Karta informacyjna dotycząca szkolenia wstępnego z zakresu ochrony danych osobowych

Instruktaż przeprowadzony w dniu:

……

(data)

Robert Tomza – Inspektor Ochrony Danych w Szpitalu Specjalistycznym w Brzozowie

(imię i nazwisko, stanowisko służbowe przeprowadzającego instruktaż)

Zgodnie z Regulaminem przetwarzania i ochrony danych osobowych oraz Procedurami dotyczącymi stosowania tego Regulaminu wymaga się tego, aby:

1. Dostęp do danych osobowych miały osoby posiadające upoważnienie do przetwarzania danych.
2. Dane były chronione przed dostępem do nich osób nieupoważnionych.
3. Pomieszczenia, w których są przetwarzane dane osobowe, były zamykane na klucz.
4. Dostęp do kluczy posiadali tylko upoważnieni pracownicy.
5. Dostęp do pomieszczeń był możliwy tylko i wyłącznie w godzinach pracy. W sytuacji gdy jest wymagany poza godzinami pracy – **tylko na podstawie zezwolenia Administratora Danych Osobowych.**
6. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe, mogli mieć tylko upoważnieni pracownicy.
7. W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
8. Szafy, w których przechowywane są dane, były zamykane na klucz.
9. Klucze do tych szaf posiadali tylko upoważnieni pracownicy.
10. Szafy z danymi były otwarte tylko na czas potrzebny na dostęp do danych, a następnie były zamykane.
11. Dane w formie papierowej znajdowały się na biurkach tylko na czas niezbędny do wykonania czynności służbowych, a następnie były chowane do szaf.
12. Dostęp do komputerów, na których są przetwarzane dane, mieli tylko upoważnieni pracownicy.
13. Monitory komputerów, na których są przetwarzane dane, były tak ustawione, aby osoby nieupoważnione nie miały wglądu w dane.
14. Korzystać tylko i wyłącznie ze służbowych skrzynek pocztowych.
15. Niezabezpieczonych (niezaszyfrowanych) danych osobowych nie przesyłać drogą elektroniczną.
17. Sieć komputerowa była zabezpieczona przed wszelkim dostępem z zewnątrz.
18. Błędne lub nieaktualne wydruki i wersje papierowe zawierające dane osobowe lub inne informacje chronione były przeznaczone do zniszczenia zgodnie z obowiązującą procedurą.

Za prawidłowy nadzór przetwarzania danych oraz zapewnienie im odpowiedniej ochrony odpowiada każdy pracownik na swoim stanowisku pracy, zgodnie z obowiązkami pracowniczymi.

Za nieprzestrzeganie procedur bezpieczeństwa i naruszenie ochrony danych grozi odpowiedzialność finansowa, odszkodowawcza, dyscyplinarna, a w skrajnych przypadkach nawet karna.

Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia danych osobowych to głównie:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy;
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia

ochronę zasobów, lub inny komunikat o podobnym znaczeniu;
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
6) naruszenie lub próba naruszenia integralności systemu albo bazy danych;
7) próbę modyfikacji lub modyfikacja danych albo zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
8) niedopuszczalna manipulacja danymi osobowymi w systemie;
9) ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedury ochrony przetwarzania albo innych strzeżonych elementów systemu zabezpieczeń;
10) praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony informacji – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu itp.;
11) istnienie nieautoryzowanych kont dostępu do danych lub tzw. bocznej furtki itp.;
12) podmiana lub zniszczenie nośników z danymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowanie bądź skopiowanie danych;
13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych itp.).
Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych, tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.

Uwagi:

……..

Przeczytałam/przeczytałem* powyższy instruktaż, w pełni go zrozumiałam/zrozumiałem* i zaakceptowałam/zaakceptowałem*. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem.**

Ponadto jako osoba zobowiązana do przestrzegania powyższych regulacji zobowiązuję się do samodzielnego przeczytania dodatkowych informacji zamieszczonych na stronie internetowej Szpitala Specjalistycznego w Brzozowie a dotyczących zagadnień z zakresu ochrony danych osobowych (*Regulamin przetwarzania i ochrony danych osobowych wraz z Procedurami dotyczącymi stosowania tego Regulaminu, Karta szkolenia z zakresu ochrony danych osobowych – jedna z trzech, Instrukcja postępowania w przypadku naruszenia bezpieczeństwa danych osobowych itp.*).

……

(data i podpis osoby, której udzielono instruktażu)

** Niepotrzebne skreślić;*

*** Podpis jest potwierdzeniem odbycia instruktażu i zapoznania się z przepisami oraz zasadami przetwarzania i ochrony danych osobowych. Podpisaną kartę przechowuje Inspektor Ochrony Danych.*