Zasady ochrony danych osobowych w Samodzielnym Publicznym Zakładzie Opieki Zdrowotnej Wojewódzkim Szpitalu Zespolonym im. Jędrzeja Śniadeckiego w Białymstoku

Karta wstępnego instruktażu

Imię i nazwisko: .....

PESEL: .....

Stanowisko/Funkcja: .....

1. *Dane osobowe* są to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. *Dokumentacja medyczna* pacjenta (w tym informacje o stanie zdrowia oraz o korzystaniu ze świadczeń opieki zdrowotnej) jest szczególnym rodzajem danych osobowych (dane wrażliwe) i powinna być objęta wzmożoną ochroną.
3. Dane osobowe powinny być chronione przed dostępem do nich osób nieupoważnionych.
4. Każdy z pracowników/stażystów/praktykantów powinien zachować szczególną ostrożność przy przetwarzaniu danych.
5. Przez *przetwarzanie danych osobowych* rozumie się wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
6. Dostęp do danych osobowych mają wyłącznie osoby posiadające imienne upoważnienie do przetwarzania tych danych.
7. *Administratorem danych osobowych* pacjentów i pracowników Szpitala jest Samodzielny Publiczny Zakład Opieki Zdrowotnej Wojewódzki Szpital Zespolony im. Jędrzeja Śniadeckiego w Białymstoku, reprezentowany przez Dyrektora Szpitala.
8. Od dnia 25.05.2018 r. podstawą prawną regulująca przetwarzanie danych osobowych jest 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 – RODO).
9. *Dostęp do pomieszczeń*, w których są przetwarzane dane osobowe, powinny mieć tylko osoby upoważnione. Osoby nieupoważnione mogą przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności.
10. Pod nieobecność osób upoważnionych pomieszczenia, w których są przetwarzane dane osobowe, powinny być zamykane na klucz.
11. Dostęp do kluczy oraz elektronicznych kart dostępowych powinny posiadać tylko osoby upoważnione.
12. *Dostęp do komputerów*, na których przetwarzane są dane osobowe, mają tylko osoby upoważnione. Użytkownikom zabrania się korzystania z systemów informatycznych dla celów innych niż związane z wykonywaniem obowiązków służbowych.
13. Zabrania się nieautoryzowanego podłączania urządzeń teleinformatycznych oraz nośników pamięci własnych lub strony trzeciej do systemów informatycznych oraz urządzeń Szpitala.
14. Zabrania się podejmowania prób testowania, modyfikacji, naruszenia lub obchodzenia zabezpieczeń systemów informatycznych lub jakichkolwiek działań noszących takie znamiona.
15. Użytkownikom zabrania się umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej Szpitala oraz do Internetu osobom nieuprawnionym.

16. Błędne, nieaktualne lub niepotrzebne dokumenty (wydruki) papierowe zawierające dane osobowe lub inne informacje chronione powinny być niszczone są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający ich odtworzenie. Zabronione jest wyrzucanie takich dokumentów do kosza.
17. Zabronione jest wynoszenie dokumentów zawierających dane osobowe lub inne informacje chronione poza pomieszczenia Szpitala.

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

Naruszenia lub podejrzenie naruszenia zabezpieczenia ochrony danych osobowych należy zgłaszać Inspektorowi ochrony danych.

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

1. sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych, jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, niepożądana ingerencja ekipy remontowej itp.,
2. 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,
3. pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów, lub inny komunikat o podobnym znaczeniu,
4. ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych elementów systemu zabezpieczeń,
5. podmienienie lub zniszczenie nośników z danymi oraz skasowanie lub skopiowanie danych (dokumentów) bez odpowiedniego upoważnienia,
6. rażące naruszenie dyscypliny w zakresie przestrzegania procedur bezpieczeństwa informacji (korzystanie z kont innych użytkowników, niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, praca na informacjach służbowych w celach prywatnych itp.).

Uwagi:

Przeczytałam/em powyższy instruktaż, w pełni go zrozumiałam/em i zaakceptowałam/em. Zobowiązuję się go przestrzegać, co potwierdzam własnoręcznym podpisem:

.....
(data i podpis osoby, której udzielono instruktażu)

.....
(Inspektor ochrony danych)

Białystok, ...
(miejscowość, data)