Zasady bezpieczeństwa informacji medycznej

Centrum Onkologii - Instytutu im. Marii Skłodowskiej - Curie w Warszawie

Rozdział 1
Cel regulaminu.
§ 1

Celem niniejszego regulaminu jest wskazanie zasad oraz reguł postępowania z:
- papierową dokumentacją medyczną pacjentów lub pracowników (medycyna pracy)
- papierową dokumentacją naukową zawierająca dane medyczne, a dotycząca pacjentów lub pracowników
- informacją medyczną, zgromadzoną w systemach informatycznych, a dotycząca pacjentów lub pracowników
- informacją naukową, zgromadzoną w systemach informatycznych, a zawierająca dane medyczne pacjentów lub pracowników.

Rozdział 2
Zakres regulaminu.
§ 1

Niniejszy regulamin dotyczy wszystkich pracowników, współpracowników, podwykonawców, konsultantów, pracowników czasowych, studentów, doktorantów, praktykantów korzystających z dostępu do dokumentacji medycznej i naukowej zawierającej dane medyczne pacjentów/pracowników.
Wszystkie w/w osoby są zwanej dalej Użytkownikami informacji medycznej.

Rozdział 3
Polityka dostępu
§ 1

1. Zasady bezpieczeństwa informacji medycznych stanowią, iż użytkownicy informacji medycznej są odpowiedzialni za bezpieczeństwo i zgodność z prawem korzystania z danych medycznych wytworzonych w Centrum Onkologii w Warszawie lub pozyskanych przez COI od innych podmiotów.
2. Użytkownicy informacji medycznych są zobowiązani przestrzegać:
a) zapisy niniejszego regulaminu
b) zasady bezpieczeństwa przetwarzania danych osobowych.
3. Użytkownicy informacji medycznej, korzystający z prywatnych urządzeń przetwarzających dane należące do COI, takich jak: komputery, laptopy, palmtopy, tablety itp., w czasie jej przetwarzania również podlegają:
a) zapisom niniejszego regulaminu
b) zasadom bezpieczeństwa przetwarzania danych osobowych.

§ 2

1. Przy pracy z papierową dokumentacją zawierającą dane medyczne zabronione jest:
   a) Pozostawianie dokumentacji w miejscach ogólnie dostępnych bez stałego nadzoru pracownika COI
   b) Wydawanie dokumentacji pacjentowi np. oczekującemu na spotkanie z lekarzem
   c) Pozostawianie jej po pracy na biurku (wymagane jest przechowywanie pod zamknięciem)
   d) Przekazywanie pracownikom COI nie upoważnionym do dostępu do niej
   e) Udostępnianie jej osobom/podmiotom nie uprawnionym
   f) Wyrzucanie do śmieci dokumentów zawierających dane medyczne, nie zniszczonych w niszczarce w sposób umożliwiających łatwe odczytanie danych.

2. Przy przetwarzaniu informacji medycznej w systemach informatycznych zabronione jest:
   a) dokonywanie wpisów za inne osoby, modyfikacje wpisów wykonanych przez inne osoby
   b) udostępnienie innym osobom swoich danych autoryzacyjnych (login, hasło)
   c) przetwarzanie informacji medycznej na sprzęcie nie zabezpieczonym przez: zawirusowaniem, dostępem osób nie uprawnionych.

d) umieszczanie ekranu/wyświetlacza urządzenia przetwarzającego, w sposób umożliwiający czytanie informacji przez osoby nie uprawnione
e) pozostawiania włączonego sprzętu bez nadzoru pracownika, bez włączonego wygaszacza ekranu, zabezpieczonego hasłem
f) umieszczanie sprzętu przetwarzającego w miejscach ogólnie dostępnych, bez nadzoru pracownika.

3. Wymagane jest by sprzęt komputerowy służący do przetwarzania informacji medycznej:
a) Był wyposażony w aktualne wersję oprogramowania antywirusowego z aktualnymi danymi dotyczącymi wykrywanych wirusów
b) Był wyposażony w aktualne wersję oprogramowania służącego do przetwarzania (np. aktualna wersja oprogramowania przeglądarki stron internetowych)
c) Był wyposażony w aktualne wersję oprogramowania systemowego (system operacyjny) oraz aktualne wersje oprogramowania użytkowego/narzędziowego (brak luk umożliwiających włamanie i dostęp do przetwarzanych danych)
d) Automatyczna transmisja danych zawierających informacje medyczną w sieci ma być szyfrowana.
e) Przekazywanie danych ad hoc zawierających informacje medyczną musi odbywać się z zastosowaniem pseudoszyfrowania (np. spakowanie plików z zastosowanie hasła, hasło ma być przekazane w inny sposób niż dane) lub szyfrowania.

4. Osoby odpowiedzialne za systemy informatyczne gromadzące dane medyczne są zobowiązani do sporządzania kopii bezpieczeństwa. Kopie bezpieczeństwa muszą być przechowywane w sposób umożliwiający zachowanie trwałości i bezpieczeństwa danych.

5. Użytkownicy przetwarzający informację medyczną są zobowiązani do zgłaszania do: Inspektora Ochrony Danych oraz Działu Informatyki COI (w zakresie przetwarzania komputerowego) zauważonych nieprawidłowości w jej przetwarzaniu.

§ 3

Użytkownik przetwarzający informację medyczną zgadza się na:
a) monitorowanie zachowania użytkownika w sieci włączając w to takie elementy jak: dostęp do zasobów plikowych, dostęp do zasobów teleinformatycznych, itp.
b) wyrywkowe sprawdzanie stanu technicznego sprzętu dostępowego
c) cykliczną zmianę hasła do konta dostępowego (do sieci), nie rzadziej niż co 90 dni.
d) login do konta będzie składał się z emaila firmowego.

Rozdział 4

§ 1

Naruszenie regulaminu

Każdy Użytkownik, któremu udowodni się niestosowanie do niniejszego regulaminu lub omijanie jego zapisów może być pociągnięty do odpowiedzialności dyscyplinarnej, zgodnie z obowiązującymi przepisami.

§ 2

Odpowiedzialność

Użytkownik przetwarzający informację medyczną ponosi pełną odpowiedzialność za wszelkie szkody przez niego spowodowane w odległych lub lokalnych systemach komputerowych oraz za wszelkie inne straty lub nadużycia popełnione przy użyciu udostępnionych mu zasobów, sprzętu i programów użytkowych.