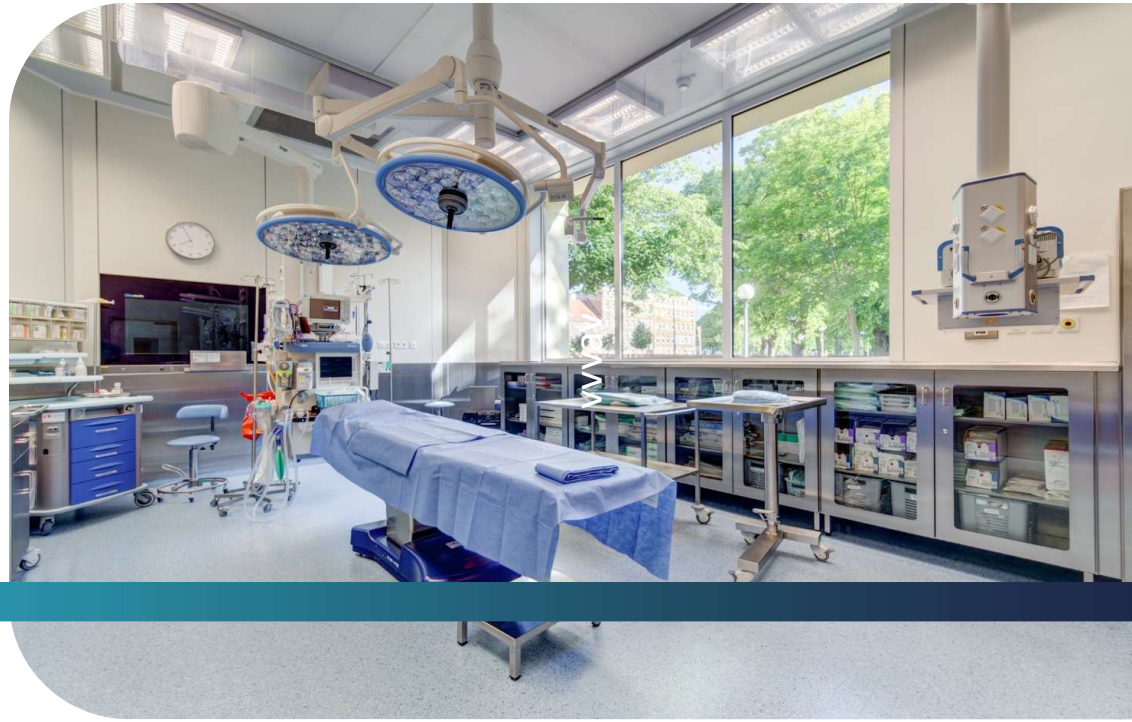
UNIWERSYTECKI
SZPITAL
KLINICZNY NR 2
PUM w Szczecinie

Incydenty związane z bezpieczeństwem danych osobowych w pracy Szpitala



Inspektor Ochrony Danych

Załącznik nr 16 do Polityki Ochrony Danych Osobowych data
wydanie:2 data

DANE OSOBOWE

Oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

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, jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową

lub społeczną tożsamość tej osoby.

DANE OSOBOWE SZCZEGÓLNYCH KATEGORII

Są to dane ujawniające informacje o stanie zdrowia, pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, biometryczne, dotyczące zdrowia, seksualności oraz orientacji seksualnej osoby fizycznej.

PRZETWARZANIE DANYCH OSOBOWYCH

Oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych. Są to wszelkie operacje wykonywane na danych osobowych.

Przetwarzaniem danych jest ich zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, rozpowszechnianie, udostępnianie, przesyłanie, usuwanie i niszczenie

INCYDENTY ZWIĄZANE Z BEZPIECZEŃSTWEM DANYCH OSOBOWYCH - PRZYKŁADY

PRZYKŁADOWE NARUSZENIA OCHRONY DANYCH OSOBOWYCH – wykorzystywanie prywatnego sprzętu do przetwarzania d.o.

POLSKA POLITYKA ŚWIAT KORONAWIRUS WOJNA W UKRAINIE

Zobacz na Gazeta.pl Profesor walczy na wojnie i... prowadzi zajęcia ze studentami Czytaj teraz

Lekarz błaga złodzieja o oddanie danych

Ewa Fertak

Lekarzowi z Centrum Zdrowia Dziecka skradziono w Szczyrku laptop. Tymczasem są tam medyczne dane ważne dla życia kilkudziesięciu ciężko chorych dzieci!

W 2007 r. Doktorowi Piotrowi Zwolińskiemu z Centrum Zdrowia Dziecka skradziono w Szczyrku laptop. W utraconym sprzęcie przechowywane były dane ważne dla życia kilkudziesięciu ciężko chorych na epilepsję dzieci. Doktor Zwoliński wystąpił w TV z apelem do złodzieja o oddanie laptopa. Bezskutecznie.

Doktor przetwarzał dane osobowe przy użyciu prywatnego sprzętu, przez co dane nie były chronione we właściwy sposób, a kopie danych nie były wykonywane. **Dane medyczne pacjentów zostały utracone przez Centrum Zdrowia Dziecka, w ich posiadanie weszła nieznana osoba.**

WYKORZYSTYWANIE PRYWATNEGO SPRZĘTU DO PRZETWARZANIA D.O.

Jest sprzeczne z postanowieniami PROCEDURY PRACY ZDALNEJ zgodnie z którą:

1. „Dostęp zdalny do sieci szpitala odbywa się za pośrednictwem VPN skonfigurowanego przez Wydział Informatyczny i Ochrony Cyberprzestrzeni na urządzeniach przenośnych będących własnością szpitala.
2. Dostęp zdalny konfigurowany jest tylko na laptopach służbowych. Wyjątek stanowią firmy zewnętrzne, gdzie dostęp zdalny do zasobów elektronicznych został określony w umowie.
3. Konfiguracja następuje na podanie zatwierdzone przez Dyrekcję. Przedmiotowe podanie jest dostępne w zasobach Intranet.”

WYKORZYSTYWANIE PRYWATNEGO SPRZĘTU DO PRZETWARZANIA D.O.

Jest sprzeczne z zasadami opisanymi w POLITYCE OCHRONY DANYCH OSOBOWYCH USK-2

1. „Dokumenty elektroniczne zawierające w swojej treści jakiekolwiek dane osobowe przetwarzane w zasobach USK-2 mogą być przekazywane poprzez:
2. wewnątrz organizacji – poprzez wspólny dysk sieciowy, na którym uprawnienia do katalogów są nadane indywidualnie dla konkretnych użytkowników lub grup użytkowników (nie większych niż komórka organizacyjna szpitala),
3. wewnątrz i na zewnątrz organizacji – poprzez służbową skrzynkę email (domena usk2.szczecin.pl). Wiadomość powinna zostać zaadresowana przy zachowaniu szczególnej staranności oraz dbałości, aby wprowadzony adres email odbiorcy był prawidłowy. Dokument przed wysłaniem powinien zostać spakowany i jednocześnie zaszyfrowany hasłem (archiwum szyfrowane ZIP, RAR, 7Z). Ustalone hasło należy przekazać odbiorcy za pomocą kanału innego niż email np. SMS, telefon, itp.
4. na zewnątrz organizacji – poprzez elektroniczną skrzynkę podawczą (ePUAP) przypisaną do podmiotu organizacji. Wiadomość powinna zostać zaadresowana przy zachowaniu szczególnej staranności oraz dbałości, aby wprowadzony adres skrytki odbiorcy był prawidłowy. Dokument przed wysłaniem powinien zostać spakowany i jednocześnie zaszyfrowany hasłem (archiwum szyfrowane ZIP, RAR, 7Z). Ustalone hasło należy przekazać odbiorcy za pomocą kanału innego niż ePUAP np. email, SMS, telefon, itp.”

POZOSTAWIANIE POMIESZCZEŃ,SPRZĘTU i DOKUMENTACJI BEZ NADZORU

Przyszedł tylko po receptę. Po chwili niósł szpitalny monitor do lombardu

TVN24 | Kraków 8 maja 2023, 13:07 Autor: bp/tok Źródło: małopolska policja

POZOSTAWIANIE POMIESZCZEŃ,SPRZĘTU i DOKUMENTACJI BEZ NADZORU

RODO w szpitalu

14 LISTOPADA 2019 07:00

NIK o ochronie danych osobowych w szpitalach

Zmiana w podejściu do ochrony danych osobowych i prywatności pacjentów w szpitalach jest nie tylko konieczna, ale i pilna. Jak wykazała bowiem kontrola NIK rutyna i utarte schematy działania gubią personel szpitali, zobowiązany do dbałości o bezpieczeństwo danych osobowych i medycznych pacjentów. Tylko pojedyncze ze skontrolowanych szpitali wprowadziły rozwiązania, które stwarzały warunki do odpowiedniego przechowywania papierowej dokumentacji medycznej oraz gwarantowały prawo pacjentów do prywatności w trakcie rejestracji lub na salach szpitalnych. W pozostałych placówkach nie zapewniono skutecznej ochrony danych osobowych i medycznych przed ujawnieniem osobom nieupoważnionym.

W ponad połowie skontrolowanych szpitali doszło do naruszeń ochrony danych osobowych, z czego w sześciu sytuacja była na tyle poważna, że konieczne było powiadomienie Prezesa Urzędu Ochrony Danych Osobowych. W Szpitalu Specjalistycznym im. Ludwika Rydygiera w Krakowie Sp. z o.o. **jeden z pacjentów niechcący zabrał dokumentację medyczną innego pacjenta jednej z poradni,** a w Wojewódzkim Specjalistycznym Szpitalu Dziecięcym im. Św. Ludwika w Krakowie **mężczyzna z zaburzeniami psychicznymi ukradł z pomieszczenia rejestracji trzy kartoteki pacjentów - dwóch z nich nie odnaleziono. W 9 z 24 skontrolowanych szpitali papierowa dokumentacja pacjentów na oddziałach szpitalnych przechowywana była w niezamykanych szafkach lub na półkach.** W ocenie NIK

POZOSTAWIANIE POMIESZCZEŃ,SPRZĘTU i DOKUMENTACJI BEZ NADZORU

Jest sprzeczne z zasadami opisanymi w POLITYCE OCHRONY DANYCH OSOBOWYCH USK-2

„Osoby upoważnione do przetwarzania danych osobowych

1. Wszystkie osoby, które zostały upoważnione do przetwarzania danych osobowych lub przetwarzają dane osobowe zawarte w dokumentacji medycznej pacjentów na podstawie zapisów art. 24 ust. 2 pkt. 1) ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta:
2. odpowiadają za zachowanie danych osobowych w poufności zarówno w trakcie jak i po ustaniu zatrudnienia;
3. **są zobowiązane zabezpieczać powierzone im dane osobowe w sposób wykorzystujący wszelkie formy ochrony organizacyjnej i technicznej udostępnione przez Administratora."**

„W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka, *która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym.* (…) Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety."

„W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe."

POZOSTAWIANIE POMIESZCZEŃ,SPRZĘTU i DOKUMENTACJI BEZ NADZORU

Jest sprzeczne z zasadami opisanymi PROCEDURZE ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY W SYSTEMIE:

„Użytkownik jest zobowiązany do uniemożliwienia wglądu do danych wyświetlanych na monitorze osobom niepowołanym, tzw. polityka czystego ekranu.”

„Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu”

WSPÓŁDZIELENIE KONT W SYSTEMACH INFORMATYCZNYCH

Udostępnianie indywidualnych loginów i haseł do systemów informatycznych

Przypominamy, że udostępnianie indywidualnych loginów i haseł do systemów informatycznych (w tym AMMS i Infomedica) jest zabronione. Współdzielenie kont powoduje brak możliwości jednoznacznej identyfikacji osób wykonujących operacje w systemach informatycznych. Dotyczy to także sytuacji wynikających z zastępstw innych pracowników. W przypadku braku uprawnień do określonych funkcjonalności lub zasobów istnieje możliwość ich rozszerzenia poprzez wypełnienie i procedowanie wniosku „karty uprawnień użytkownika". Szczegóły postępowania opisuje Instrukcja Zarządzania Systemami Informatycznymi (Zarządzenie Dyrektora SPSK-2 nr 84/2023 z dnia 31 marca 2023 r.).

Data dodania ogłoszenia: 13.09.2023

WSPÓŁDZIELENIE KONT W SYSTEMACH INFORMATYCZNYCH

Jest złamaniem przepisów Ustawy Kodeks Karny z dnia 6 czerwca 1997r.

Art. 267.

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie

Brak weryfikacji danych wprowadzanych do systemu

cowzdrowiu.pl

Najnowsze Pacjenci Pracownicy medyczni POZ i AOS Finanse Leki Wyroby medyczne

10 tys. zł kary za złe informacje w skierowaniu. Powód: ochrona danych

Autor : Aleksandra Kurowska

2022-08-02 11:33

Brak weryfikacji danych wprowadzanych do systemu

CO ROBIĆ KIEDY W USK-2 DOJDZIE DO NARUSZENIA?

- Jak najszybciej zabezpieczyć miejsce powstania incydentu przed dostępem osób nieupoważnionych – jeśli wymaga tego charakter incydentu;
- Niezwłocznie zawiadomić bezpośredniego przełożonego i Inspektora Ochrony Danych (nr tel. 914661477, adres e-mail iod@usk2.szczecin.pl

UNIWERSYTECKI
SZPITAL
KLINICZNY NR 2
PUM w Szczecinie

Dziękuję za uwagę

www.usk2.szczecin.pl