SKUTECZNE SPOSOBY ZABEZPIECZENIA DANYCH W ELEKTRONICZNEJ DOKUMENTACJI MEDYCZNEJ

13 ważnych wytycznych dla placówek medycznych

1 Wykonuj i sprawdzaj kopie zapasowe

- Zasady i częstotliwość tworzenia kopii zapasowych opisz w polityce bezpieczeństwa informacji w części dotyczącej środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności.
- Koniecznie regularnie wykonuj kopie zapasowe i zastępuj nimi poprzednio wykonane.
- Kopie zapasowe danych w formie elektronicznej możesz tworzyć automatycznie przez odpowiednie oprogramowanie lub manualnie przez wyznaczoną do tego osobę.
- Testuj kopie zapasowe przez zastosowanie protokołu porównawczego poprawności danych oryginalnych i ich kopii. W przypadku niezgodności lub nieczytelności danych powtórz wykonanie kopii zapasowej.

2 Utrzymuj ciągłość działania systemów informatycznych

- W celu ochrony przetwarzanych danych osobowych przed ich przypadkową utratą stosuj urządzenia podtrzymujące działanie systemów teleinformatycznych.
- Stosuj urządzenia podtrzymujące napięcie elektryczne w razie awarii prądu przez okres niezbędny do zabezpieczenia danych osobowych (zapisanie bieżącej pracy, ponowne zabezpieczenie hasłem bazy danych itp.).

3 Przygotuj raport podsumowujący inwentaryzację oprogramowania

- W polityce bezpieczeństwa informacji w części dotyczącej środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności uwzględnij bieżącą inwentaryzację sprzętu informatycznego i badanie jego dalszej przydatności do celów bezpiecznego przetwarzania danych osobowych.
- Sporządź raport z inwentaryzacji komputerów i prowadź rejestr komputerów przenośnych.

4 Dokumentuj czynności z zakresu eksploatacji, aktualizacji i monitoringu systemu oraz oprogramowania

- Zastosuj pseudonimizację i szyfrowanie danych osobowych, regularnie testuj, mierz i oceniaj skuteczność środków technicznych i organizacyjnych, które mają zapewnić bezpieczeństwo przetwarzania danych.
- Przygotuj raporty z naruszenia ochrony danych oraz rejestr incydentów bezpieczeństwa, działań korygujących i zapobiegawczych.
- W przypadku naruszenia ochrony danych osobowych bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, zgłoś je organowi nadzorczemu – możesz to tego wykorzystać formularze udostępnione przez UODO.

5 Stosuj politykę haseł, stwórz użytkownikom indywidualne konta i nadaj loginy

- Każdemu użytkownikowi systemu teleinformatycznego, który ma dostęp do przetwarzanych danych, nadaj odrębny identyfikator oraz hasło dostępu.
- Zadbaj, aby system informatyczny wymuszał nie rzadziej niż raz na 30 dni zmianę hasła składającego się co najmniej z 6–7 znaków.
- Stosuj fizyczne urządzenia, klucze przypisane do konkretnego użytkownika, których podłączenie do urządzenia stanowi element procesu weryfikacji uprawnień.

6 Twórz historię logów

- Twórz historię logów i na bieżąco je kontroluj, aby ocenić aktualność zastosowanych zabezpieczeń oraz ich skuteczność.
- Taka kontrola pozwoli Ci szybko wykryć zarejestrowany nieuprawniony dostęp do zbioru danych osobowych, a także bezzwłocznie podjąć działania ograniczające ryzyko nieupoważnionego dostępu w przypadku podejmowanych prób ataków na systemy zabezpieczeń (np. wirusy, włamania, ataki typu exploit, DoS, spyware, spoofing, hijacking, sniffing itp.).
- Historia logów gwarantuje przechowywanie informacji o wprowadzeniu, modyfikacji lub usunięciu danych przetwarzanych w zasobie i użytkowniku, informacji o odbiorcach danych.

7 Blokuj hasła i konta byłego pracownika

- Nie przydzielaj identyfikatora osoby, która utraciła upoważnienie do przetwarzania danych w imieniu administratora, innej osobie.
- W przypadku urządzeń przenośnych (oprócz zabezpieczenia zbioru danych osobowych) stosuj zabezpieczenia teleinformatyczne uniemożliwiające uruchomienie sprzętu przez osoby postronne w przypadku jego utraty.

8 Aktualizuj oprogramowanie, w tym antywirusowe

- Poddawaj przeglądom oprogramowanie, a w razie konieczności uaktualniaj stosowane zabezpieczenia.
- Na bieżąco aktualizuj stosowane oprogramowanie, w tym przede wszystkim programy kontrolujące przepływ informacji między systemem informatycznym a siecią publiczną (firewall, komercyjne oprogramowanie antywirusowe, zapewniające bieżącą aktualizację baz danych wirusów i szkodliwych programów).

9 Stosuj hasła na BIOS i programy szyfrujące połączenia

- W przypadku urządzeń przenośnych zastosuj zabezpieczenia teleinformatyczne uniemożliwiające uruchomienie sprzętu przez osoby postronne w przypadku jego utraty. Dotyczy to również zabezpieczenia hasłem podstawowego systemu wejścia-wyjścia, umożliwiającego pośrednią kontrolę procesu uruchamiania sprzętu.
- Osobę upoważnioną do przetwarzania danych osobowych, korzystającą z urządzeń przenośnych, przeszkol z zakresu ochrony sprzętu przed jego utratą lub uszkodzeniem.
- Szyfruj połączenia i dane przesyłane na odległość za pomocą systemów teleinformatycznych.
- Stosuj środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej (np. hasła dostępu).

10 Chroń dane przed błędami, utratą, nieuprawnioną modyfikacją

- Ogranicz liczbę osób i uprawnienia do inicjowania poszczególnych procesów (stosuj zabezpieczenia przed usunięciem, zmianą lub kopiowaniem w zależności od funkcji i poziomu uprawnień użytkownika).

11 Używaj mechanizmów automatycznej blokady stanowiska pracy

- Stosuj tzw. zasadę czystego ekranu, polegającą między innymi na jego automatycznym wygaszeniu w przypadku braku aktywności po stronie użytkownika.
- Zastosuj rozwiązanie, które do wybudzenia urządzenia będzie wymagało wprowadzenia hasła dostępowego identyfikującego konkretną osobę uprawnioną.

12 Odpowiednio zabezpiecz serwerownię

- Ogranicz dostęp do serwerowni, gdzie przechowujesz dane osobowe, wyłącznie do osób imiennie upoważnionych przez administratora lub do osób nieuprawnionych wyłącznie w obecności osoby upoważnionej.
- Urządzenia, na których przetwarzasz dane osobowe, przechowuj w warunkach określonych przez ich producenta.
- Zamontuj system kontroli dostępu. Załóż klimatyzację lub mierz temperaturę i wilgotność w serwerowni.

13 W umowach serwisowych podpisanych ze stronami trzecimi zawrzyj zapisy gwarantujące odpowiedni poziom bezpieczeństwa informacji

- Zawrzyj stosowną umowę powierzenia, podlegającą prawu unijnemu lub prawu państwa członkowskiego, obejmującą zagwarantowanie ochrony na poziomie odpowiadającym co najmniej ochronie zapewnianej przez administratora.
- Zadbaj o wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO oraz chroniło prawa osób, których dane dotyczą.
- Wyrażaj – bądź nie – zgodę na dalsze powierzenie danych przez podmiot przetwarzający.

Patroni medialni:

DOKUMENTACJA MEDYCZNA W PRAKTYCE plus ALERT E-ZDROWIE

LEKARZ MEDYCYNY PRACY

RODO W OCHRONIE ZDROWIA

ZARZĄDZANIE PLACÓWKĄ MEDYCZNĄ

SERWIS ZOZ.pl ZARZĄDZANIE W OCHRONIE ZDROWIA

Wiedza i Praktyka sp. z o.o., ul. Łotewska 9a, 03-918 Warszawa, nr rejestrowy BDO: 000008579,
Centrum Obsługi Klienta: tel. 22 518 29 29, faks: 22 617 60 10, www. formularze.wip.pl

HMD0018