokumentacji medycznej – sytuacje wrażliwe

Codzienne ryzyka w punkcie rejestracji i kontaktu z pacjentem

- **Weryfikacja tożsamości:** Zawsze sprawdzaj dokument tożsamości – nie wydawaj dokumentacji „po nazwisku” lub „z numeru kolejki”.
- **Bezpieczeństwo w punkcie wydania:** Nie zostawiaj dokumentacji medycznej na ladzie ani w miejscach widocznych dla innych pacjentów.
- **Jedna osoba – jeden dokument:** Na biurku powinna znajdować się tylko jedna dokumentacja na raz, aby uniknąć pomyłek.
- **Zachowanie poufności:** Nie omawiaj danych osobowych pacjenta w obecności osób trzecich – nawet w kolejce.

Photo by siriwan arunsiriwattana on Unsplash

Czyste biurko, ekran, drukarka – złoty standard

Bezpieczeństwo danych w codziennym środowisku pracy

Czyste biurko
Nie zostawiaj dokumentacji medycznej na biurku, gdy nie jesteś obecny – gabinet może być dostępny dla osób trzecich.

Czysty ekran
Odchodząc od komputera – zablokuj ekran (Windows + L) lub wyloguj się z systemu.

Bezpieczna drukarka
Odbieraj wydruki natychmiast po wydrukowaniu – nie zostawiaj ich na podajniku.

Zasada widoczności
Każdy widoczny dokument lub ekran może zostać nieumyślnie udostępniony osobie postronnej.

Rozmowa z pacjentem – jak chronić dane?

Zasady komunikacji w przestrzeni szpitala klinicznego

Unikaj wywoływania po diagnozie
Nie używaj sformułowań typu: „Pan z kiłą” – posługuj się numerem lub imieniem i nazwiskiem.

Nie wykrzykuj danych
Nie mów głośno o badaniach lub stanie zdrowia pacjenta w miejscach ogólnodostępnych.

Rozmowa tylko w ustronnym miejscu
Dyskutuj o diagnozie i leczeniu z pacjentem z dala od innych osób.

Minimalizacja danych w komunikacji
Używaj tylko niezbędnych danych – bez nadmiarowych szczegółów przy innych pacjentach.

Wysyłka danych e-mailem – kiedy i jak?

Zasady bezpiecznego przesyłania dokumentacji medycznej

- **Korzystaj z poczty służbowej:** Danych osobowych nie wolno przesyłać z prywatnych kont (gmail, wp, onet itp.).
- **Szyfruj załączniki z danymi:** Zabezpieczaj pliki hasłem – nie używaj PESEL ani innych danych pacjenta jako hasła.
- **Hasło osobnym kanałem:** Hasło do pliku przesyłaj SMS-em lub podaj telefonicznie – nigdy w tej samej wiadomości.
- **Zawsze sprawdzaj odbiorcę:** Zweryfikuj adres e-mail, zanim klikniesz „Wyślij” – literówka to potencjalne naruszenie.

Photo by engin akyurt on Unsplash

Pomieszczenia i dostęp fizyczny

Nie zostawiaj danych bez opieki – nawet na chwilę

Nie zostawiaj nikogo samemu
Nie wolno zostawiać osób postronnych w gabinecie, dyżurce czy pokoju z dokumentacją.

Zamykaj pomieszczenia
Po opuszczeniu gabinetu – zamknij drzwi na klucz, nawet jeśli wychodzisz tylko „na chwilę".

Dane nie mogą leżeć luzem
Dokumentacja musi być schowana – nie zostawiaj kart pacjentów na biurku czy parapecie.

Gotowy incydent RODO
Otwarte pomieszczenie + dane na widoku = nieuprawniony dostęp i naruszenie przepisów.

Tablice, wykazy i listy

Gdzie kończy się prywatność pacjenta?

Dane nie dla wszystkich
Nazwiska i rozpoznania nie mogą być widoczne dla osób postronnych – także pacjentów.

Zakaz umieszczania rozpoznań
Tablica z napisem „Nowak – cukrzyca” to naruszenie danych wrażliwych.

Tablice tylko dla personelu
Muszą znajdować się w zamkniętej dyżurce lub pokoju socjalnym, nie na korytarzu.

Czasowe zestawienia
Wykazy np. do posiłków muszą być zabezpieczone i dostępne tylko dla uprawnionych.

Hasła i loginy – jak chronić dostęp do systemu

Bezpieczne logowanie w środowisku szpitala klinicznego

- **Indywidualne konto to obowiązek:** Zawsze loguj się tylko na swoje konto – nie wolno korzystać z loginu innej osoby.
- **Nie przekazuj haseł:** Nawet chwilowe „zaloguj mnie" to poważne naruszenie zasad bezpieczeństwa.
- **Nie zapisuj haseł na karteczkach:** Hasła na monitorze lub pod klawiaturą to otwarte zaproszenie dla osoby niepowołanej.
- **Regularna zmiana haseł:** Hasła należy zmieniać co jakiś czas i nie używać tych samych w prywatnych serwisach.

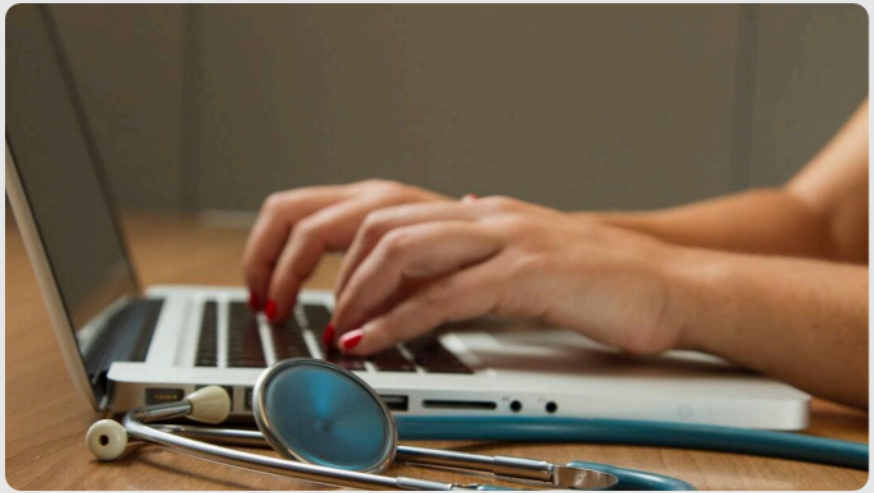

Photo by National Cancer Institute on Unsplash

Zasady korzystania z systemów informatycznych

Bezpieczna praca z danymi pacjentów w EMR, HIS, RIS, LIS

Zaloguj się samodzielnie
Nie używaj konta koleżanki z dyżuru ani wspólnych loginów – każdy ruch w systemie jest rejestrowany.

Nie przeglądaj „z ciekawości”
Otwieranie dokumentacji pacjenta, którym się nie opiekujesz, to naruszenie przepisów i etyki.

Wyloguj się po zakończeniu pracy
Zamknięcie okna systemu to za mało – użyj funkcji „Wyloguj” lub zablokuj ekran.

Zgłaszaj błędy i nadużycia
Jeśli zauważysz nieautoryzowany dostęp lub usterkę – poinformuj niezwłocznie IT lub IOD.

Nie instaluj – zagrożenia z nieautoryzowanego oprogramowania

Bezpieczeństwo systemów szpitalnych w praktyce

Zakaz samodzielnych instalacji
Nie wolno instalować aplikacji bez zgody działu IT – nawet jeśli „wydają się pomocne”.

Źródła z internetu to ryzyko
Pobrane z sieci programy mogą zawierać złośliwe oprogramowanie lub luki bezpieczeństwa.

Zagrożenie dla całej sieci
Jedna aplikacja może otworzyć dostęp do danych całego szpitala – np. przez ransomware.

Używaj tylko zatwierdzonych narzędzi
Dział IT udostępnia listę bezpiecznych i dozwolonych programów – trzymaj się jej.

Phishing – jak rozpoznać zagrożenie?

Oszustwa e-mailowe wymierzone w pracowników szpitali

Podejrzany nadawca
E-mail od nieznanej osoby lub instytucji, często z dziwnym adresem.

Pilny temat wiadomości
Tematy typu: „Twoje konto zostanie zablokowane” – mają wywołać panikę.

Załączniki lub linki
Kliknięcie w nie może prowadzić do instalacji wirusa lub wyłudzenia danych.

Zgłaszaj podejrzane wiadomości
Nie otwieraj, nie odpowiadaj – przekaż mail do działu IT lub IOD.

Ślady dostępu (audit trail)

System pamięta każdy ruch użytkownika

Każde działanie jest rejestrowane
System zapisuje kto, kiedy i do jakich danych uzyskał dostęp.

Rozliczalność personelu
Dostęp do danych musi być uzasadniony służbowo – nie „z ciekawości".

Analiza zdarzeń w przypadku incydentu
Dzienniki logowań pozwalają wykryć nadużycia i naruszenia.

Odpowiedzialność indywidualna
Nie można zasłonić się „wspólnym kontem" – każde konto jest osobiste.

Co robić, gdy dojdzie do incydentu?

Postępowanie w razie naruszenia ochrony danych osobowych

Zabezpiecz sytuację
Ogranicz dostęp do danych – odbierz dokumenty, zablokuj system, przerwij wysyłkę.

Zgłoś do IOD
Niezwłocznie poinformuj Inspektora Ochrony Danych: daneosobowe@usk.poznan.pl.

Opisz zdarzenie
Zbieraj fakty: co się wydarzyło, kto był zaangażowany, jakie dane mogły „wyciec".

Działaj szybko – masz tylko 72h
Administrator danych ma ograniczony czas na zgłoszenie incydentu do UODO.

Rola Inspektora Ochrony Danych

Z kim się kontaktować w razie wątpliwości lub naruszeń?

IOD – osoba pierwszego kontaktu
Każdy pracownik może i powinien zgłaszać pytania lub incydenty do Inspektora Ochrony Danych.

Bez oceniania i obwiniania
Nie musisz wiedzieć, czy coś było naruszeniem – lepiej zapytać niż zignorować.

Poufność i wsparcie
Zgłoszenia są traktowane poważnie, ale nie prowadzą automatycznie do kar – celem jest zabezpieczenie danych.

Kontakt IOD
Adres e-mail: **daneosobowe@usk.poznan.pl** – zawsze dostępny dla pracowników szpitala.

Przechowywanie, wydawanie i niszczenie dokumentacji medycznej

Jak postępować z dokumentacją zgodnie z RODO i standardami szpitala

Przechowuj w zamkniętych szafach
Dokumentacja medyczna powinna być zabezpieczona – dostęp wyłącznie dla personelu uprawnionego.

Weryfikuj tożsamość odbiorcy
Przed wydaniem dokumentacji – sprawdź dowód i zgodność z danymi pacjenta lub pełnomocnictwem.

Nie zostawiaj dokumentów „na ladzie”
Dokumentacja nie może być widoczna lub dostępna dla innych pacjentów – nawet chwilowo.

Niszczenie tylko w niszczarce
Nie wolno wyrzucać dokumentów do zwykłego kosza – używaj szpitalnej niszczarki.

Zasada najmniejszych uprawnień (Least Privilege)

Dostęp do danych w modelu RBAC w szpitalu klinicznym

- **Dostęp tylko do potrzebnych danych:** Każdy pracownik powinien widzieć tylko te dane, które są mu niezbędne do pracy.
- **RBAC – dostęp zależny od roli:** Systemy szpitalne przydzielają uprawnienia na podstawie funkcji zawodowej (np. lekarz, rejestratorka).
- **Nie żądaj danych „na zapas”:** Unikaj otwierania danych „na wszelki wypadek” – to potencjalne naruszenie.
- **Regularny przegląd dostępów:** Uprawnienia muszą być okresowo weryfikowane i dostosowywane do zmian w zatrudnieniu.

Photo by Natanael Melchor on Unsplash

Zero Trust – nie ufaj nikomu automatycznie

Model bezpieczeństwa w środowisku klinicznym

- **Brak domyślnego zaufania:** Każdy dostęp do systemu musi być zweryfikowany, niezależnie od lokalizacji użytkownika.
- **Weryfikacja przy każdej próbie:** System wymusza logowanie, uwierzytelnianie i potwierdzenia przy każdej sesji.
- **Minimalizacja ryzyk wewnętrznych:** Pracownicy wewnętrzni mogą popełniać błędy lub nadużycia – system ich nie uprzywilejowuje.
- **Audyt i monitorowanie działań:** Każdy dostęp do danych jest logowany, a nieprawidłowości analizowane.

Photo by Martha Dominguez de Gouveia on Unsplash

Szyfrowanie danych i załączników

Jak bezpiecznie przesyłać dane pacjentów e-mailem

Szyfruj dokumenty przed wysyłką
Stosuj zaszyfrowane pliki (np. PDF z hasłem) przy przesyłaniu danych pacjentów.

Hasło zawsze innym kanałem
Hasła nie przesyłaj w tej samej wiadomości – przekaż je telefonicznie lub SMS-em.

Nie używaj PESEL jako hasła
Wybieraj silne, unikalne hasła – dane osobowe nie mogą być kluczem dostępu.

Adres i załącznik – sprawdzaj podwójnie
Przed kliknięciem „Wyślij” – upewnij się, że plik i odbiorca są właściwi.

Przykłady poważnych naruszeń

Czego unikać w praktyce szpitalnej

Wydanie dokumentacji niewłaściwej osobie
Najczęstsze naruszenie – wysokie ryzyko naruszenia praw pacjenta.

Mail z danymi do złego adresata
Brak szyfrowania lub błędny adres odbiorcy to realne ryzyko wycieku danych.

Dostęp „z ciekawości”
Przeglądanie danych bez uzasadnienia służbowego narusza zasady i zostawia ślad w systemie.

Dokumenty „na ladzie”
Zostawienie historii choroby lub wyników na widoku to gotowy incydent RODO.

Minimalizacja danych

Przetwarzaj tylko to, co niezbędne

Tylko dane konieczne do celu
Nie zbieraj i nie przechowuj więcej danych niż potrzeba do wykonania zadania.

Unikaj zbędnych informacji
Nie proś o PESEL, adres czy diagnozę, jeśli nie są potrzebne do bieżącej czynności.

Anonimizacja i pseudonimizacja
Tam, gdzie to możliwe – używaj danych zminimalizowanych lub zastępczych.

Minimalizacja w dokumentach
Unikaj wielostronicowych wydruków z nadmiarem danych – dostosuj zakres do celu.

Privacy by Design i Default

Ochrona danych od początku i na każdym etapie

- **Wbudowana ochrona prywatności:** Systemy IT i procedury muszą mieć ochronę danych zaplanowaną od fazy projektu.
- **Domyślna ochrona danych:** Minimalny zakres danych i najniższy poziom dostępu powinien być standardem.
- **Automatyzacja zabezpieczeń:** Systemy powinny same wymuszać dobre praktyki – np. wylogowanie, maskowanie danych.
- **Szpitalny lifecycle danych:** Ochrona obejmuje cały cykl życia danych: od zbierania, przez przechowywanie, po usunięcie.

Photo by Martha Dominguez de Gouveia on Unsplash

Dostępność i niedyskryminacja

Równość dostępu do danych i opieki – standardy WCAG i zasady etyczne

WCAG – standardy dostępności
Systemy i komunikaty muszą być czytelne, kontrastowe, dostępne dla osób z niepełnosprawnościami.

Brak barier fizycznych i informacyjnych
Informacja o danych musi być zrozumiała, niezależnie od stanu zdrowia pacjenta.

Szacunek do godności pacjenta
Unikaj komunikatów mogących naruszyć prywatność – nie krzycz, nie komentuj.

Równość w dostępie do danych
Każdy pacjent – niezależnie od statusu czy pochodzenia – ma równe prawa do informacji o swoich danych.

Fizyczna ochrona prywatności

Układ przestrzeni i głos w ochronie danych w szpitalu

- **Zasady rozmów z pacjentem:** Rozmawiaj w ustronnym miejscu, z poszanowaniem intymności – nie przy innych pacjentach.
- **Layout gabinetów i poczekalni:** Unikaj sytuacji, w których inni pacjenci mogą słyszeć lub widzieć dane innej osoby.
- **Zasłony i fizyczne bariery:** Korzystaj z parawanów, zasłon lub innych barier w sytuacjach wymagających dyskrecji.
- **Ogranicz widoczność dokumentacji:** Dokumentacja nie może być dostępna z korytarza ani dla osób postronnych.

Photo by Adhy Savala on Unsplash

Retencja i niszczenie danych

Jak długo przechowujemy dokumentację i jak ją bezpiecznie usuwamy

- **Retencja według przepisów:** Dokumentację medyczną przechowujemy zgodnie z ustawą – zazwyczaj 20 lat od zakończenia leczenia.
- **Bezpieczeństwo w archiwum:** Dostęp do dokumentacji mają tylko upoważnione osoby – szafy i pomieszczenia muszą być zabezpieczone.
- **Zgodne niszczenie dokumentów:** Po upływie okresu retencji – dokumenty niszczone są w certyfikowanych niszczarkach.
- **Brak archiwizacji na własną rękę:** Nie wolno zabierać dokumentacji do domu ani przechowywać jej poza szpitalem.

Photo by Maksym Kaharlytskyi on Unsplash

Podsumowanie – najważniejsze zasady

Co zapamiętać z perspektywy pracy w szpitalu klinicznym

Zawsze weryfikuj odbiorcę danych
Nie wydawaj dokumentacji bez sprawdzenia tożsamości – to najczęstsze źródło naruszeń.

Szyfruj, sprawdzaj, nie wysyłaj pochopnie
Zanim prześlesz dane – zabezpiecz je, upewnij się, że trafią do właściwej osoby.

Dostęp tylko wtedy, gdy potrzebny
Nie przeglądaj danych z ciekawości – każda aktywność jest rejestrowana.

Zgłaszaj nieprawidłowości do IOD
Kontakt do Inspektora: daneosobowe@usk.poznan.pl – nie zostawiaj wątpliwości bez reakcji.