UNIWERSYTECKA KLINIKA
STOMATOLOGICZNA
PUM

VADEMECUM RODO
Student _Praktykant _ RODO świadomy.
Ochrona danych osobowych -to również Twoja sprawa
(jako osoba przygotowująca się do wykonywania zawodu medycznego).

[1] **VADEMECUM RODO dla Studenta_Praktykanta –** to zbiór podstawowych, wybranych informacji i zasad obowiązujących w Klinice, przepisach prawa w zakresie bezpieczeństwa informacji, w tym ochrony danych osobowych, prywatności i cyberbezpieczeństwa o charakterze praktycznym, **w ramach szkolenia obowiązkowego**.

[2] **RODO** - 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).

1. Jako osoba przygotowująca się do wykonywania zawodu medycznego możesz uzyskać dostęp do dokumentacji medycznej jedynie w zakresie niezbędnym do realizacji celów dydaktycznych, na podstawie art. 26 ust. 3a Ustawy o prawach Pacjenta i Rzeczniku Praw Pacjenta, pod nadzorem uprawnionego personelu medycznego.
2. Jesteś zobowiązany:
   1) do zachowania tajemnicy prawem chronionej, danych i informacji dotyczących podejmowanych czynności, bez względu na sposób, formę ich utrwalenia lub przekazania, o ile informacje nie są powszechnie znane, bądź obowiązek ich ujawnienia wynika z obowiązujących przepisów prawa;

      ⚠ zapamiętaj, że powyższe zobowiązanie zachowuje ważność w przypadku danych osobowych oraz sposobów ich zabezpieczenia bezterminowo, a w przypadku informacji zawartych w dokumentacji medycznej, także po śmierci pacjenta.

Nie opowiadaj o swoich opiekunach, pracownikach, pacjentach na forum, np. w komunikacji miejskiej w drodze powrotnej z praktyki do domu.

Nie udzielaj informacji zawierających dane osobowe w miejscach ogólnodostępnych w obecności osób trzecich/nieuprawnionych.

Nie wykorzystuj uzyskanych na zajęciach informacji/danych osobowych w życiu prywatnym.

   2) do podpisania w Klinice, przed przystąpieniem do praktyki_ Oświadczenie_Studenta_Praktykanta;
   3) do ochrony informacji, w tym danych osobowych, przed niepowołanym dostępem, nieuzasadnioną modyfikacją lub zniszczeniem, nielegalnym ujawnieniem lub pozyskaniem oraz przetwarzaniem danych osobowych z godnością i poszanowaniem praw i wolności osób, których dane dotyczą (w szczególności pacjentów);
   4) do przestrzegania przepisów RODO, ustawy o ochronie danych osobowych oraz innych przepisów dotyczących przetwarzania danych [w tym przepisów branżowych i wewnętrznych Kliniki];
   5) do informowania niezwłocznie o zauważonych nieprawidłowościach w przetwarzaniu informacji i danych osobowych, incydentach bezpieczeństwa i naruszeniach;
   6) do dołożenia szczególnej staranności w działaniu;

7) do aktualizowania wiedzy z dziedziny bezpieczeństwa informacji, ochrony danych osobowych i prywatności oraz cyberbezpieczeństwa.

3. Możesz przetwarzać dane osobowe w Klinice wyłącznie na podstawie obowiązujących przepisów prawa, pod warunkiem przestrzegania przepisów RODO, ustawy o ochronie danych osobowych, przepisów branżowych i unormowań wewnętrznych; zgodnie ze swoimi uprawnieniami.

4. Przed przystąpieniem do zajęć jesteś zobowiązany znać podstawowe definicje, a w szczególności wiedzieć: Co to są dane osobowe ?:

Dane osobowe - art. 4 pkt 1 RODO

4.1. Dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą).

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

4.3. Dane osobowe to mogą być informacje odnoszące się do każdego z aspektów życia osoby - jej życia zawodowego, prywatnego, wykształcenia, wiedzy czy cech charakteru.

4.4. Dane osobowe oznaczają informacje …… o osobie fizycznej…

To nie są osoby fizyczne:
- Zakład Ubezpieczeń Społecznych
- Urząd Skarbowy
- Policja
- Narodowy Fundusz Zdrowia
- Ministerstwo Zdrowia
- Ministerstwo Finansów

To jest osoba fizyczna, np.:
- Jan Kowalski - pacjent
- Jan Kowalski - pracownik
- Jan Kowalski – skarżący i wnoszący
- Inspektor BHP
- Inspektor Ochrony Danych

Tożsamość tych osób znasz lub bez problemu ustalisz

4.5. Jak rozpoznawać dane osobowe „zwykłe", a dane szczególnych kategorii:

Dane osobowe tzw. „zwykłe"
Nie jest to katalog zamknięty, np. Imię i nazwisko, nr PESEL, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy, adres zamieszkania, wizerunek, NIP, REGON, adres e-mail, nr telefonu

Dane osobowe szczególnych kategorii- szczególnie chronione !!!
Jest to katalog zamknięty. Wyłącznie dane określone w art. 9 ust. 1 RODO dane 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; seksualności lub orientacji seksualnej tej osoby; **dane dotyczące stanu zdrowia**.

dane osobowe dotyczące wyroków skazujących i naruszeń prawa

4.6. **Dane dotyczące stanu zdrowia** oznaczają:

4.6.1. dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia (informacja o korzystaniu przez konkretną osobę fizyczną z usług danej placówki opieki zdrowotnej wchodzi w zakres danych dotyczących zdrowia i jest informacją objętą ochroną danych osobowych i to ochroną przewidzianą dla danych szczególnych kategorii (art. 4 pkt. 15 RODO);

4.6.2. oznaczają wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia tej osoby. Są to również informacje o danej osobie zbierane podczas jej rejestracji do usług opieki zdrowotnej i realizacji tych usług. Ponadto informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych oraz wszelkie informacje o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym, stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, zaliczane są do danych dotyczących zdrowia. Również numer, symbol, czy inne oznaczenie przypisane konkretnej osobie w celu jednoznacznego jej zidentyfikowania do celów zdrowotnych. Przy czym nie ma znaczenia źródło pozyskania tych danych tj. niezależnie kto i za pomocą jakiego urządzenia je pozyskał: może to być lekarz lub inny pracownik ochrony zdrowia, urządzenie medyczne, badanie diagnostyczne, procedury medyczne np. in vitro (motyw nr 35 RODO).

4.7. **Dane genetyczne** – oznaczają dane osobowe dotyczące **odziedziczonych lub nabytych cech genetycznych** osoby fizycznej, które ujawniają **niepowtarzalne informacje o fizjologii lub zdrowiu** tej osoby i które wynikają w szczególności z **analizy próbki biologicznej** pochodzącej od tej osoby fizycznej. (Informacja zawarta w kodzie genetycznym człowieka definiuje np. kolor oczu, włosów, skóry, grupę krwi a także zaburzenia: odżywiania, aktywności enzymów oraz choroby jak daltonizm, albinizm, głuchota wrodzona, mukowiscydoza czy nowotwory).

4.8. **Dane biometryczne** – oznaczają dane osobowe, które **wynikają ze specjalnego przetwarzania technicznego**, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz **umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby**, takie jak wizerunek twarzy lub dane daktyloskopijne (odciski palców, wizerunek twarzy, siatkówka czy tęczówka oka, behawioralne lub psychiczne cechy danej osoby, **przetwarzane specjalnymi metodami technicznymi**).

ZAPAMIĘTAJ

1. Informacje osobowe mają charakter subiektywny, ocenny i w większości przypadków będą zależały od kontekstu, w którym się znajdują. Osoba może być zidentyfikowana pośrednio lub bezpośrednio.
2. Dane osobowe oznaczają informacje o osobie fizycznej.
3. Dane szczególnych kategorii, w tym informacje o stanie zdrowia, to dane osobowe, które z racji swego charakteru są szczególnie wrażliwe i wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności.
4. Dane zawarte w dokumentacji medycznej chronimy nawet po śmierci pacjenta.
5. Dane osobowe mogą być wszędzie:
   - ✓ przechowywane w systemach (np. komputery użytkowników, bazy danych, aplikacje),
   - ✓ pisane, drukowane, przechowywane w formie papierowej (np. dokumenty służbowe, dokumentacja medyczna, umowy, projekty, plany, itd.),
   - ✓ przechowywane na różnych nośnikach (np. pendrive, CD\DVD, dyski przenośne, taśmy magnetyczne),
   - ✓ przesyłane pocztą elektroniczną,
   - ✓ słowo mówione.

5. Przed przystąpieniem do zajęć jesteś zobowiązany nie tylko znać podstawowe definicje, ale musisz wiedzieć jak postępować z danych osobowymi pacjenta. Pamiętaj, że w Klinice zabrania się:
   1) wynoszenia danych osobowych poza siedzibę Kliniki;
   2) podejmowania działań mających na celu uzyskanie nieupoważnionego dostępu do zasobów sieci lub komputerów, np. podszywanie się pod innych użytkowników, monitorowanie łącz lub skanowanie portów;
   3) podłączać i współuczestniczyć w podłączaniu do sieci urządzeń;
   4) jakiejkolwiek ingerencji w oprogramowanie Kliniki;
   5) eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp. miejscach. Stosuj Politykę czystego biurka!
   6) przesyłania dokumentacji medycznej, dokumentów służbowych zawierających tajemnicę prawnie chronioną, prywatną pocztą elektroniczną;
   7) przesyłania danych osobowych faksem;
   8) spożywania posiłków, napojów oraz używania ognia w bliskim sąsiedztwie środków przetwarzania danych osobowych (komputerów, dokumentów, itd.);
   9) wykorzystywania prywatnych urządzeń, np. telefonów komórkowych, komputerów przenośnych, portali społecznościowych, np. Facebooka; Skype (bądź innego komunikatora) do przetwarzania danych osobowych pacjentów.

ZAPAMIĘTAJ
tak nie należy postępować !!!

6. W trakcie zajęć dydaktycznych stosuj powyższe zasady oraz dodatkowo:
   1) nie bądź anonimy – noś identyfikator osobowy. Odmowa podania pacjentowi danych identyfikacyjnych powołując się na RODO jest niezgodna z obowiązującymi przepisami prawa;
   2) zwróć szczególną uwagę na sytuacje przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, np. ladach, kopiarkach, drukarkach, biurkach, blatach, parapetach itp.
   3) podmiotowo traktuj każdego pacjenta;
   4) respektuj prawa pacjenta wynikające z ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a w szczególności dbaj o prawo do poszanowania intymności i godności, tajemnicy informacji, prawa do poszanowania życia prywatnego i rodzinnego;
   5) w miejscach gdzie jest to niezbędne korzystaj z parawanów;
   6) zamykaj drzwi do pomieszczeń (szczególnie w trakcie uczestniczenia w procesie udzielania świadczeń zdrowotnych);
   7) unikaj omawiania stanu zdrowia pacjenta w miejscach, w których przebywają osoby nieuprawnione, inni pacjenci (np. w miejscach ogólnodostępnych);
   8) zwracaj się do pacjenta używając zwrotu „Pan/Pani" wraz z dodaniem imienia; wyjątkiem są przypadki, gdy jest to konieczne dla podejmowania nagłych czynności ratowania życia bądź zdrowia;
   9) transportuj (przenoś) dokumenty zawierających dane osobowe bezpiecznie; tj. dbaj, aby osoby postronne nie miały do nich wglądu; stosuj [w tym odpowiednio] torby, teczki, odwracaj, zakrywaj, itd.
   10) niezwłocznie niszcz z użyciem niszczarek dokumenty niepotrzebne w dalszej praktyki np. błędne wydruki zawierające dane osobowe. Pamiętaj, że dokumentacja medyczna podlega archiwizacji zgodnie z obowiązującymi przepisami prawa. Pamiętaj, że zabrania się niszczenia dokumentów zawierających dane osobowe poprzez ich ręczne porwanie, czy wyrzucanie ich do worków z odpadami;
   11) dbaj o poufność informacji (między innymi zamykaj drzwi do pomieszczeń w trakcie prowadzonych rozmów telefonicznych, itp. czynności w ramach, których przetwarzane są dane osobowe; nie zbieraj „wywiadu" w miejscach ogólnodostępnych w obecności osób postronnych).

7. Masz prawo:
   1) kontaktować się z Inspektorem Ochrony Danych we wszystkich sprawach związanych z ochroną danych osobowych;
   2) korzystać z prywatnych urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających wyłącznie do celów czysto osobistych, ściśle i obiektywnie związanych z życiem prywatnym; Pamiętaj, że korzystanie z tych urządzeń nie może naruszać sfery osobistej oraz praw i wolności innych osób, a w szczególności pacjentów.

   w Klinice zabrania się korzystania z Internetu służbowego w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym, a także: grania w gry komputerowe; pobierania z Internetu plików, a tym bardziej instalowania oprogramowania niezwiązanego z wykonywaniem ww. zadań (jakichkolwiek plików muzycznych, wideo, a szczególnie nielegalnego oprogramowania); przeglądania treści o charakterze rozrywkowym oraz uczestniczenia w prywatnych portalach społecznościowych, jeżeli nie jest to związane z realizowaniem zadań w ramach programu.

8. Jesteś zobowiązany pamiętać, że:
   1) przestrzeganie zasad dotyczących bezpieczeństwa informacji, ochrony danych osobowych i prywatności oraz cyberbezpieczeństwa minimalizuje ryzyko wystąpienia incydentu bezpieczeństwa, dlatego dokładaj staranności w działaniu na każdym etapie realizacji zadań dydaktycznych.
   2) W przypadku wystąpienia incydentu bezpieczeństwa lub zdarzenia mającego znamiona incydentu zobowiązany jest niezwłocznie powiadomić pracowników Kliniki.

Poniżej przykładowy katalog incydentów bezpieczeństwa:

przypadkowe lub niezgodne z prawem zniszczenie danych
utracenie danych
nieuprawnione zmodyfikowanie danych

nieuprawnione ujawnienie danych
nieuprawniony dostęp do danych osobowych przesyłanych
nieuprawniony dostęp do danych przechowywanych
nieuprawniony sposób przetwarzania danych
brak podstawy prawnej do przetwarzania danych osobowych lub wskazana podstawa prawna nie jest jednoznaczna
niewłaściwe uwierzytelnienie użytkowników w systemach teleinformatycznych
nieuprawniony dostęp przez użytkowników
nieuprawniony dostęp przez osoby z zewnątrz
nieuprawnione wykorzystanie aplikacji przetwarzającej dane osobowe
możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub inne "złośliwe oprogramowanie"
nadużywanie zasobów
infiltracja komunikacji elektronicznej
brak niezaprzeczalności
osadzanie kodu złośliwego
awaria techniczna systemu lub infrastruktury sieciowej
awaria środowiska wsparcia
awaria systemu lub oprogramowania sieciowego
awaria oprogramowania aplikacji
niewłaściwe odzyskiwanie po awarii (w tym tworzenia kopii zapasowych i przywracania systemów)
kradzież przez użytkowników w tym kradzież sprzętu lub danych
nieprzestrzeganie zasad ochrony danych osobowych !!!!

⚠ **Poniżej przykładowy katalog skutków naruszeń:**

Dyskryminacja
Kradzież tożsamości lub oszustwo dotyczące tożsamości
Strata finansowa osoby fizycznej
Naruszenie dobrego imienia osoby fizycznej
Naruszenie poufności danych osobowych chronionych tajemnicą zawodową (naruszenie godności i prywatności), w tym na skutek nieuprawnionego odwrócenia pseudonimizacji
Uszczerbek na zdrowiu lub śmierć
Wszelka inna znacząca szkoda gospodarcza lub społeczna osoby fizycznej

9. Odpowiedzialność za nieprzestrzeganie zasad:

⚠
1) każdy Praktykant, który przetwarza w Klinice dane osobowe ponosi odpowiedzialność;
2) postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie zasad bezpieczeństwa, co może skutkować odpowiedzialnością przewidzianą w przepisach prawa. Klinika ma prawo odsunąć Praktykanta od zajęć w przypadku, gdy Praktykant nie przestrzega zasad dotyczących bezpieczeństwa informacji, w tym ochrony danych osobowych;
3) postępowanie sprzeczne z powyższymi zobowiązaniami może również narazić Klinikę na sankcje;
4) odpowiedzialność karna(ustawa o ochronie danych osobowych):

„Art. 107. *1.* ***Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony,*** *podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. 2. Jeżeli czyn określony w ust. 1* ***dotyczy danych*** *ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, 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 trzech.”***

SANKCJE

- Odpowiedzialność cywilna
- Odpowiedzialność karna
- Administracyjne kary pieniężne
- Utrata wizerunku

ZAPAMIĘTAJ

Odpowiedzialność w jednakowym stopniu dotyczy realizacji zadań, podejmowania decyzji, i inicjatywy wymaganej zgodnie z kompetencjami.

Ochrona danych osobowych - to również Twoja sprawa.
Dbaj o nie - tak jak chciałabyś/chciałbyś, żeby dbano o Twoje.

Dziękuję za uwagę.

Kontaktuj się z Inspektorem Ochrony Danych, rozmawiaj z nim, pytaj … jest dla Ciebie ☺

Sporządziła:
Inspektor Ochrony Danych
mgr Beata Remecka
Data aktualizacji: 28.09.2023r. – wydanie 2.0.