UNIWERSYTECKA KLINIKA STOMATOLOGICZNA PUM

VADEMECUM RODO dla Studenta
Student RODO- świadomy.
Ochrona danych osobowych -to również Twoja sprawa.

[1] **VADEMECUM RODO dla Studenta –** 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).

Zakres uprawnień i zadań Studenta związanych z ochroną danych osobowych, ochroną prywatności i cyberbezpieczeństwem.

1. Student jako osoba przygotowująca się do wykonywania zawodu medycznego, uprawniony jest do wglądu do dokumentacji medycznej, na podstawie art. 26 ust. 3a Ustawy o prawach Pacjenta i Rzeczniku Praw Pacjenta.
2. Student może uzyskać dostęp do dokumentacji medycznej jedynie w zakresie niezbędnym do realizacji celów dydaktycznych/klinicznych.
3. Dostęp do dokumentacji medycznej nadzorowany jest przez personel medyczny, sprawujący opiekę nad studentami.
4. Dostęp do stref nadzorowanych (Poradni) i realizacja zadań może odbywać się wyłącznie pod nadzorem personelu medycznego sprawującego opiekę nad studentami.
5. Student jest zobowiązany do podpisania zobowiązania do zachowania informacji w poufności/oświadczenia osoby upoważnionej.
6. Student zobowiązany jest do zachowania:
   a) w tajemnicy informacji zawartych w dokumentacji medycznej, także po śmierci pacjenta;
   b) tajemnicy prawem chronionej, danych i informacji dotyczących podejmowanych czynności w związku z odbywaniem zajęć dydaktycznych/klinicznych, bez względu na sposób, formę ich utrwalenia lub przekazania, w szczególności w formie pisemnej, kserokopii, faksu lub zapisu elektronicznego, o ile informacje nie są powszechnie znane bądź obowiązek ich ujawnienia nie wynika z obowiązujących przepisów prawa;
   c) powyższe zobowiązanie zachowuje ważność w przypadku danych osobowych oraz sposobów ich zabezpieczenia bezterminowo.

Nie opowiadaj o swoich przełożonych, współpracownikach na forum, np. w komunikacji miejskiej w drodze powrotnej z pracy do domu.

Nie udzielaj informacji zawierających dane osobowe w miejscach ogólnodostępnych w obecności osób trzecich. Nie rozpowiadaj o pacjentach

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

7. Student może przetwarzać dane osobowe w Klinice wyłącznie na podstawie obowiązujących przepisów prawa, pod warunkiem przestrzegania przepisów RODO[2)], ustawy o ochronie danych osobowych, przepisów branżowych i **unormowań wewnętrznych**.

8. Przed przystąpieniem do zajęć Student zobowiązany jest znać podstawowe definicje. Co to są dane osobowe?:

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

⚠ Dane osobowe mogą być wszędzie:
- ✓ przechowywane w systemach (np. serwery plików, 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.

⚠
1. Dane osobowe definiuje się jako informacje, dzięki którym możliwe jest zidentyfikowanie osoby fizycznej.
2. Oznacza to, że osoba ta nie musi być wskazana bezpośrednio - wystarczy nam zbiór informacji, które pozwolą bezpośrednio lub pośrednio daną osobę zidentyfikować.

9. Studentowi 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 bez zezwolenia Informatyków;
   4) jakiejkolwiek ingerencji w oprogramowanie Kliniki;
   5) eksponowania dokumentów zawierających dane osobowe w miejscach niezabezpieczonych np. biurkach, ladach, półkach, parapetach itp. miejscach;
   6) samodzielnego korzystania ze służbowej poczty elektronicznej Kliniki (bez zgody opiekuna czy innego uprawnionego pracownika Kliniki);
   7) przesyłania dokumentów służbowych zawierających tajemnicę prawnie chronioną, w tym dane osobowe na prywatną pocztę elektroniczną oraz zabrania się przesyłania dokumentów prywatnych na służbową pocztę elektroniczną;
   8) przesyłania samodzielnie pocztą elektroniczną danych osobowych niezaszyfrowanych;
   9) przesyłanie danych osobowych faksem;
   10) spożywania posiłków, napojów oraz używać ognia w bliskim sąsiedztwie środków przetwarzania danych osobowych (komputerów, dokumentów, itd.).

10. Student zobowiązany jest do:
   1) noszenia identyfikatora; odmowa podania pacjentowi danych identyfikacyjnych powołując się na RODO jest niezgodna z obowiązującymi przepisami prawa;
   2) stosowania polityki czystego biurka, zwrócenia szczególnej uwagi na sytuacje przypadkowego pozostawienia dokumentów zawierających dane osobowe w miejscach ogólnodostępnych, np. ladach, kopiarkach, drukarkach, biurkach, blatach, parapetach itp.

3) podmiotowego traktowania każdego pacjenta i respektowania praw pacjenta, a w szczególności prawa do poszanowania intymności i godności, tajemnicy informacji, prawa do poszanowania życia prywatnego i rodzinnego;
4) korzystania z parawanów w pomieszczeniach wieloosobowych lub w miejscach gdzie jest to niezbędne;
5) zamykania drzwi do pomieszczeń (w trakcie udzielania świadczeń zdrowotnych, po ich zakończeniu);
6) unikania omawiania stanu zdrowia pacjenta w miejscach, w których przebywają osoby nieuprawnione, inni pacjenci (np. w miejscach ogólnodostępnych);
7) zwracania 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;
8) transportowania (przenoszenia) dokumentów zawierających dane osobowe bezpiecznie; dbać, aby osoby postronne nie miały do nich wglądu; stosować [w tym odpowiednio] torby, teczki, odwracać, zakrywać, itd.

i) niezwłocznego niszczenia z użyciem niszczarek dokumenty niepotrzebne w dalszej pracy i niepodlegające archiwizacji, np. błędne wydruki zawierające dane osobowe; zabrania się niszczenia dokumentów zawierających dane osobowe poprzez ich ręczne porwanie, czy wyrzucanie ich do worków z odpadami;
j) dbać o poufność informacji, w tym między innymi zamykać drzwi do pomieszczeń w trakcie prowadzonych rozmów telefonicznych, itp. czynności w ramach, których przetwarzane są dane osobowe; nie zbierać „wywiadu" w miejscach ogólnodostępnych w obecności osób postronnych;
k) dbać o bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych.

11. Student ma 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; korzystanie z tych urządzeń nie może naruszać sfery osobistej oraz praw i wolności innych osób, pacjentów;
    3) korzystać z Internetu służbowego wyłącznie do realizacji zadań dydaktycznych i klinicznych (celów służbowych) za zgodą opiekunów;

⚠ 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) bez pisemnej zgody Prezesa Kliniki; przeglądania treści o charakterze rozrywkowym oraz uczestniczenia w portalach społecznościowych, jeżeli nie jest to związane z wykonywaniem zadań służbowych.

12. Student jest zobowiązany pamiętać, że:
    1) przestrzeganie zasad dotyczących ochrony danych osobowych minimalizuje ryzyko wystąpienia incydentu bezpieczeństwa, dlatego zobowiązany jest dokładać staranności w działaniu na każdym etapie realizacji zadań dydaktycznych/klinicznych związanych z przetwarzaniem danych osobowych.
    2) W przypadku wystąpienia incydentu bezpieczeństwa lub zdarzenia mającego znamiona incydentu zobowiązany jest niezwłocznie powiadomić personel 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 Kliniki

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

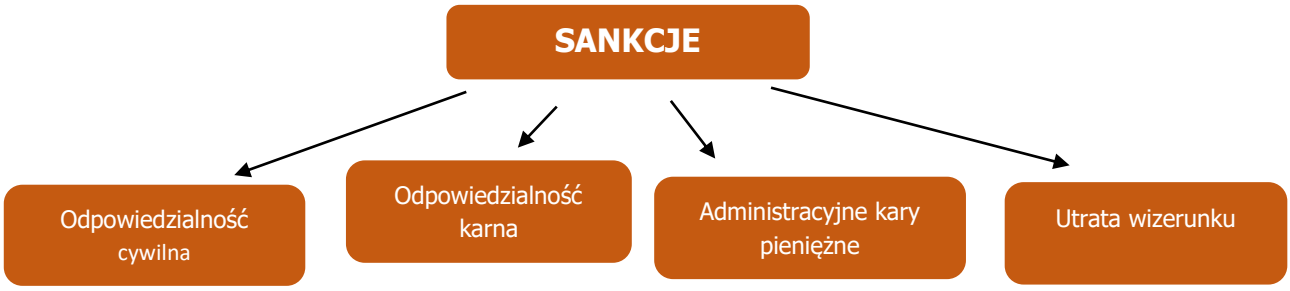
Poniżej przykładowy katalog skutków naruszeń:

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

13. Odpowiedzialność Studenta i Kliniki.

1) każdy Student, który przetwarza w Klinice dane osobowe ponosi odpowiedzialność;
2) postępowanie Studenta sprzeczne z powyższymi zobowiązaniami, może być uznane przez Klinikę za naruszenie zasad bezpieczeństwa, co może skutkować odpowiedzialnością przewidzianą w przepisach prawa. Klinika ma prawo odsunąć Studenta od zajęć w przypadku, gdy Student nie przestrzega zasad dotyczących bezpieczeństwa informacji, w tym ochrony danych osobowych;
3) postępowanie Studenta sprzeczne z powyższymi zobowiązaniami może 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.”***



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: Beata Remecka – Inspektor Ochrony Danych UKS PUM Sp. z o.o.
Data sporządzenia: 30.09.2022r. – wydanie 2.0.