Zasady przetwarzania danych osobowych

Inspektor Ochrony Danych Klaudia Goclik

e-mail: iod@pulmonologia.olsztyn.pl

Obowiązujące akty prawne

- Pisząc i mówiąc „RODO” mamy na myśli 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). Jest to akt prawny przyjęty przez Unię Europejską regulujący zasady ochrony danych osobowych – zastępuje dyrektywę 95/46/WE z 1995 r.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Czym są dane osobowe – art. 4 RODO?

- Dane osobowe- oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); 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;
- Imię i nazwisko, adres zamieszkania, nr PESEL, nr dowodu osobistego, nr telefonu, adres e-mail, stanowią dane osobowe;

Dane wrażliwe- dane szczególnej kategorii zgodnie z art. 4 RODO

- Ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej.
- „dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

Inne ważne definicje z art. 4 RODO:

- 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; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
- 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;

<u>Każda czynność na danych jest ich przetwarzaniem, sam fakt przechowywania danych oznacza, że je przetwarzamy.</u>

Najważniejsze definicje art. 4 RODO:

- pseudonimizacja- oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- zgoda- osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
- 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;

Kiedy można przetwarzać dane osobowe?

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. podstawa prawna przetwarzania danych. Typowymi podstawami przetwarzania danych zwykłych są:

a) zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a) RODO);

b) przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby (art. 6 ust. 1 lit. b) RODO);

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c) RODO);

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 lit. d) RODO);

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e) RODO)

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f) RODO)

Poprzez realizację praw osób, których dane dotyczą mamy na myśli prawa wskazane w art. 15-22 RODO, tj. prawo do:

- dostępu do danych,
- sprostowania danych,
- usunięcia danych („prawo do bycia zapomnianym”),
- ograniczenia przetwarzania danych,
- przenoszenia danych,
- sprzeciwu,
- niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu.

Jak należy zabezpieczać dane osobowe?

RODO odchodzi od praktyki polegającej na wskazywaniu w przepisach prawa konkretnych środków zabezpieczenia danych osobowych, jakie mają zostać wdrożone przez administratora lub podmiot przetwarzający. Zamiast tego, RODO wprowadza tzw. podejście oparte na ryzyku.

Istota podejścia opartego na ryzyku sprowadza się do tego, że każdy podmiot przetwarzający dane osobowe powinien samodzielnie określić, jakie konkretne środki zabezpieczenia danych należy wdrożyć. Dobór środków zabezpieczenia powinien być oparty o:

a) charakter, zakres, kontekst i cele przetwarzania,

b)ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,

c) stan wiedzy technicznej,

d) koszt wdrażania.

RODO nie nakazuje stosowania żadnych konkretnych środków zabezpieczenia danych. RODO wskazuje tylko przykładowe środki techniczne i organizacyjne, które mogą służyć osiągnięciu tego celu, tj. zapewnienia stopnia bezpieczeństwa odpowiadającego ryzyku. Są nimi w szczególności:

1. pseudonimizacja i szyfrowanie danych osobowych;

2. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

3. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

4. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Co to jest obowiązek zgłaszania naruszeń ochrony danych?

RODO nakłada na podmioty przetwarzające dane osobowe prawny obowiązek informowania o incydentach bezpieczeństwa dotyczących danych osobowych. Jest to bardzo istotna zmiana w stosunku do ustawy z 29 sierpnia 1997 r., która tego rodzaju rozwiązania w ogóle nie zawierała.

Incydent bezpieczeństwa zwany jest w przepisach RODO naruszeniem ochrony danych osobowych i może polegać na:

a) naruszeniu bezpieczeństwa prowadzącym do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania danych osobowych

b) naruszeniu bezpieczeństwa prowadzącym do nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Przykłady:

- zagubienie nośnika z danymi osobowymi,
- uzyskanie dostępu do danych przez osobę do tego nieuprawnioną,
- włamanie do systemu służącego do przetwarzania danych osobowych.

O wystąpieniu incydentu należy poinformować organ nadzorczy (PUODO). Informacja powinna zostać przekazania niezwłocznie, lecz nie później, niż w ciągu 72 godzin od stwierdzenia naruszenia. W pewnych przypadkach należy również informować o incydencie osoby, których dane dotyczą – będzie tak wtedy, gdy naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą.

Przykłady:

- uzyskanie przez osoby nieuprawnione dostępu do loginów i haseł klientów systemu bankowości elektronicznej,
- zagubienie nośnika zawierającego dokumentację medyczną pacjentów.

Sankcje w RODO- finansowe

PRZEDSIĘBIORCY

- do 2% całkowitego rocznego globalnego obrotu z poprzedniego roku obrotowego lub do 10 000 000 euro

lub

- do 4% całkowitego rocznego globalnego obrotu z poprzedniego roku obrotowego lub do 20 000 000 euro

OSOBY FIZYCZNE

- do 10 000 000 euro

lub

- 20 000 000 euro

Sankcje w RODO- inne

- **Odpowiedzialność karna-** przepisy karne zostały zawarte w ustawie o ochronie danych osobowych i przewidują one – w zależności od rodzaju czynu – karę grzywny, karę ograniczenia wolności lub karę pozbawienia wolności nawet **do lat trzech.**

- **Odpowiedzialność cywilna -** osoba, której dane dotyczą, ma prawo do odszkodowania za szkodę majątkową lub niemajątkową wynikłą z naruszenia RODO.

- **Odpowiedzialność pracownicza-** w skrajnych przypadkach niesubordynacja pracownika może zostać uznana za ciężkie naruszenie podstawowych obowiązków pracowniczych i skutkować nawet rozwiązaniem umowy w trybie dyscyplinarnym, z winy pracownika.

ZAGADNIENIA PRAKTYCZNE

Czy podmiot leczniczy może udostępnić telefonicznie informacje o fakcie hospitalizacji pacjentów o wskazanej przez rozmówcę tożsamości?

- Gdy nie ma pewności co do tożsamości rozmówców, ale udzielenie takich informacji może mieć wpływ na stan zdrowia bądź życia pacjenta- tak, ale może to mieć miejsce w wyjątkowych przypadkach.
- W przypadku kiedy odmowa udzielenia informacji o pobycie pacjenta w szpitalu może uniemożliwić realizację prawa członków rodziny bądź osób bliskich do informacji o stanie zdrowia pacjenta, podmiot powinien udzielić takich informacji w sytuacjach nagłych (np. wypadek drogowy) oraz w stanach zagrożenia życia dla pacjenta.
- Placówka powinna jednak dostatecznie uprawdopodobnić, że rozmówca jest osobą uprawnioną do uzyskania tej informacji poprzez zadanie pytań kontrolnych np. PESEL, adres miejsca zamieszkania;
- Zgodnie z zasada minimalizacji należy przekazywać telefonicznie wyłącznie te informacje, które są niezbędne do działania w stanie wyższej konieczności.

Czy podmiot leczniczy może wykorzystywać utrwaloną już metodę ujawniania informacji o stanie zdrowia w zakresie temperatury pacjenta?

- Na tzw. kartach przyłóżkowych, tak. Podmiot medyczny może wykorzystywać w swojej praktyce karty przyłóżkowe. Rezygnacja z nich jest natomiast dobra praktyką.
- W bardzo wielu przypadkach nagłe pogorszenie się stanu zdrowia pacjenta, może wymagać natychmiastowego dostępu do jego danych identyfikacyjnych.
- Karta przyłóżkowa daje taką gwarancję. Podmiot lecznicy może całkowicie zrezygnować z kart przyłóżkowych z uwzględnieniem obowiązków wynikających z przepisów art. 36 ust. 3, 5 i 6 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
- W przypadku gdy stosowanie kart jest konieczne, należy je zabezpieczyć poprzez:

- zastosowanie ramek na karty przyłóżkowe chroniących dane osobowe zawarte w kartach;
- konstrukcja ramki powinna uniemożliwić odczytanie danych;
- **zastosowanie nakładki zabezpieczającej dane pacjenta na karcie przyłóżkowej;**
- odwrócenie kart przyłóżkowych;

Na powyższe zwracał uwagę NIK przy kontrolach podmiotów medycznych pod względem RODO jako niezgodne z art. 24 ust. 1 RODO, w którym jako jeden z obowiązków ADO wskazano wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę danych osobowych.

Czy podmiot leczniczy może uzależnić wgląd do dokumentacji medycznej osoby trzeciej ?

- Od posiadanego upoważnienia udzielonego przez pacjenta, którego dotyczy dokumentacja, opatrzonego własnoręcznym podpisem albo złożonym w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym, zgodnie z przepisami o prawach pacjenta i Rzeczniku Praw Pacjenta, upoważnienie w danej placówce może być udzielone w dowolnej formie, a ograniczenie formy upoważnienia stanowi naruszenie praw pacjenta.
- Należy jednak pamiętać, ze placówka powinna mieć pewność w zakresie tożsamości osoby udzielającej upoważnienia. Jeżeli pacjenta udziela takiego upoważnienia bezpośrednio w obecności personelu dopuszczalna powinna być taka forma oświadczenia.
- Należy również pamiętać, że podmiot udzielający świadczeń zdrowotny, realizując swoje obowiązki związane z prowadzeniem dokumentacji medycznej, zobligowany został także do prowadzenia wykazu z informacjami dotyczącymi udostępnionej dokumentacji medycznej.

Czy możliwe jest oznaczenie produktów leczniczych imieniem i nazwiskiem pacjenta ?

- Tak. Ze względu na ograniczenie ryzyka pomyłek, oznaczenie imieniem i nazwiskiem pacjenta, gdy korzysta ze świadczenia w podmiocie leczniczym jest dopuszczalne. Dotyczy to wszystkich produktów leczniczych. Podstawą prawną przetwarzania danych osobowych w powyższym zakresie jest art. 9 ust. 1 lit. h RODO.
- Konsekwencje związane z podaniem niewłaściwego produktu medycznego mogą mieć poważny wpływ na zdrowie, a nawet życie pacjentów, powyższe przesłanka stanowi bezpośrednią podstawę prawną do imiennego oznaczania produktów medycznych.
- Niemożliwe byłoby zbieranie w tym zakresie zgód od pacjentów na przetwarzanie danych osobowych, bowiem gdyby on takiej zgody nie wyraził placówka miałaby ogromy problem.

Czy lekarz i personel medycyny na sali chorych może zwracać się do pacjentów po imieniu i nazwisku?

- Lekarz nie powinien na sali chorych zwracać się po imieniu i nazwisku do pacjenta. Można natomiast zwracać się do pacjenta używając chociażby zwrotu „Pani/Pan” wraz z dodaniem imienia, co jednocześnie zagwarantuje poszanowanie godności pacjenta. Wyjątkiem są przypadki, gdy lekarz nie może zidentyfikować pacjenta w inny sposób, niż poprzez użycie jego nazwiska, bądź gdy jest to konieczne dla podejmowania nagłych czynności ratowania życia bądź zdrowia.
- Zgodnie z art. 9 ust. 2 lit. h RODO przetwarzanie danych osobowych dotyczących stanu zdrowia, możliwe jest, gdy jest niezbędne dla celów profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki zdrowotnej, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa państwa członkowskiego.
- Zgodnie z art. 36 ust. 3 i 5 ustawy z dnia 15 kwietnia 2011 o działalności leczniczej, pacjentów zaopatruje się w znaki identyfikacyjne. Znak identyfikacyjny zawiera informacje pozwalające na ustalenie: imienia i nazwiska , daty urodzenia pacjenta. Jedynie w uzasadnionych przypadkach może od tego odstąpić. Przyczynę wraz z odmową zastosowania takiego środka identyfikacji zawiera się w dokumentacji medycznej.
- Informacje ww. znaku mają być tak zapisane, żeby uniemożliwić jego identyfikację przez osoby nieuprawnione.
- Celem ww. przepisów jest zatem uniemożliwienie identyfikacji pacjenta przez osoby postronne. Tym samym przyjęcie jako zasady zwracania się do pacjenta przez personel medyczny po imieniu i nazwisku, byłoby niezgodne z celem jaki wynika z ww. przepisów.

Czy lekarz może na sali chorych rozmawiać z pacjentem o jego chorobie?

- Gdy nie ma gwarancji, czy nie słyszą tego inni pacjenci, a stan zdrowia pacjenta pozwala na przeprowadzenie takiej rozmowy poza salą chorych, to co do zasady, przekazywanie przez personel medyczny pacjentowi informacji ujawnionych dane o stanie jego zdrowia, na sali wieloosobowej, powinny być ograniczone do minimum niezbędnego do realizacji celu w którym są przetwarzane;
- Działania nie będące monitorowaniem stanu zdrowia, zadawanie pytań o samopoczucie czy uzyskiwanie i przekazywanie informacji związanych z procesem leczenia. Bez wątpienia mogą należeć do nich informowanie o pobieraniu świadomej zgody na procedury medyczne, informacja o diagnozie sposobie leczenia itp. Jeżeli stan zdrowia na to pozwala udzielanie takich informacji powinno odbywać się w gabinecie lekarskim, bądź w innym miejscy gdzie nie przebywają inne osoby nieuprawnione.
- Komunikacja z pacjentem związana bezpośrednio z realizacją bieżącego monitorowania stanu zdrowia pacjenta, w tym pytanie o samopoczucie, uzyskanie i przekazanie podstawowych informacji związanych z procesem leczenia. Chodzi o czynności związane z obchodem lekarskim lub pielęgniarskim, informacje o zmianie leków i planowanych badaniach. W takich sytuacjach możliwe jest przekazywanie informacji o stanie zdrowia pacjenta na sali chorych.
- W trakcie wykonywania bieżących czynności medycznych na sali mogą przebywać wyłącznie osoby uprawnione. Na życzenie pacjenta może być również osoba bliska.
- W przypadku, gdy rozmowa o stanie zdrowia pacjenta związana jest bezpośrednio z ratowaniem życia bądź zdrowia i nieprzeprowadzenie rozmowy w trybie natychmiastowym mogłoby narazić pacjenta na uszczerbek, możliwe jest przeprowadzenie rozmowy w każdym miejscu.

Czy placówka zdrowia może na drzwiach gabinetów lekarskich zamieszczać imiona i nazwiska oraz specjalizacje lekarzy przyjmujących pacjentów?

- Tak zamieszczenie imion i nazwisk oraz specjalizacje lekarza na drzwiach gabinetów lekarskich nie narusza RODO.
- Informacje o imieniu i nazwisku lekarza oraz jego specjalizacji są jego zwykłymi danymi osobowymi. Zgodnie z art. 6 ust. 1 lit. c RODO podstawą przetwarzania danych zwykłych jest realizacja obowiązku wynikającego z przepisów prawa.
- Zgodnie z art. 31 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych pacjent ma prawo wyboru lekarza, a zgodnie art. 36 ustawy u działalności leczniczej osoby zatrudnione w szpitalu bądź pozostające w stosunku cywilnoprawnym z podmiotem leczniczym, którego zakładem leczniczym jest szpital, są zobowiązane nosić w widocznym miejscu identyfikator zawierający imię i nazwisko oraz funkcję tej osoby.
- Dane lekarze, w tym w szczególności imię, nazwisko, rodzaj i stopień posiadającej specjalizacji , czy też umiejętności z zakresu węższych dziedzin medycyny lub udzielania określonych świadczeń zdrowotnych, zawarte są w rejestrze prowadzonym we właściwa okręgową radę lekarską zgodnie z art. 8 ust. 1 ustawy z dnia 5 grudnia 1996 o zawodach lekarza i lekarz dentysty oraz zgodnie z Rozporządzeniem Ministra z dnia 26 czerwca 2012 r., w sprawie szczegółowych wymagań, jakim powinny odpowiadać pomieszczenia i urządzenia podmiotu wykonującego działalność leczniczą, przesądza o obowiązku oznaczania gabinetów lekarskich.

W jaki sposób w czasie wzywania pacjentów do gabinetów lekarskich można zapewnić im anonimowość, gdy placówka nie ma środków na wdrożenie elektronicznego systemu identyfikacji pacjentów (numerki), a na korytarzu przebywa czasami ogromna ilość pacjentów?

- Dążyć należy do minimalizacji ryzyka ujawnienia informacji osobom postronnym, w szczególności danych o stanie zdrowia, z uwzględnieniem konkretnych uwarunkowań technicznych, organizacyjnych i lokalowych w placówce. Zastosowane rozwiązania nie mogą w żadnym zakresie zakłócać udzielania świadczeń opieki zdrowotnej ani narażać zdrowia lub życia pacjentów.
- Przykładowe sposoby wywoływania pacjenta w podmiocie leczniczym:

- wezwanie z wykorzystanie numeru identyfikacyjnego. Nadanego zgodnie ze wskazaniem art. 36 ust. 5 ustawy o działalności leczniczej znaku/ pseudonimu numerycznego. Wpisanie tych numerów do dokumentacji medycznej następuje z jednoczesnym przekazaniem ich pacjentowi. Pacjent wzywany jest wówczas do gabinetu po tym numerze.
- wezwanie po numerze nadanym podczas rejestracji. Takie rozwiązanie nie wymaga nakładów finansowych, a wiąże się jedynie z nadawaniem unikalnego numeru podczas rejestracji w sposób, zapewniający przekazanie numeru lekarzowi w gabinecie oraz pacjentowi.
- Wezwanie po godzinie wizyty. Umawianie na konkretną godzinę w sposób uniemożlwiający pokrywanie się godzin.
- Wezwanie po godzinie + imię (Pan Andrzej z godziny 11.30) + ewentualnie numer gabinetu.

W jaki sposób zapewnić anonimowość pacjentów w trakcie rejestracji przed wizytą lekarską ?

Możliwe sposoby dokonania rejestracji pacjenta w podmiocie leczniczym z potwierdzeniem tożsamości:

- w podmiocie powinno zostać wyznaczone miejsce do realizacji procesu rejestracji, oznaczenia miejsca powinny w wyraźny sposób wskazywać obszar, w którym może znajdować się wyłącznie obsługiwany pacjent.

a) Naklejenie na podłodze przed stanowiskiem rejestracji taśmy w jaskrawych barwach wyznaczających obszar, w którym przebywa tylko osoba obsługiwana;

b) Zamieszczenie komunikatu o konieczności przebywania przy jednym stanowisku recepcyjnym tylko jednego pacjenta;

c) Oddzielenie strefy rejestracji ścianką. Płytą plexi- w strefie pojedyncze miejsce siedzące lub stojące. Osoby nieuprawnione pozostają poza barierą fizyczną;

d) Oddzielenie strefy rejestracji barierka- osoby nieuprawnione pozostają poza strefą rejestracji za barierką;

e) Wprowadzenie odpowiedniej odległości między stanowiskami;

f) Wprowadzenie strefy rejestracji w osobnym pomieszczeniu poza korytarzem miejscem dla oczekujących;

g) Wprowadzenie możliwości rejestracji elektronicznej/ telefonicznej.

h) Możliwe wyznaczenie odrębnego od recepcji głównej, odizolowanego stanowiska do rejestracji telefonicznej, w ramach której dochodzi do odczytywania danych osobowych

W jaki sposób zweryfikować pacjenta ?

a) Osoba rejestrująca prosi pacjenta o okazanie dokumentu weryfikującego tożsamość;

b) Jeżeli pacjent odmawia okazania dokumentu weryfikującego tożsamość można poprosić go o podanie danych identyfikacyjnych tj. PESEL lub inny numer identyfikacyjny;

c) Możliwe jest zastosowanie kartek/ formularzy, na których pacjent wpisuje wymagane dane identyfikacyjne. Kartki muszą być niszczone niezwłocznie po wykorzystaniu, w sposób umożliwiający odtworzenie zapisanej treści. Jeżeli nie ma możliwości ich natychmiastowego zniszczenia, należy odkłada w bezpiecznym miejscu i niszczyć niezwłocznie po zakończeniu pracy;

d) Jeżeli pacjent dobrowolnie bez wezwania okazuje dokument weryfikujący tożsamość lub przekazuje istnie informacje, umożliwiające ustalenie tożsamości nie należy odmawiać przyjęcia dobrowolnie podanych danych.

e) Wprowadzenie możliwości bezpiecznej rejestracji elektronicznej

Wnioski z kontroli przeprowadzonej prze NIK w szpitalach.

- Pozytywnie oceniono opracowanie i wdrożenie odpowiedniej dokumentacji oraz procedur dotyczących ochrony danych osobowych;
- Personel został poinformowany o przepisach RODO oraz regulacjach wewnętrznych szpitala.
- Przeprowadzenie analizy procesów przewarzania danych.
- Nadanie uprawnień w systemach informatycznych adekwatne do miejsca pracy i wykonywanych zadań.
- Wywiązywanie z obowiązku zawarcia umów powierzenia przetwarzania danych osobowych.
- Udostępnianie danych medycznych odbywało się zgodnie z obowiązującymi przepisami.
- Stwierdzenie, że przyjęte w szpitalach sposób oznaczania opasek identyfikacyjnych pacjentów oraz stosowania ramek na karty przyłóżkowe były niezgodne z obowiązującymi przepisami
- Nie zastosowano odpowiednich środków ochrony podczas nieobecności lekarza w jednym z gabinetów, co stwarzało niebezpieczeństwo dostępu do danych osobowych i medycznych pacjentów przez osoby nieuprawnione.
- Nieterminowe poinformowanie Prezesa Urzędu Ochrony Danych osobowych o wyznaczeniu IOD.

Proste zasady

1. Blokuj komputer

Za każdym razem, gdy odchodzisz od biurka zastosuj blokadę komputera. Pozwoli to zminimalizować ryzyko ujawnienia danych osobom nieupoważnionym.

2. Stosuj zasadę czystego biurka

Dokumenty zawierające dane osobowe pozostawione bez nadzoru na biurkach mogą dostać się w ręce osób nieupoważnionych. Występuje ryzyko nieuprawnionego ujawnienia danych.

3. Odbieraj dokumenty z drukarki

Wydrukowane i nieodebrane z drukarki dokumenty zawierające dane osobowe mogą zostać przejęte przez osoby do tego nieupoważnione. Unikaj takich sytuacji i zawsze odbieraj wydrukowane dokumenty.

4. Przechowuj dokumenty zawierające dane osobowe w zamykanych na klucz meblach.

Dokumenty przechowywane np. w szafie bez zamka nie są chronione w sposób prawidłowy ponieważ każda osoba ma do nich dostęp.

5. Usuwaj skany dokumentów z dysku komputera.

6. Nie ujawniaj danych pacjentów osobom nieupoważnionym

7. Pracuj na sprzęcie firmowym.

Zasady bezpiecznego korzystania z poczty elektronicznej

- **1. Nie zapisuj hasła do swojej poczty w przeglądarce**

Traktuj pocztę elektroniczną jak system bankowy. Nigdy nie zapisuj hasła do swojej poczty w przeglądarce internetowej. Uchroni Cię to przed dostępem do niej przez osoby niepowołane lub wykradzeniem hasła przez wirusy bezpośrednio z systemu przeglądarki.

- **2. Zawsze pamiętaj by się wylogować**

Wyrób w sobie nawyk wylogowywanie się z poczty elektronicznej. Wiele systemów w szczególności on-line, posiada ustawioną bardzo długą sesję. To znaczy, że jeśli się raz zalogujesz, pozostajesz zalogowany przez wiele dni. Jest to bardzo niebezpieczne.

- **3. Używaj silnego i unikalnego hasła do skrzynki pocztowej**

Cyberprzestępcy mają dostęp do milionów jak nie miliardów standardowych haseł. Używając prostych haseł umożliwiasz im włamanie się na Twoje konto z użyciem metod Brute Force. W hasłach nie używaj imion czy nazwisk swoich lub osób najbliższych. Nie używaj numerów identyfikacyjnych np. PESEL czy dat urodzenia. Hasło powinno być długie, zawierać znaki specjalne, spacje i raczej być w formie zdania niż pojedynczego sformułowania. Do wrażliwych serwisów jak skrzynki pocztowe stosuj różne, unikalne hasła. Złamanie hasła w innych serwisach w których masz konta nie spowoduje automatycznie przechwycenia kolejnych kont usługowych.

Zasady bezpiecznego korzystania z poczty elektronicznej

- **4. Nigdy nie udostępniaj swojego hasła**

Nigdy nie udostępniaj swojego hasła do kont pocztowych żadnym osobom trzecim. Jest to bardzo niebezpieczne a co więcej nie będziesz miał żadnej informacji o tym, co ta osoba przeglądała w twojej poczcie.

- **5. Zawsze weryfikuj nadawcę**

Zawsze sprawdzaj nadawcę wiadomości oraz domenę z której jest ona przysłana. Wprawny haker co prawda jest w stanie podszyć się pod dowolny adres ale coraz większa ilość usługodawców pocztowych jest w stanie wykrywać takie wiadomości i je blokować. Nie mniej jednak, cyberprzestępcy wysyłając fakowe wiadomości stosują adresy mailowe o podobnej nazwie do banków czy dużych usługodawców, co może uśpić Twoją uwagę. Weryfikując nadawcę sprawdzaj adres e-mail z jakiego przyszła wiadomość a nie nazwę.

- **6. Sprawdź poprawność pisowni wiadomości**

Wiele wiadomości wysyłanych jest automatycznie przez roboty. Często wiadomości te są automatycznie tłumaczone z innych języków. Sprawia to, że treść wiadomości posiada głównie błędy stylistyczne i gramatyczne. Jeżeli otrzymasz wiadomość z łamaną polszczyzną, możesz być niemal pewien że było ona wygenerowana z translatora. Bądź ostrożny przy takich wiadomościach.

Zasady bezpiecznego korzystania z poczty elektronicznej

- **7. Nie odpowiadaj na SPAM**

Odpowiadanie na SPAM potwierdza istnienie adresu e-mail a tym samym może wygenerować kolejną dawkę niechcianych wiadomości.

- **8. Nie klikaj w linki umieszczone w mailach**

Nigdy nie klikaj w linki zamieszczone w mailach. Jeżeli wiadomości mają postać HTML, możesz zostać przekierowany na inną stronę niż podana w treści wiadomości. Lepiej wkleić link do paska adresu w przeglądarce i przed uruchomieniem sprawdzić jaką ma postać. Linkowanie do dziwnej nieznanej strony powinno stanowić dla Ciebie ostrzeżenie.

- **9. Uważaj na podejrzane załączniki nawet od znajomych**

Hakerzy często wysyłają SPAM i wirusy z przejętych kont do listy kontaktów. Otrzymując wiadomość od rodziny, znajomych lub znanych kontrahentów Twoja czujność jest uśpiona. Uważaj w szczególności na pliki spakowane ZIP, RAR, 7-ZIP itp. oraz dokumenty PDF, które bardzo często transportują wirusy, trojany, robaki i inne programy szpiegujące.

Zasady bezpiecznego korzystania z poczty elektronicznej

- **10. Korzystaj z dostawców poczty elektronicznej, którzy skanują załączniki pod kątem wirusów**

Przy wyborze Twojego dostawcy usług pocztowych kieruj się jakością a nie ceną. Wybieraj tych dostawców, którzy stosują skanery antywirusowe na załącznikach, które otrzymujesz. Zmniejszy to ryzyko zainstalowania wirusa na twoim urządzeniu.

- **11. Uważaj na podejrzane załączniki nawet od znajomych**

Hakerzy często wysyłają SPAM i wirusy z przejętych kont do listy kantaków. Otrzymując wiadomość od rodziny, znajomych lub znanych kontrahentów Twoja czujność jest uśpiona. Uważaj w szczególności na pliki spakowane ZIP, RAR, 7-ZIP itp. oraz dokumenty PDF.

- **12. Korzystaj z dwustopniowej weryfikacji**

Trudno się do tego przyzwyczaić i jest to nieco uciążliwe rozwiązanie, ale o ile to możliwe korzystaj z dwustopniowej weryfikacji. Polega ona na konieczności wpisania podczas każdego logowania dodatkowego kodu (tokena) wysłanego poprzez SMS lub na aplikację mobilną. Zwiększy to poziom bezpieczeństwa Twojego konta i uchroni Cię przed dostępem do niego nawet w przypadku ujawnienia hasła.

- **13. Nie wysyłaj wrażliwych danych bez szyfrowania**

Nigdy nie wysyłaj wrażliwych danych pocztą elektroniczną w formie niezabezpieczonej. Wrażliwe są wszelkie informacje, numer PESEL, wiek, miejsce zamieszkania, skany dokumentów itp. Jeżeli musisz przekazać takie dokumenty lub informacje, wprowadź je w oddzielnym dokumencie, spakuj do archiwum zip, rar, 7z lub innego z hasłem, a następnie prześlij zaszyfrowane. Hasło zawsze dostarczaj innym kanałem np. poprzez SMS lub komunikator.