PROXIMUS
INTEGRACJA INFORMACJI

NOWE WYZWANIA DLA MEDYCYNY I INFORMATYKI
20 MARCA 2015

Bezpieczeństwo danych - ryzyka

ANALIZA RYZYKA W BEZPIECZEŃSTWIE INFORMACJI

PYTANIA

- Co chronimy i przed kim?
- Jaką wartość ma informacja /uwzględniając konsekwencje jej wycieku/?
- Jakie zagrożenia związane są z brakiem informacji na czas?

KONTEKST

- Bezpieczeństwo wrażliwych danych medycznych w rozumieniu regulacji prawnych i kontraktowych
- Wpływ interesariuszy na bezpieczeństwo informacji

ANALIZA RYZYKA W BEZPIECZEŃSTWIE INFORMACJI

Ryzyka prawne

prawdopodobieństwo poniesienia **strat** materialnych i niematerialnych powstające m.in.: na skutek

- błędnego lub zbyt późnego uchwalenia regulacji prawnych;
- niestabilności uregulowań prawnych /ponad 400 projektów ustaw i rozporządzeń przygotowanych przez Ministerstwo Zdrowia/
- zmian w orzecznictwie;
- niewłaściwego ukształtowania stosunków prawnych;
- niekorzystnych rozstrzygnięć sądów lub jednostek nadrzędnych rozstrzygających sprawy sporne powstających na tle stosunków prawnych danej jednostki z otoczeniem zewnętrznym,
- czynnika ludzkiego

ANALIZA RYZYKA W BEZPIECZEŃSTWIE INFORMACJI

ROZPORZĄDZENIE MINISTRA ZDROWIA

z dnia 25 czerwca 2013 r. **w sprawie Systemu Statystyki w Ochronie Zdrowia**

§ 4

2. System zarządzania bezpieczeństwem informacji spełnia wymagania określone w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne dla systemu zarządzania bezpieczeństwem informacji oraz uwzględnia, w zakresie zarządzania bezpieczeństwem informacji w ochronie zdrowia, normę **PN-EN ISO 27799:2010** Informatyka w ochronie zdrowia – Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem **ISO/IEC 27002**, albo normę lub wersję normy ją zastępującą

ANALIZA RYZYKA W BEZPIECZEŃSTWIE INFORMACJI

ROZPORZĄDZENIE RADY MINISTRÓW

z dnia 12 kwietnia 2012 r**. w sprawie Krajowych Ram Interoperacyjności**

Rozdział IV. § 20. 3

Wymagania określone [..w rozporządzeniu..] uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy **PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:. **1) PN-ISO/IEC 17799, 2) PN-ISO/IEC 27005, 3) PN-ISO/IEC 24762**

PROXIMUS
INTEGRACJA INFORMACJI

ANALIZA RYZYKA W BEZPIECZEŃSTWIE INFORMACJI

STANDARDY

ISO 31000 SYSTEM ZARZĄDZANIA RYZYKIEM

ujęcie organizacyjne i zarządcze

ISO 27005 SYSTEM ZARZĄDZANIA RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI

ochrona **aktywów** informacyjnych organizacji

POSTEPOWANIE Z RYZYKIEM

- Akceptacja ryzyk,
- Przenoszenie ryzyk,
- Unikanie ryzyk

PROXIMUS
INTEGRACJA INFORMACJI

POUFNOŚĆ – INTEGRALNOŚĆ – DOSTĘPNOŚĆ

ZASADA PID

Kto ma dostęp do danych medycznych?
Sposoby autoryzacji i autentykacji dostępu do danych medycznych

OCHRONA DANYCH OSOBOWYCH

Odpowiedzialność Administratora Danych za bezpieczeństwo danych

WRAŻLIWOŚĆ DANYCH MEDYCZNYCH

Dokumentacja w zakresie ochrony danych uwzględniająca **art. 27** Ustawy o ochronie danych osobowych

- Wykaz zbiorów danych osobowych z określeniem systemu i aplikacji
- Zakres danych osobowych przetwarzanych w systemach
- Sposób przemieszczania danych pomiędzy systemami

Motto

Bo wypadek to dziwna rzecz, nigdy go nie ma dopóki się nie wydarzy!!!

PROXIMUS
INTEGRACJA INFORMACJI

Przemysław Bańko
przemyslaw.banko@proximus-it.pl
608 090 880

Dziękuję za uwagę