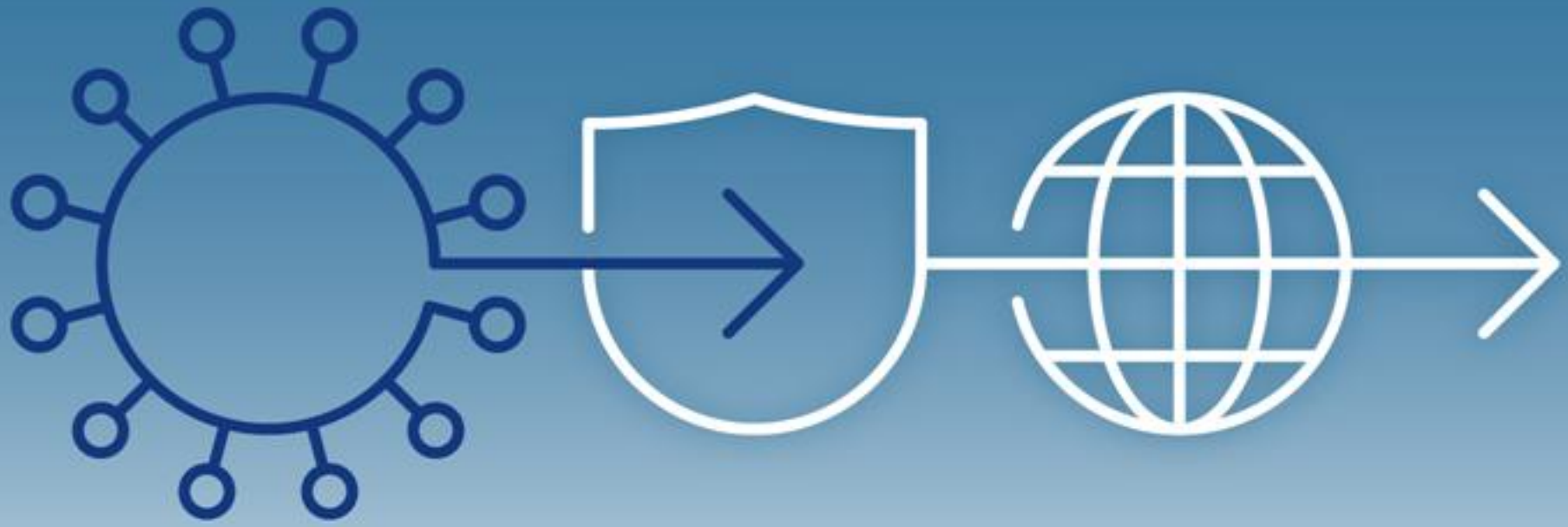
Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Naukowe Centrum Prawno-informatyczne

Bezpieczeństwo elektronicznej dokumentacji medycznej

Autor: dr inż. Krzysztof Świtała

Wydział Prawa i Administracji UKSW

Regulacje

Prawne:

- Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania wydane na podstawie art. 30 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta
- Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia
- 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)
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – operatorzy usług kluczowych

Normy techniczne:

ISO 27799 - Informatyka w ochronie zdrowia - Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002

Zabezpieczenie dokumentacji medycznej –podstawowe założenia (§ 1 ust. 4 r.d.m.)

- jest zapewniona jej **dostępność wyłącznie dla osób uprawnionych**, o których mowa w art. 24 ust. 2 i art. 26 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz innych przepisach prawa powszechnie obowiązującego;
- są **zastosowane metody i środki ochrony dokumentacji**, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Zabezpieczenie dokumentacji medycznej - wymagania (§ 1 ust. 5 r.d.m.)

- systematycznego szacowania ryzyka zagrożeń oraz **zarządzania tym ryzykiem**;
- opracowania i stosowania **udokumentowanych procedur** zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania;
- stosowania **środków bezpieczeństwa adekwatnych do zagrożeń**, uwzględniających najnowszy stan wiedzy;
- dbałości o **aktualizację oprogramowania**;
- bieżącego **kontrolowania funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia**, a także **okresowego dokonywania oceny skuteczności** tych sposobów;
- przygotowania i realizacji **planów przechowywania dokumentacji** w długim czasie, w tym jej przenoszenia na informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

Zabezpieczenie systemu teleinformatycznego służącego do prowadzenia dokumentacji medycznej - wymagania (§ 1 ust. 6 r.d.m.)

- integralność treści dokumentacji i metadanych polegającą na **zabezpieczeniu przed wprowadzaniem zmian**, z wyjątkiem zmian wprowadzanych w ramach udokumentowanych procedur;
- **stały dostęp do dokumentacji dla osób uprawnionych** oraz zabezpieczenie przed dostępem osób nieuprawnionych;
- wymagalność **identyfikacji osoby sporządzającej dokumentację** oraz dokonującej wpisu lub innej zmiany i zakresu dokonanych zmian w dokumentacji lub metadanych;
- informację o **czasie sporządzenia dokumentacji** oraz dokonania wpisu lub innej zmiany;
- przyporządkowanie **cech informacyjnych dla odpowiednich rodzajów dokumentacji**, zgodnie z § 10 pkt 3;
- możliwość **prowadzenia i udostępniania dokumentacji w formatach i standardach** wydanych na podstawie art. 11 ust. 1a i 1b ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2019 r. poz. 408, 730, 1590 i 1905), a w przypadku ich braku - możliwość prowadzenia i udostępniania dokumentacji w standardach HL7 oraz DICOM lub innych standardach i formatach;
- możliwość **wydruku dokumentacji**;
- możliwość **eksportu całości danych w standardach i formatach**, o których mowa w pkt 6, w sposób umożliwiający odtworzenie ich w innym systemie teleinformatycznym.

Zabezpieczenie dokumentacji medycznej – gwarancje integralności, poufności i dostępności (§ 1 ust. 7 r.d.m.)

Podmiot zapewnia odpowiednie warunki zabezpieczające dokumentację przed

- zniszczeniem, uszkodzeniem lub utratą (integralność) i
- dostępem osób nieupoważnionych, a także (poufność)
- umożliwiające jej wykorzystanie bez zbędnej zwłoki (dostępność).

Podsumowanie

- Realizacja atrybutów bezpieczeństwa informacji zawartych w dokumentacji medycznej, takich jak **poufności, integralności i dostępności**; dodatkowo mogą być brane pod uwagę inne własności, takie jak **autentyczność, rozliczalność, niezaprzeczalność i niezawodność**;
- Prowadzenie dokumentacji przetwarzania danych obejmującej polityki i **procedury**;
- Realizacja uporządkowanego procesu **zarządzania ryzykiem**;
- Kontrola dostępu – **uwierzytelnianie użytkowników** i autoryzacja zakresu dostępu do zasobów;
- Stosowanie rozwiązań **kryptograficznych**;
- Wykonywanie i zarządzanie **kopiami zapasowymi**;
- Stosowanie **otwartych formatów danych** (HL7 CDA, DICOM) – zapobieganie uzależnieniu od dostawcy oprogramowania (ang. vendor lock-in);
- Przeglądy i **ciągłe doskonalenie zabezpieczeń** organizacyjnych i technicznych.

Dziękuję za uwagę