Polityka bezpieczeństwa ochrony i przetwarzania danych osobowych wraz z instrukcją zarządzania systemem informatycznym

w Indywidualnej Specjalistycznej Praktyce Lekarskiej Piotr Wiśniewski

wydana w dniu 19.02.2013

Zawartość

I. Wykaz zbiorów danych przetwarzanych w placówce 2

II. Zakres danych osobowych przetwarzanych w placówce 2

III. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe 3

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych 3

V. Odpowiedzialność 4

VI. Rejestr użytkowników 4

VII. Instrukcja dotycząca sposobu zarządzania systemem informatycznym 5

A. Zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania 5

B. Procedura rozpoczęcia i zakończenia pracy 6

C. Zabezpieczenie systemu przed nieuprawnionym dostępem 6

D. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych 7

VIII. Wydruki 7

IX. Zasady udostępniania danych 7

X. Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa 8

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych w celach określonych w art. 27 ust. 2 pkt 7 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) przetwarzanych przez Indywidualną Specjalistyczną Praktykę Lekarską Piotr Wiśniewski (w skrócie: ISPL Piotr Wiśniewski) przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka obowiązuje wszystkich pracowników ISPL Piotr Wiśniewski oraz dostawców, podmiotów współpracujących na podstawie umów cywilnoprawnych, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Przetwarzanie danych osobowych w ISPL Piotr Wiśniewski odbywa się za pomocą systemów informatycznych.

Administratorem Danych Osobowych jest Kierownik ISPL Piotr Wiśniewski, który pełni rolę także Administratora Bezpieczeństwa Informacji oraz Administratora Systemu Informatycznego.

Słownik :

1. ABI - administrator bezpieczeństwa informacji, przez którego należy rozumieć pracownika ISPL Piotr Wiśniewski wyznaczonego do nadzorowania przestrzegania zasad ochrony, określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów prawa.

2. Administrator danych osobowych- należy przez to rozumieć : Kierownik jednostki.

3. ASI - administrator systemu informatycznego- osoba odpowiedzialna za funkcjonowanie systemu informatycznego ISPL Piotr Wiśniewski.

4. Dane osobowe - wszelkie informacje umożliwiające zidentyfikowanie osoby korzystającej z usług medycznych w ISPL Piotr Wiśniewski.

5. Identyfikator- należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym tzw. login.

6. Pracownik - należy przez to rozumieć osobę zatrudnioną w formie umowy o pracę lub umowy cywilno-prawnej.

7. Użytkownik systemu - należy przez to rozumieć osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym ISPL Piotr Wiśniewski. Użytkownikiem systemu może być pracownik ISPL Piotr Wiśniewski wykonujący pracę na podstawie umowy o pracę, umowy zlecenia lub innej umowy cywilno- prawnej.

8. Ustawa - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

I. Wykaz zbiorów danych przetwarzanych w placówce

Wykaz zbiorów danych przetwarzanych w placówce wymieniony jest w załączniku nr 1 do niniejszej polityki bezpieczeństwa, będący jej integralną częścią.

II. Zakres danych osobowych przetwarzanych w placówce

W ISPL Piotr Wiśniewski utworzono i wydzielone następujące zbiory danych osobowych:

- A. "Rejestr Pacjentów", w którym przetwarzane są następujące dane: imię i nazwisko, adres zamieszkania, numer telefonu, adres e-mail, nr PESEL,

III. Wykaz budynków, pomieszczeń lub części pomieszczeń, w których przetwarzane są dane osobowe

1. Przetwarzanie danych osobowych odbywa się w pomieszczeniach, w których funkcjonuje ISPL Piotr Wiśniewski:

    - Gdańsk, ul. Asnyka 9/1

2. Pomieszczenia, w których przetwarzane są dane osobowe chronione są systemem alarmowym. Dostęp do stref przetwarzania danych osobowych mają jedynie upoważnieni pracownicy oraz ABI. System jest wyłączany przez ostatniego pracownika opuszczającego pomieszczenie, w którym przetwarzane są dane osobowe. ABI ma obowiązek kontroli, nie rzadziej niż raz na 14 dni, historii operacji wykonywanych w strefach przetwarzania danych osobowych. Z kontroli tych sporządza protokół według wzoru stanowiącego Załącznik A.

3. Zabrania się przebywania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe bez obecności osób upoważnionych.

IV. Procedury nadawania i zmiany uprawnień do przetwarzania danych osobowych

1. Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z następującymi dokumentami:

    a. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity - Dz. U. z 2002 r. Nr 101 poz.926 z późn. zm.),

    b. rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024)

    c. niniejszą polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym.

2. Zapoznanie się z powyższymi dokumentami użytkownik systemu potwierdza własnoręcznym podpisem na oświadczeniu, którego wzór stanowi Załącznik nr 2.

3. Przetwarzania danych osobowych może dokonywać jedynie użytkownik systemu upoważniony przez administratora danych osobowych. Wzór upoważnienia stanowi Załącznik nr 3.

4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez ASI dla każdego użytkownika systemu unikalnego identyfikatora hasła ze wskazaniem zakresu dostępnych danych i operacji.

5. Hasło pierwszego logowania w systemie ustanawia ABI. Każdy użytkownik systemu informatycznego ma obowiązek dokonać jego zmiany na indywidualne, co najmniej

pięcioznakowe hasło, w skład którego muszą wchodzić litery oraz cyfry. Ustanowione hasło indywidualne, użytkownik systemu przekazuje ABI w zamkniętej i podpisanej kopercie.

V. Odpowiedzialność

1. Użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony.

2. Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy ABI użyje hasła użytkownika podczas jego nieobecności. ABI ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany kierownik jednostki oraz użytkownik systemu, którego hasło zostało użyte. Po zapoznaniu się z protokołem, użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je ABI. Zapis pkt IV.5 zd. 3 stosuje się odpowiednio.

3. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

4. Na pisemny i uzasadniony wniosek koordynatora komórki organizacyjnej ABI może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień. W uzasadnionej sytuacji ABI może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości kierownika jednostki, koordynatora komórki organizacyjnej i użytkownika systemu, którego sprawa dotyczy.

5. Hasło oraz uprawnienia użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ASI.

6. Użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

VI. Rejestr użytkowników

1. ABI jest zobowiązany do prowadzenia i ochrony rejestru użytkowników i ich uprawnień w systemie informatycznym.

2. Rejestr musi odzwierciedlać aktualny stan systemu w zakresie użytkowników i ich uprawnień oraz umożliwić przeglądanie historii zmian w systemie informatycznym.

3. Rejestr, którego wzór stanowi Załącznik nr 4 zawiera:

a) imię i nazwisko użytkownika,
b) identyfikator użytkownika,
c) zakres uprawnienia,
d) datę nadania uprawnień,
e) datę odebrania uprawnień,
f) przyczynę odebrania uprawnień,

g) podpis ABI.

VII. Instrukcja dotycząca sposobu zarządzania systemem informatycznym

A. Zasady zabezpieczania sprzętu informatycznego, danych i oprogramowania

Uwzględniając kategorie przetwarzanych danych osobowych oraz zagrożenia wprowadza się wysoki poziom bezpieczeństwa w systemie informatycznym służącym do przetwarzania danych osobowych, zgodnie ze stosownym rozporządzeniem właściwego ministra.

1. Kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie. Pomieszczenia, w których znajduje się sprzęt komputerowy służący do przetwarzania danych osobowych wyposażone są w solidne zamki oraz elektroniczny system kontroli dostępu. Ostatni z pracowników, który opuszcza pomieszczenie ma obowiązek zamknąć drzwi na klucz oraz załączyć czujniki ruchu.

2. Kopie danych zawartych w systemie tworzy się każdorazowo po zakończeniu dnia pracy. Kopia tworzona jest przez ASI/ABI , przechowywana jest na zdalnym serwerze, do którego dostęp ma wyłącznie ASI/ABI. Każda następna kopia zapisywana jest w miejsce poprzedniej.

3. Pliki zawierające dane osobowe (np. skany wyników badań) nie mogą być przechowywane na wymienialnych nośnikach tj. płyty cd, pendrive, dyski zewnętrzne.

4. W systemie komputerowym ISPL Piotr Wiśniewski pliki zawierające dane osobowe mogą być przechowywane wyłącznie w postaci zaszyfrowanej. Pliki są usuwane z komputera w sposób uniemożliwiający ich odzyskanie (np. standard DOD 5220.22 lub algorytm Gutmanna).

5. Komputer będący elementem sytemu ISPL Piotr Wiśniewski musi posiadać zainstalowane mechanizmy ochronne oraz komercyjne oprogramowanie antywirusowe. Należy dochować wszelkiej staranności, aby zapobiec kradzieży komputera.

6. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:

   a) likwidacji- pozbawia się danych poprzez formatowanie oraz fizyczne uszkodzenie, uniemożliwiające ich odczytanie,

   b) przekazania- pozbawia się zapisu zawierającego dane osobowe,

   c) naprawy- pozbawia się zapisu danych osobowych lub naprawia pod nadzorem osoby do tego upoważnionej przez ABI.

7. Na stanowiskach pracy, na których przetwarzane są dane osobowe, ekrany monitorów powinny być ustawione w sposób uniemożliwiający osobom trzecim wgląd w wyświetlane informacje.

8. W razie przerwania pracy stosuje się „wygaszacz ekranu”

9. Każdy z komputerów zabezpieczony jest hasłem dostępu, składającym się z co najmniej pięciu znaków, w skład których wchodzą zarówno litery jak i cyfry. Każdy z pracowników ma obowiązek comiesięcznej zmiany hasła dostępu do komputera.

B. Procedura rozpoczęcia i zakończenia pracy

1. Komputer uruchamia się po wprowadzeniu do niego hasła.
2. Przy wejściu do systemu przetwarzającego dane osobowe wprowadza się identyfikator oraz hasło dostępu.
3. Zakończenie pracy związanej z przetwarzaniem danych odpowiadać winno wszystkim regułom bezpieczeństwa informacji.

C. Zabezpieczenie systemu przed nieuprawnionym dostępem

1. Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:
   a) na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe,
   b) każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,
   c) aktualizacje programów antywirusowych muszą być dokonywane nie rzadziej niż raz w tygodniu,
   d) zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
   e) zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.
2. Każdy użytkownik systemu musi zostać przeszkolony z obsługi programu antywirusowego, co poświadcza stosownym podpisem, zgodnie z załącznikiem B do niniejszej polityki bezpieczeństwa.
3. ABI przeprowadza cykliczne kontrole antywirusowe na wszystkich komputerach systemu nie rzadziej niż raz na 14 dni kalendarzowych. Z kontroli tych sporządza się protokół zgodnie z załącznikiem C do niniejszej polityki bezpieczeństwa, stanowiącym jej integralną cześć.
4. Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.

D. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

1. Procedury naprawy sprzętu komputerowego:

   a) naprawa sprzętu komputerowego użytkowanego w systemie może odbywać się w siedzibie biura i dokonywać jej może jedynie wyspecjalizowaną firma informatyczna. Czynności te muszą być wykonywane w obecności ABI lub ASI lub innego upoważnionego przez nich użytkownika systemu,

   b) naprawa sprzętu komputerowego użytkowanego w systemie poza siedzibą biura musi zostać poprzedzona usunięciem z twardego dysku wszelkich aplikacji przetwarzających i zawierających dane o charakterze osobowym. ASI odpowiedzialny jest za stworzenie kopii tej bazy, która jest przechowywana jest na zdalnym serwerze, do którego dostęp ma wyłącznie ASI. Po powrocie z serwisu sprzętu komputerowego, ASI ponownie instaluje bazę danych.

2. Procedura przeglądu systemu:

   a) przeglądu systemu dokonuje firma informatyczna obsługująca jednostkę pod względem informatycznym,

   b) czynności przeglądowe muszą odbywać się w obecności ASI lub ABI lub innego upoważnionego przez nich pracownika.

VIII. Wydruki

1. ISPL Piotr Wiśniewski nie przechowuje wydruków, kartotek ani dokumentów papierowych, na których znajdują się dane osobowe.

2. Wydruki zawierające dane osobowe przeznaczone do usunięcia niszczy się w niszczarce, natomiast inne przechowywane są w warunkach uniemożliwiających dostęp do nich osób nieupoważnionych.

IX. Zasady udostępniania danych

1. Dane osobowe przetwarzane zgodnie z art. 27 ust. 2 pkt 7 ustawy mogą być wydane jedynie na pisemny wniosek osoby, której dotyczą lub pisemny wniosek osoby upoważnionej na piśmie przez zainteresowanego.

2. Dopuszcza się przekazywanie danych osobowych, o których mowa w art. 27 ust. 2 pkt 7 ustawy podmiotom i organom upoważnionym na podstawie odrębnych przepisów, wskazanym w art. 26 ustawy z dnia 6 listopada 2008r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2009r. nr 52 poz. 417)

3. Wzór wniosku o udostępnienie danych osobowych, o których mowa w rozdziale IX ust.1 niniejszej polityki bezpieczeństwa stanowi załącznik nr 5.

4. Z czynności przekazania danych, o których sporządza się protokół przekazania, którego wzór stanowi Załącznik nr 6.

5. ABI zobowiązany jest do prowadzenia ewidencji udostępniania danych osobowych ze zbiorów zgodnie z załącznikiem nr 7.

6. Dokumentacja medyczna jest udostępniana:

   a) do wglądu w siedzibie ISPL Piotr Wiśniewski,

   b) poprzez sporządzenie jej wyciągów, odpisów lub kopii,

   c) poprzez wydanie oryginału za pokwitowaniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, jeżeli uprawniony podmiot lub organ żąda udostępnienia oryginałów tej dokumentacji.

X. Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ABI lub inną upoważnioną osobę.

2. ABI (lub upoważniona osoba) w porozumieniu z ASI po otrzymaniu powiadomienia:

   a) sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,

   b) sprawdza sposób działania programów (w tym obecność wirusów komputerowych),

   c) sprawdza jakość komunikacji w sieci telekomunikacyjnej,

   d) sprawdza zawartość zbioru danych osobowych,

   e) poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.

3. W przypadku stwierdzenia naruszenia zabezpieczeń danych administrator:

   a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),

   b) w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,

c) zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,

d) niezwłocznie przywraca prawidłowy stan działania systemu,

e) dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

f) sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ABI przekazuje administratorowi danych osobowych.

5. ABI, w porozumieniu z administratorem danych osobowych, podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:

a) jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenia antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

b) jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza się dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wnioskuje do administratora danych osobowych o wyciągnięcie konsekwencji przewidzianych prawem,

c) jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organy ścigania.