Prawo i bezpieczeństwo przekazu medycznych danych osobowych zgodnie z dyrektywą europejską i polskim ustawodawstwem

Dr n. med. Leszek Sikorski
Centrum Systemów Informacyjnych Ochrony Zdrowia

Legionowo 18 września 2008 r.

Uwarunkowania europejskie

- Konwencja Nr 108 Rady Europy z 28.01.1981 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
- Dyrektywa 95/46 EC Parlamentu Europejskiego wydana wspólnie z Radą Unii Europejskiej z 24.10. 1995 r., dotycząca ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz wolnego przepływu danych (uszczegółowienie Konwencji).

Uwarunkowania europejskie II

- Wytyczne OECD w zakresie ochrony prywatności i przepływu danych osobowych przez granice
- Wytyczne OECD w zakresie bezpieczeństwa systemów informatycznych
- Rekomendacja R (97) 5 Komitetu Ministrów do Państw Członkowskich dotycząca ochrony medycznych danych osobowych

Prawo do ochrony danych osobowych, jako element prawa do prywatności

- Art. 47 Konstytucji gwarantujący obywatelom prawo do prywatności
- art. 51 Konstytucji zgodnie z którym nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby a także, że zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

- sytuacje, w których przetwarzanie jest dopuszczalne
- prawa osób, których dane dotyczą
- obowiązki administratorów danych

Rozporządzenie wykonawcze

- Rozporządzenie 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.

Główne cele w ochronie zdrowia do których potrzebne jest przetwarzanie danych

- Świadczenie opieki – np. Dokumentacja medyczna
- Badania kliniczne
- Procesy administracyjne
- Statystyka

Zagrożenia i ich zakres - uwarunkowania

- Poziom ochrony danych, wg którego dane są chronione przed nieupoważnionym dostępem podczas przechowywania lub przesyłania
- Liczba osób, które mają upoważnienie dostępu
- Rodzaj przechowywanych danych medycznych
- Poziom trudności w identyfikowaniu osoby, do której danych uzyskano dostęp

Wybrane pojęcia

- Przetwarzanie danych osobowych
- Medyczne dane osobowe
- Identyfikowalna osoba
- Zgoda osoby, której dotyczą dane

Europejska dyrektywa o ochronie danych osobowych

- Cele ogólne
- Zakres obowiązywania – przetwarzanie elektroniczne i nieelektroniczne
- Zasady dotyczące jakości danych
- Kryteria legalności

Osobowe dane medyczne – prawa osoby, której dotyczą dane

- Informacje przekazywane osobie, której dotyczą dane
- Prawo dostępu do danych
- Prawo do sprzeciwu
- Środki sądowe, odpowiedzialność i sankcje

Obowiązki administratora

- Środki techniczne i organizacyjne
- Wybór przetwarzającego
- Zależność administratora i przetwarzającego

Przesyłanie osobowych danych medycznych – do kraju poza UE

- Przekazywanie możliwe jest tylko wtedy, gdy ten kraj zapewnia właściwą ochronę danych
- Odstępstwa od zakazów
- Zapewnianie dopuszczalności przesyłania danych

Podstawy zapewnienia dopuszczalności przesyłania danych

- Kraj EEA (Szwajcaria)
- Depersonalizacja danych
- Wyrażenie zgody przez zainteresowaną osobę
- Podleganie warunkom umowy
- Żądanie prawidłowej ochrony

Polityka bezpieczeństwa w odniesieniu do państw trzecich

- Wymagania
- Cel polityki bezpieczeństwa

Zapewnienie bezpieczeństwa

- Zasady ogólne
- Zasady o niższym stopniu ogólności
- Wytyczne
- „Środki”

HLSP – High Level Security Policy 1

- Zawartość
- Wsparcie ze strony kierownictwa jednostki organizacyjnej
- Dokumentowanie zastosowanych środków
- Osoby odpowiedzialne
- Zgoda na przetwarzanie
- Informowanie o przetwarzaniu

HLSP – High Level Security Policy-2

- Zakaz dalszego przekazywania danych bez uzyskania zgody
- Ochrona i odszkodowania
- Bezpieczeństwo przetwarzania
- Odpowiedzialność personelu o innych kontrahentów
- Prawidłowość ochrony danych w państwie trzecim

Działania wspierające w zakresie bezpieczeństwa przetwarzania

- Cele ogólne
- Szyfrowanie i podpisy elektroniczne
- Kontrola dostępu i uwierzytelnianie użytkowników
- Zapis przebiegu zdarzeń

Działania wspierające w zakresie bezpieczeństwa przetwarzania II

- Bezpieczeństwo fizyczne i środowiskowe
- Zarządzanie aplikacjami i sieciami
- „Wirusy”
- Naruszenia bezpieczeństwa

Działania wspierające w zakresie bezpieczeństwa przetwarzania III

- Plan ciągłości działania
- Posługiwanie się danymi szczególnie wrażliwymi
- Normy

Metoda ankietowa oceny prawidłowości ochrony danych

- Rodzaj i okoliczności przesyłania
- Przegląd środowiska regulacyjnego
- Ograniczenia celu, przejrzystość i sprzeciw
- Jakość danych i proporcjonalność

Metoda ankietowa oceny prawidłowości ochrony danych II

- Bezpieczeństwo
- Dostęp i poprawianie
- Ograniczenia dalszego przesyłania
- Środki zaradcze

Metodologia pochodzi z pracy “Worst Case Scenarios: the Legal Consequences”, Barber B, Vincent R and Scholes M, pp 282 - 288, Current Perspectives in Healthcare Computing 1992, ed Richards B et al, pub for British Computer Society by BJHC Weybridge, ISBN 0 948198 12 5

Dziękuję za uwagę

l.sikorski@csioz.gov.pl