RYMARZ · ZDORT · MARUTA

Cyberbezpieczeństwo w ochronie zdrowia

Imagine
having us
on your side.

RZMLAW.COM

Czerwiec 2024

RYMARZ · ZDORT · MARUTA

Agenda

Wyzwania związane z informatyzacją sektora ochrony zdrowia

Z czym mamy największe problemy w obszarze cyberbezpieczeństwa?

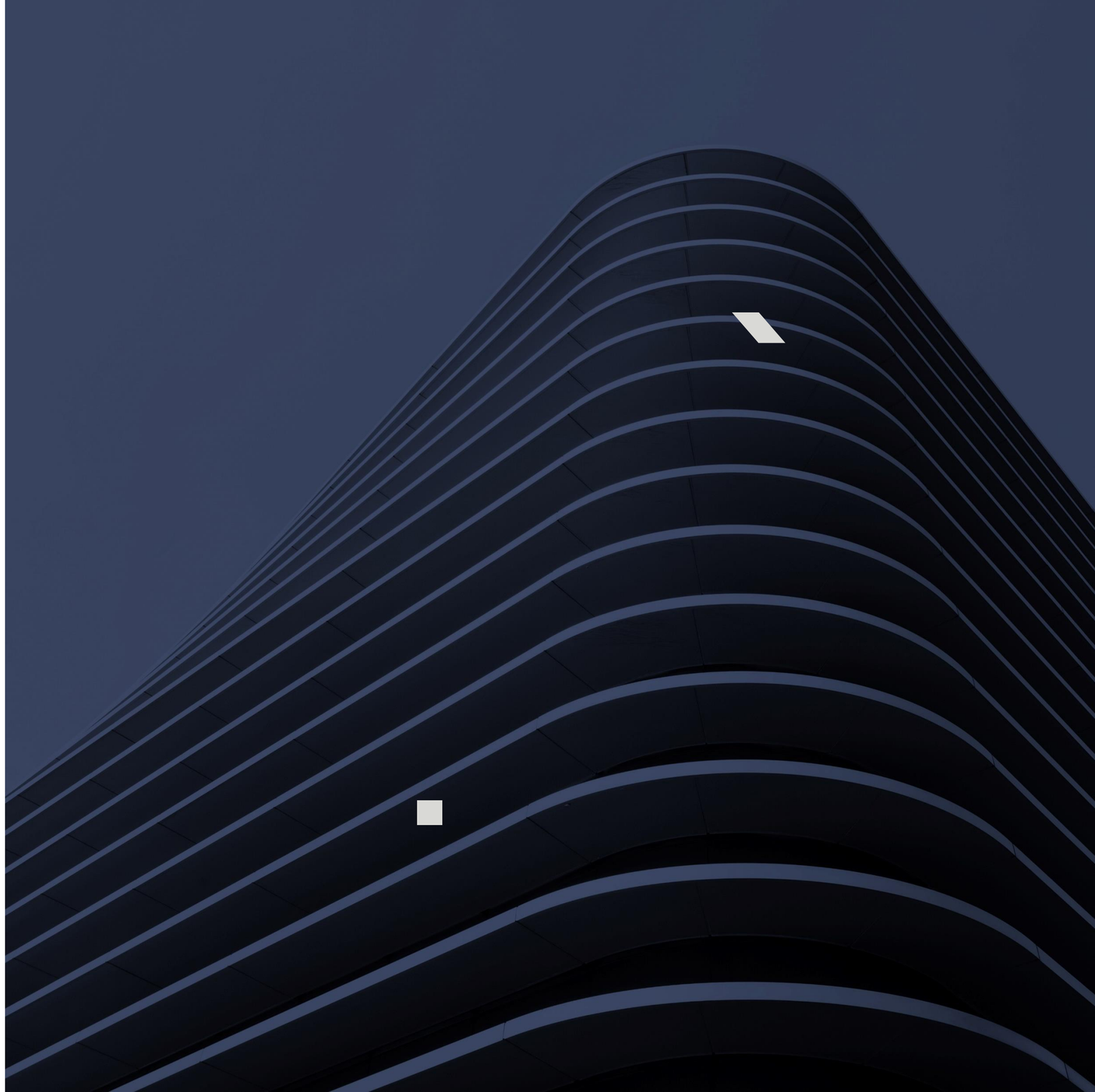
Obowiązujące wymogi prawne – wybrane regulacje

Nowelizacja Ustawy o krajowym systemie cyberbezpieczeństwa

Zestaw rekomendacji w zakresie cyberbezpieczeństwa w ochronie zdrowia

Jak sfinansować cyberbezpieczeństwo w ochronie zdrowia?

Q&A



Wyzwania związane z informatyzacją sektora ochrony zdrowia

- **Źródło danych**: VII Edycja Badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą, Grudzień 2023

Danych w postaci cyfrowej będzie dalej przybywać

Biorąc pod uwagę dostosowanie podmiotów leczniczych do wymogów ustawodawczych w zakresie EDM, jedną z kluczowych kwestii jest posiadanie przez podmiot leczniczy rozwiązania IT pozwalającego na prowadzenie dokumentacji medycznej w postaci elektronicznej oraz przetwarzanie jednostkowych danych medycznych. Deklaracje respondentów wskazują, że zdecydowana większość badanych podmiotów/praktyk **(83,3%)** posiada rozwiązania IT umożliwiające prowadzenie dokumentacji medycznej w postaci elektronicznej oraz elektroniczne przetwarzanie danych medycznych istotnych z punktu widzenia procesu leczenia, przy czym **38,0%** ankietowanych przyznało, że tylko częściowo.

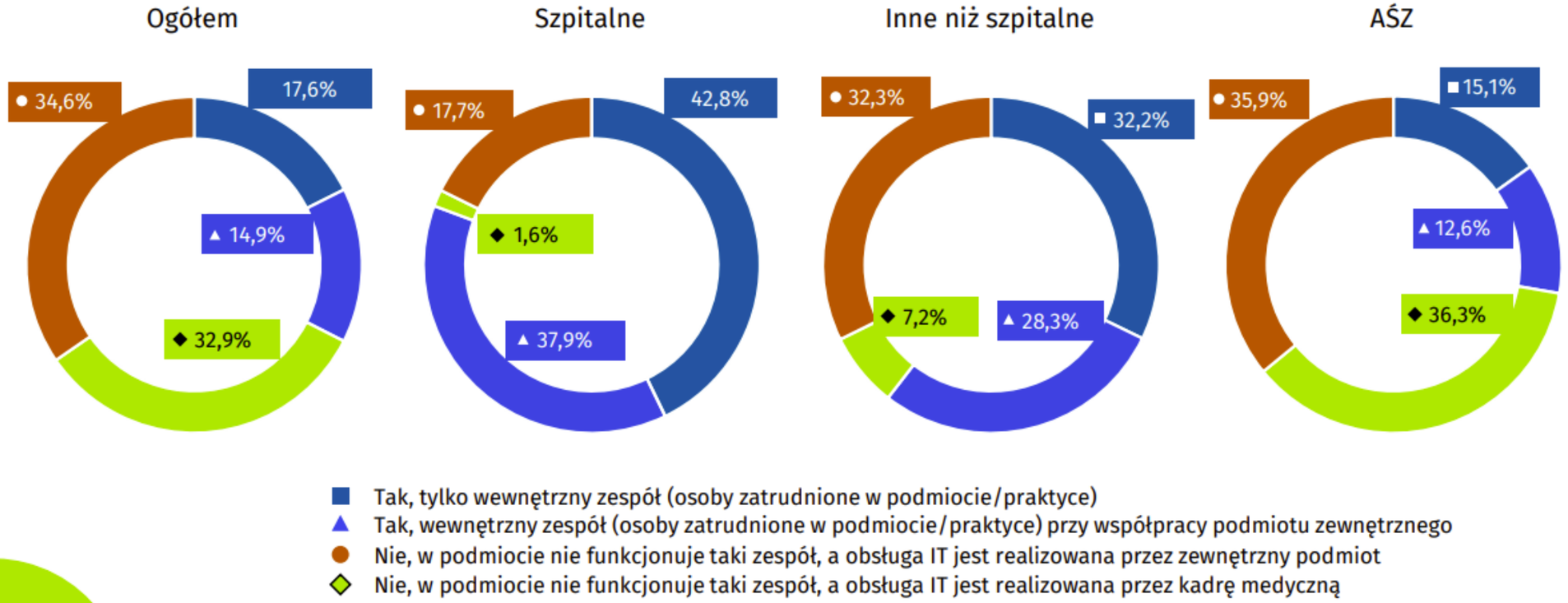
Analiza ze względu na rodzaj wykonywanej działalności wykazała, że posiadanie niezbędnych rozwiązań IT najczęściej deklarowały szpitale **(98,4%; w tym 44,5% częściowo)**, a najrzadziej ambulatoryjne świadczenia zdrowotne **(81,7%; w tym 37,2% częściowo)**.

*** Tak posiada**
^ Tak posiada, ale tylko częściowo

Rysunek 4. Czy podmiot/praktyka posiada rozwiązania IT umożliwiające prowadzenie dokumentacji medycznej w postaci elektronicznej oraz elektroniczne przetwarzanie danych medycznych istotnych z punktu widzenia procesu leczenia?

Potrzeba specjalistów w tym zakresie

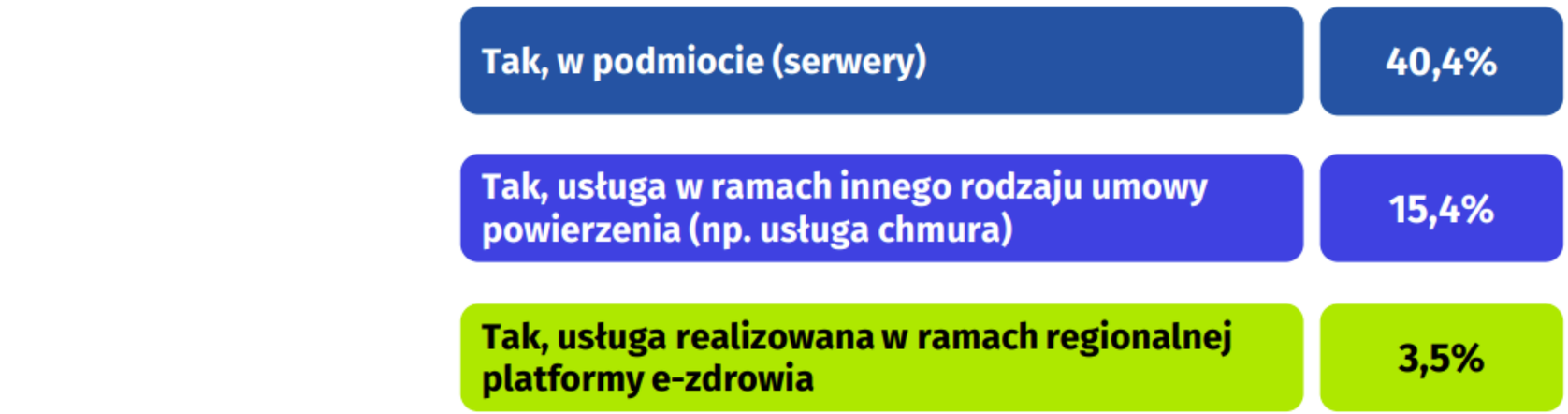
Dwie na trzy badane placówki nie posiadają wewnętrznego zespołu do obsługi informatycznej **(67,5%)**. W co trzeciej placówce zadania te zostały powierzone do realizacji podmiotowi zewnętrznemu **(34,6%)** lub obsługa IT podmiotu realizowana jest przez kadrę medyczną **(32,9%)**. Posiadanie wewnętrznego zespołu informatycznego najczęściej deklarowali przedstawiciele szpitali **(80,7%)**, a najrzadziej AŚZ **(27,7%)**.



Wykres 3. Liczba osób tworzących wewnętrzny zespół do obsługi informatycznej podmiotu/praktyki (zatrudnionych w podmiocie/praktyce).

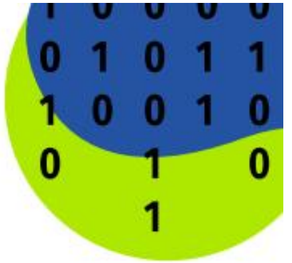
Potrzeba bezpiecznego miejsca na przechowywanie danych

Trzy na pięć ankietowanych placówek **(59,3%)** posiada Repozytorium EDM (miejsce składowania dokumentów elektronicznych wraz z metadanymi na potrzeby ich wyszukiwania). Najczęściej znajduje się ono w podmiocie **(40,4%)**. Kolejne **15,4%** badanych placówek/praktyk korzysta z usług w ramach innego rodzaju umowy powierzenia (np. usługa chmura), a jedynie **3,5%** wykorzystuje w tym celu regionalną platformę e-zdrowia.



Rysunek 12. Czy podmiot/praktyka posiada Repozytorium Elektronicznej Dokumentacji Medycznej (miejsce składowania dokumentów elektronicznych wraz z metadanymi na potrzeby ich wyszukiwania)?

Cyberbezpieczeństwo to priorytet



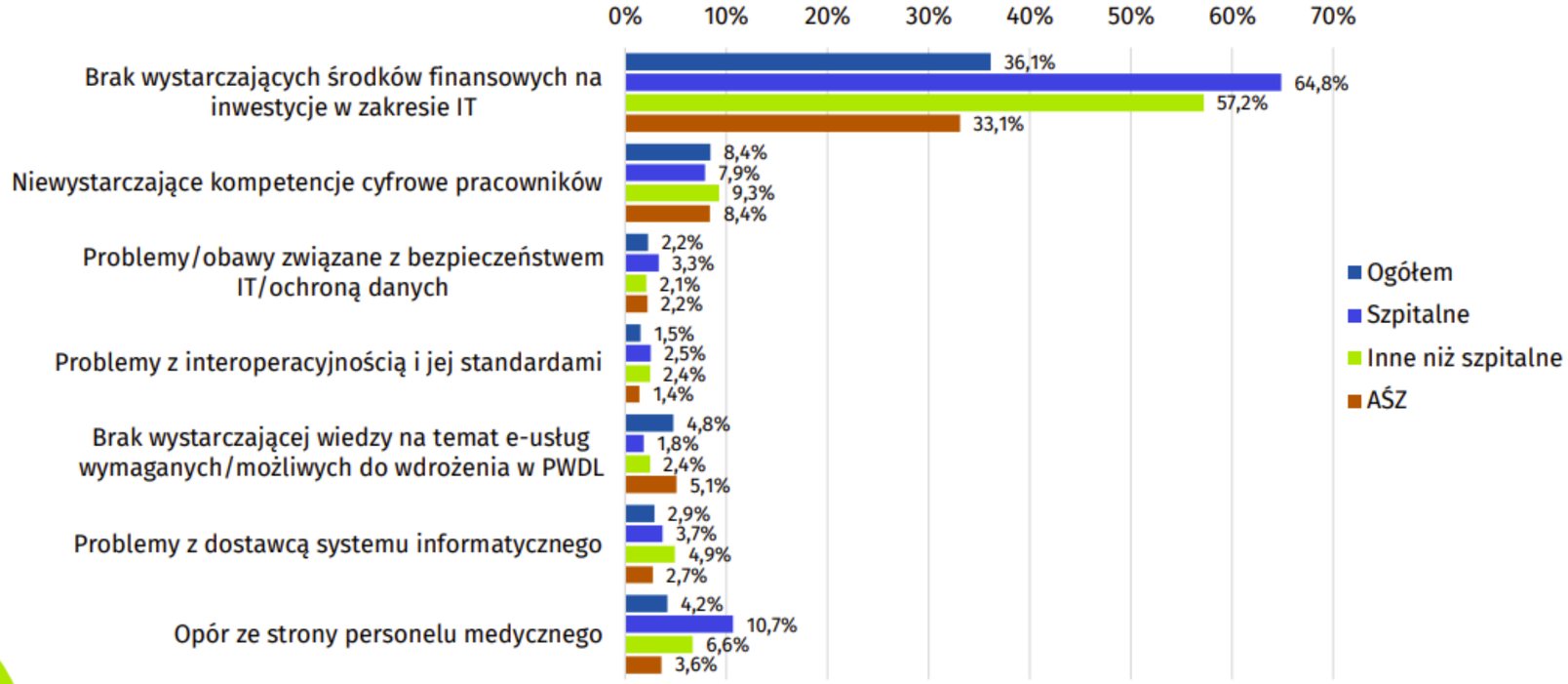
Najczęściej wskazywane potrzeby badanych placówek w zakresie cyberbezpieczeństwa to odporność na cyberataki **(25,8%)**, zwiększenie ochrony danych osobowych **(24,3%)** oraz poprawa ciągłości działania systemów informatycznych **(16,9%)**. Szersza analiza wykazała, że przedstawiciele szpitali oraz stacjonarnych i całodobowych świadczeń innych niż szpitalne najczęściej wskazywali odporność na cyberataki **(odpowiednio 31,7% i 30,1%)**, natomiast w przypadku AŚZ najwyższy odsetek wskazań odnotowano w zakresie zwiększenia ochrony danych osobowych **(26,4%)**.

Wyszczególnienie	Ogółem	Szpitalne	Inne niż szpitalne	AŚZ
Zwiększenie ochrony danych osobowych	24,3%	13,2%	15,6%	26,4%
Odporność na cyberataki	25,8%	31,7%	30,1%	24,7%
Poprawa ciągłości działania systemów informatycznych	16,9%	26,2%	20,9%	15,4%
Zwiększenie ochrony poczty elektronicznej	5,7%	8,6%	6,2%	5,3%
Poprawa stanu wiedzy o zagrożeniach informatycznych wśród pracowników/ kierownictwa jednostki	14,0%	14,5%	15,4%	13,8%
Uświadomienie ryzyka związanego ze stosowaniem systemów informatycznych	8,9%	5,9%	7,7%	9,4%
Poprawa zarządzania ryzykiem w jednostce	3,9%	5,5%	5,1%	3,6%
Inne	4,5%	8,6%	5,3%	3,9%

Tabela 2. Jakie są potrzeby podmiotu/praktyki w zakresie cyberbezpieczeństwa?

Potrzeba dofinansowania działań w tym zakresie

Kluczową barierę utrudniającą cyfryzację badanych podmiotów/praktyk stanowi brak wystarczających środków finansowych na inwestycje w zakresie IT **(36,1%)**. Taką odpowiedź wskazywały przede wszystkim szpitale **(64,8%)**. W dalszej kolejności najczęściej wskazywanym ograniczeniem były niewystarczające kompetencje cyfrowe pracowników **(8,4%)**. Odsetki takich wskazań były zbliżone we wszystkich rodzajach działalności **(od 7,9% do 9,3%)**. Należy zwrócić uwagę, że w szpitalach jako drugą najczęstszą barierę w cyfryzacji wskazywano opór ze strony personelu medycznego **(10,7%)**.



Wykres 36. Jakie bariery utrudniają cyfryzację podmiotu/praktyki?

Z czym mamy największe problemy w obszarze cyberbezpieczeństwa?

- **Źródło danych**: NIK, Informacja o wynikach kontroli - WDROŻENIE PRZEZ PODMIOTY LECZNICZE REGULACJI DOTYCZĄCYCH OCHRONY DANYCH OSOBOWYCH*
- Kontrolę NIK przeprowadzono w 24 szpitalach z sześciu województw

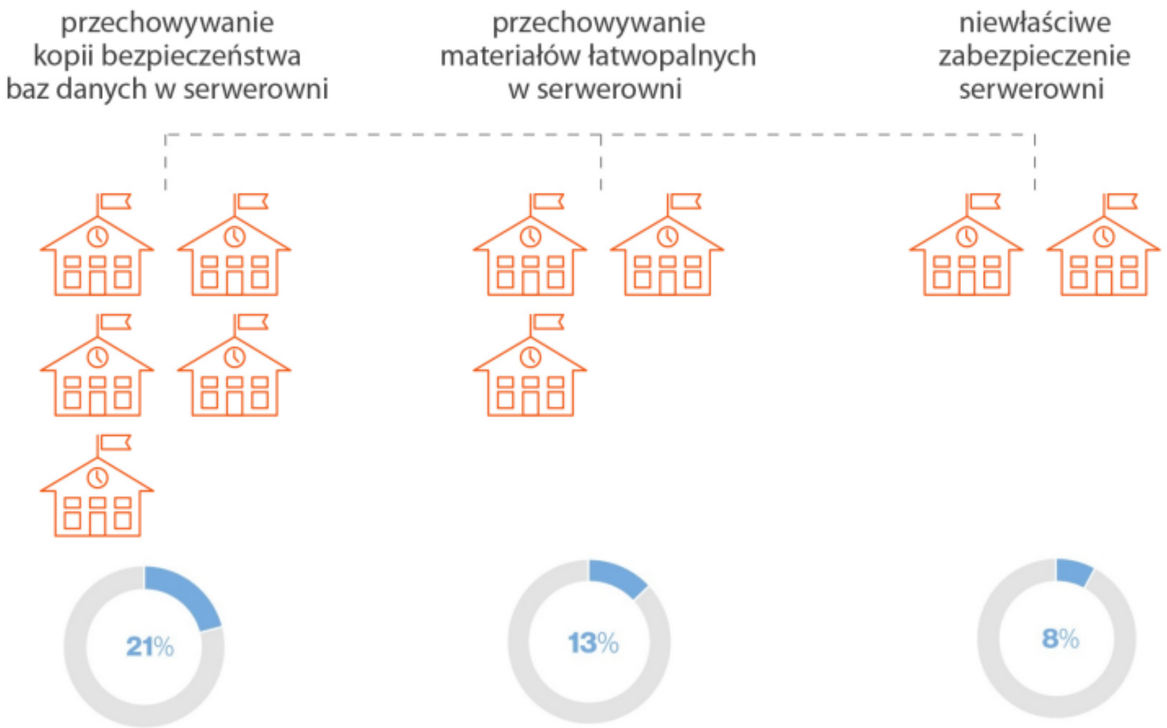
Czy właściwie przechowuję dane?

RYMARZ · ZDORT · MARUTA

14

Stwierdzony stan – bezpieczeństwo serwerowni i kopii zapasowych baz danych

Przechowywanie kopii bezpieczeństwa baz danych



Źródło: Opracowanie własne NIK na podstawie wyników kontroli.

WNIOSKI Z KONTROLI

dla organów założycielskich szpitali:

- **nadzorowanie zagadnień** związanych z ochroną danych osobowych pacjentów w podległych podmiotach leczniczych.

dla kierowników podmiotów leczniczych:

- **analizowanie ryzyka** dotyczącego ochrony danych osobowych, zgodnie z aktualną wiedzą techniczną, a następnie stosowanie rozwiązań adekwatnych do ustalonych zagrożeń,
- **wprowadzenie zindywidualizowanej autoryzacji dostępu** do posiadanych zasobów informatycznych,
- **przechowywanie kopii bezpieczeństwa** posiadanych zasobów informacyjnych w innym miejscu niż dane produkcyjne,
- **zapewnienie zabezpieczeń fizycznych** infrastruktury informatycznej, uniemożliwiających dostęp osób nieuprawnionych oraz zapewniających ochronę przed skutkami zdarzeń losowych (np. pożar, powódź, wichura),
- **przekazywanie** firmom świadczącym usługi serwisowe **jedynie danych niezbędnych do usunięcia usterek oprogramowania,**
- **regularne szkolenie** osób uczestniczących w procesach przetwarzania informacji, ze szczególnym uwzględnieniem zagrożeń bezpieczeństwa informacji, skutków naruszenia zasad bezpieczeństwa informacji, odpowiedzialności prawnej oraz stosowania środków zapewniających bezpieczeństwo informacji,

Obowiązujące wymogi prawne – kluczowe regulacje

Kluczowe regulacje

Prawo medyczne:

- Ustawa z dnia 6 listopada 2008 r. **o prawach pacjenta i Rzeczniku Praw Pacjenta** (t.j. Dz. U. z 2024 r. poz. 581).
- Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. **w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej** oraz sposobu jej przetwarzania (t.j. Dz. U. z 2024 r. poz. 798).
- Ustawa z dnia 28 kwietnia 2011 r. **o systemie informacji w ochronie zdrowia** (t.j. Dz. U. z 2023 r. poz. 2465 z późn. zm.).

Ochrona danych osobowych:

- 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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm., ,,RODO''.
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (tj. Dz. U. z 2019 r. poz. 1781z późn. zm.).

Informatyzacja państwa:

- Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie **Krajowych Ram Interoperacyjności**, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307).

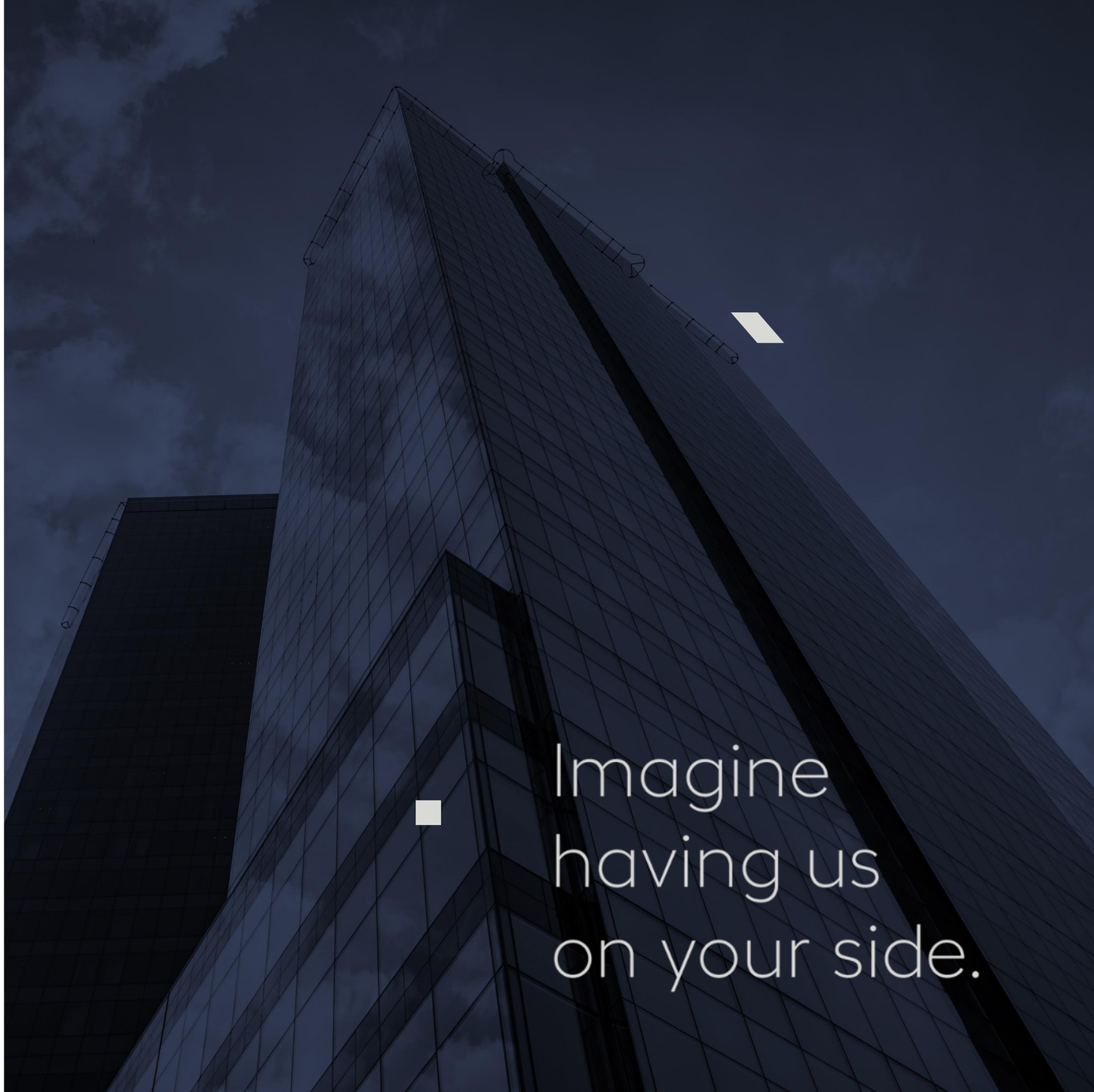
Cyberbezpieczeństwo:

- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwo (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.).
- Dyrektywa NIS 2 - powinna zostać wdrożona do polskiego porządku prawnego do dnia 18 października 2024 r. poprzez nowelizację powyższej ustawy

RYMARZ · ZDORT · MARUTA

Prawo medyczne

RZMLAW.COM



Prawo pacjenta do dokumentacji medycznej

Art. 23. [Prawo do dostępu do dokumentacji medycznej]

1. Pacjent ma prawo do dostępu do dokumentacji medycznej dotyczącej jego stanu zdrowia oraz udzielonych mu świadczeń zdrowotnych.
2. **Dane zawarte w dokumentacji medycznej podlegają ochronie określonej w niniejszej ustawie oraz w przepisach odrębnych.**

Art. 24. [Sposób prowadzenia dokumentacji medycznej; przetwarzanie danych]

1. W celu realizacji prawa dostępu do dokumentacji medycznej, podmiot udzielający świadczeń zdrowotnych jest obowiązany prowadzić, przechowywać i udostępniać dokumentację medyczną w sposób określony w niniejszym rozdziale oraz w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, a także **zapewnić ochronę danych zawartych w tej dokumentacji.**

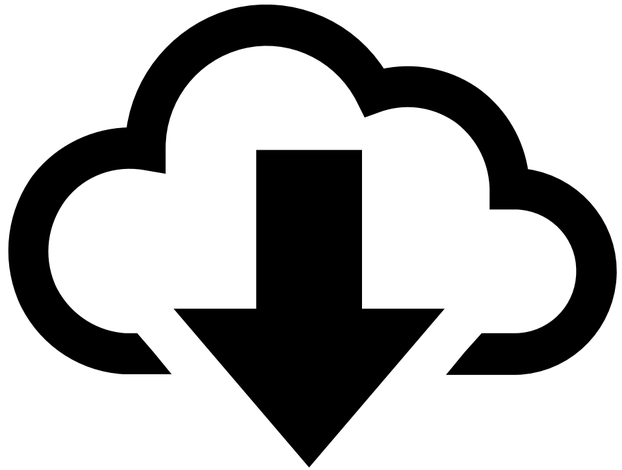
Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581).

Chmura – kluczowe regulacje

- **Jeżeli podmiot udzielający świadczeń zdrowotnych zawarł umowę o powierzeniu przetwarzania danych osobowych, realizacja tej umowy nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej.**

- Podmiot, któremu powierzono przetwarzanie danych osobowych w związku z realizacją umowy o powierzeniu przetwarzania danych osobowych jest obowiązany do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy. Podmiot ten jest związany tajemnicą także po śmierci pacjenta.

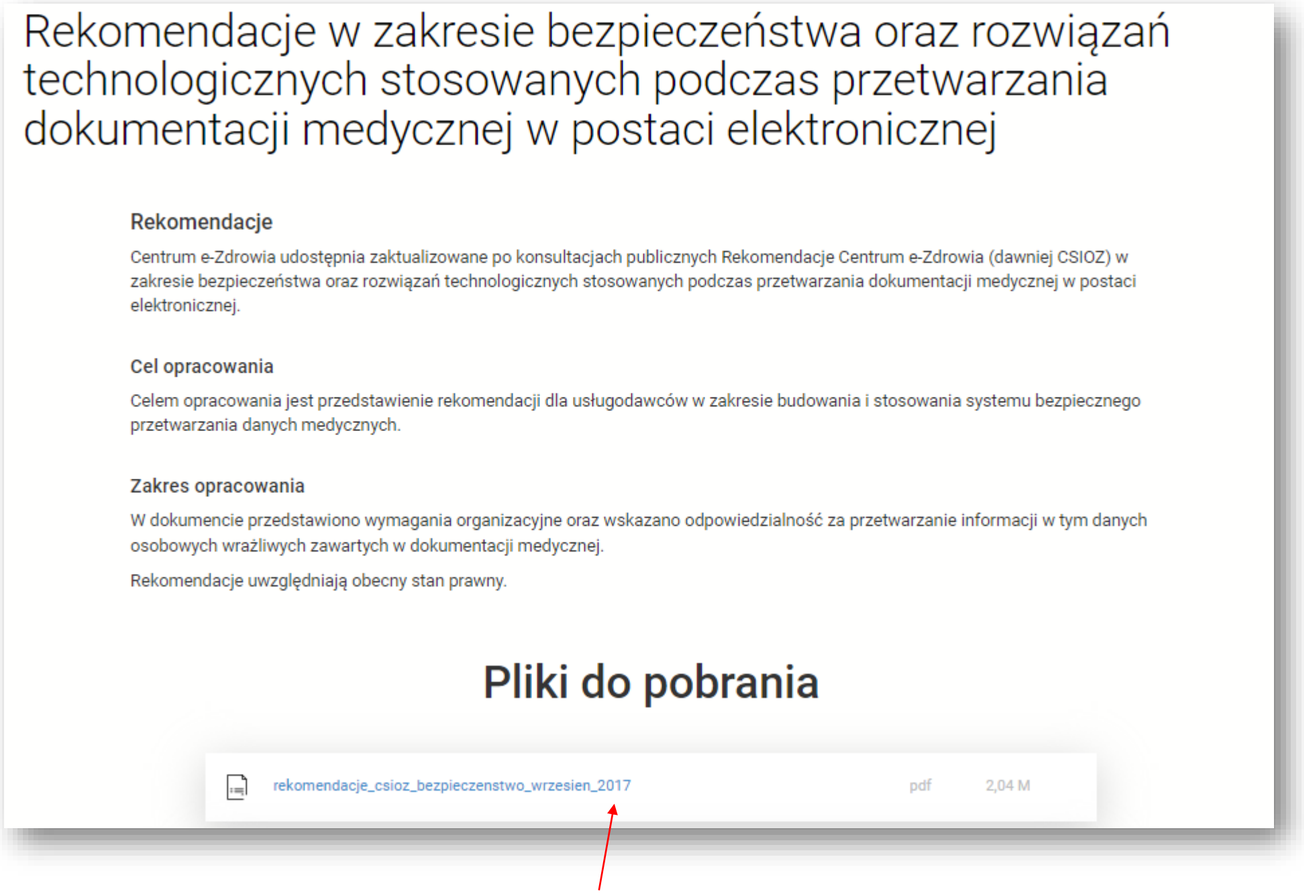
- W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, który powierzył przetwarzanie danych osobowych.



Kluczowa regulacja dla chmury obliczeniowej

Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz. U. z 2024 r. poz. 581).

Chmura w ochronie zdrowia – świadomość zmian


Rekomendacje w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej

Rekomendacje

Centrum e-Zdrowia udostępnia zaktualizowane po konsultacjach publicznych Rekomendacje Centrum e-Zdrowia (dawniej CSIOZ) w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej.

Cel opracowania

Celem opracowania jest przedstawienie rekomendacji dla usługodawców w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych medycznych.

Zakres opracowania

W dokumencie przedstawiono wymagania organizacyjne oraz wskazano odpowiedzialność za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji medycznej.

Rekomendacje uwzględniają obecny stan prawny.

Pliki do pobrania

rekomendacje_csioz_bezpieczenstwo_wrzesien_2017 pdf 2,04 M

Aktualne rekomendacje

Plan działania
w zakresie cyberbezpieczeństwa
w ochronie zdrowia

Rekomendacje Centrum E-Zdrowia w zakresie budowy systemów cyberbezpieczeństwa wersja 1.2

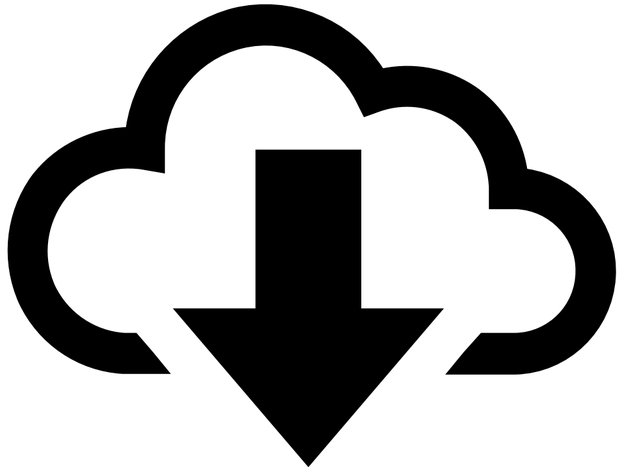
Rekomendowana jest poczta elektroniczna jako usługa. Na rynku dostępnych jest wielu dostawców usług pocztowych. Należy jednak zwrócić uwagę na dwa podstawowe parametry takiej usługi: MFA – wieloskładnikowe uwierzytelnianie oraz usługi bezpieczeństwa skrzynek pocztowych (antywirus, antymalware). Zaleca się wykorzystanie usług pocztowych w chmurze.

To jeszcze przed RODO! Wskazywane ograniczenia względem chmury są nieaktualne

Chmura w ochronie zdrowia – gdzie dalej mamy wątpliwości?

Podmioty lecznicze
w ramach zakładów karnych

Wojskowe podmioty lecznicze



Forma i zabezpieczenie dokumentacji medycznej

Forma i zabezpieczenie dokumentacji medycznej; system teleinformatyczny do prowadzenia dokumentacji medycznej

1. **Dokumentację uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:**

1) 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;
2) są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

Podmiot zapewnia odpowiednie warunki zabezpieczające dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych, a także umożliwiające jej wykorzystanie bez zbędnej zwłoki.

System teleinformatyczny, w którym jest prowadzona dokumentacja, zapewnia:

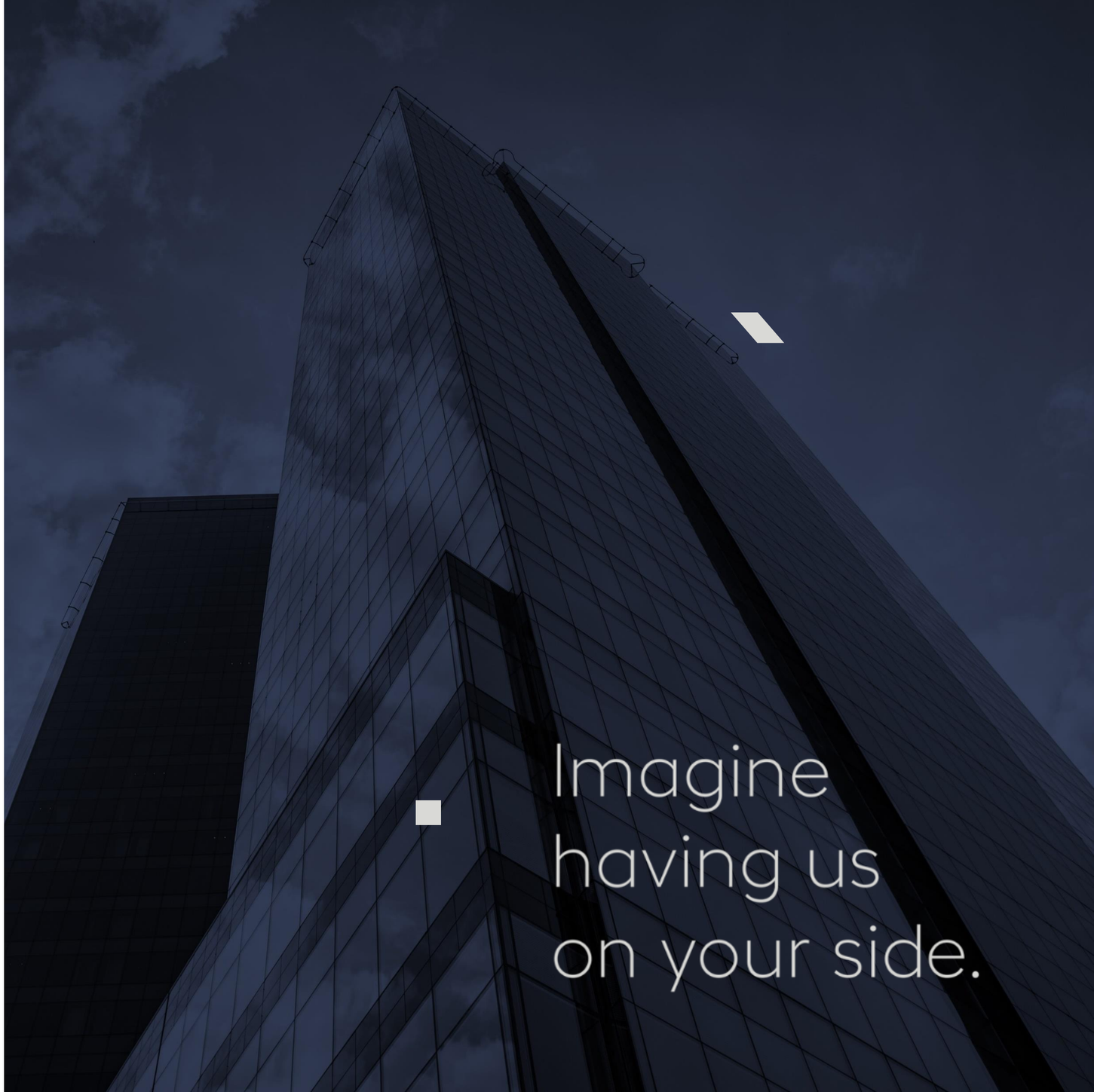
1) integralność treści dokumentacji i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem zmian wprowadzanych w ramach udokumentowanych procedur;
2) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych;
3) wymagalność identyfikacji osoby sporządzającej dokumentację oraz dokonującej wpisu lub innej zmiany i zakresu dokonanych zmian w dokumentacji lub metadanych;
4) informację o czasie sporządzenia dokumentacji oraz dokonania wpisu lub innej zmiany;
5) przyporządkowanie cech informacyjnych dla odpowiednich rodzajów dokumentacji, zgodnie z § 10 pkt 3;
6) 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 2023 r. poz. 2465), a w przypadku ich braku - możliwość prowadzenia i udostępniania dokumentacji w standardach HL7 oraz DICOM lub innych standardach i formatach;
7) możliwość wydruku dokumentacji;
8) możliwość eksportu całości danych w standardach i formatach, o których mowa w pkt 6, w sposób umożliwiający odtworzenie ich w innym systemie teleinformatycznym.

Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (t.j. Dz. U. z 2024 r. poz. 798).

RYMARZ ▪ ZDORT ◥ MARUTA

Ochrona danych osobowych

RZMLAW.COM



Bezpieczeństwo danych osobowych

Artykuł 32 RODO [Bezpieczeństwo przetwarzania]

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze**, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku**, w tym między innymi w stosownym przypadku:
    a) pseudonimizację i szyfrowanie danych osobowych;
    b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
    c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
    d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez **stosowanie zatwierdzonego kodeksu postępowania**.

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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

KODEKS POSTĘPOWANIA
DLA SEKTORA OCHRONY ZDROWIA

WYDANY ZGODNIE Z ART. 40 RODO

DOTYCZĄCY PODMIOTÓW WYKONUJĄCYCH DZIAŁALNOŚĆ LECZNICZĄ
I PODMIOTÓW PRZETWARZAJĄCYCH

Warszawa, dnia 11 grudnia 2023 r.

Wnioskodawca:

PFSz
Polska Federacja Szpitali

Podmiot monitorujący:

KPMG

Bezpieczeństwo danych osobowych

Artykuł 35 RODO [Ocena skutków dla ochrony danych]

1. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

2. **Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku** przetwarzania na dużą skalę szczególnych kategorii danych osobowych, w tym danych o stanie zdrowia.

3. **Ocena zawiera co najmniej:**
    a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora;
    b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
    c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz
    d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

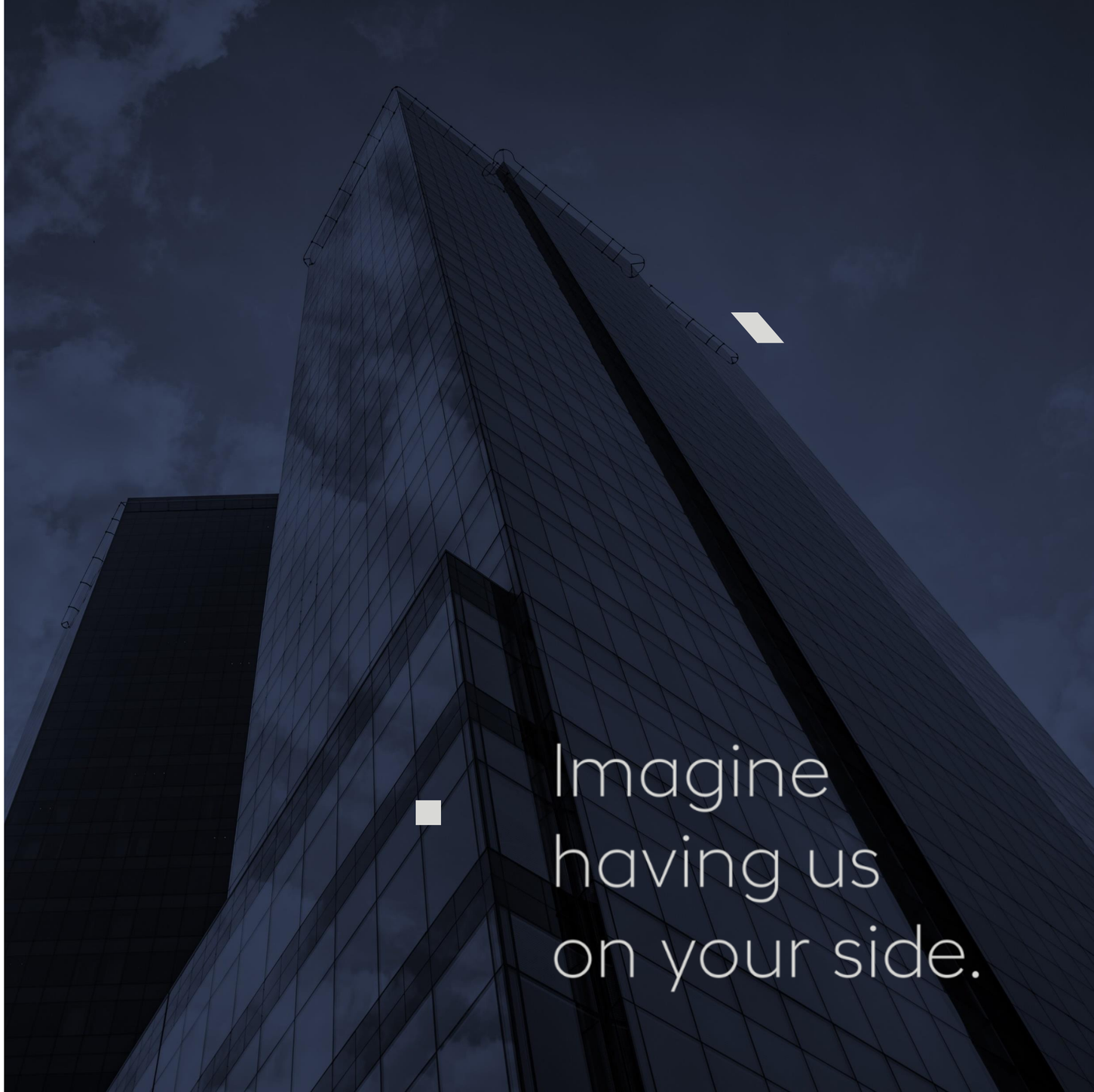
Oceniając - w szczególności do celów oceny skutków dla ochrony danych - skutki operacji przetwarzania wykonywanych przez administratora lub podmiot przetwarzający, **uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania**,.

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) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.).

RYMARZ ▪ ZDORT ◥ MARUTA

Informatyzacja państwa

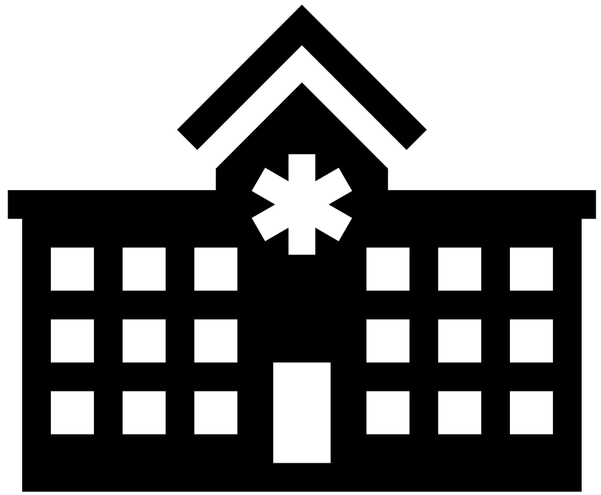
RZMLAW.COM



Obowiązki związane z używaniem systemów teleinformatycznych

Art. 13. [Obowiązki związane z używaniem systemów teleinformatycznych]

1. Podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności.



SPZOZ + spółki wykonujące działalność leczniczą realizujące zadania publiczne

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307).

System zarządzania bezpieczeństwem informacji

§ 19. [System zarządzania bezpieczeństwem informacji]

1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:
   1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
   2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
   3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
   4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
   5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
   6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
      a) zagrożenia bezpieczeństwa informacji,
      b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
      c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
   7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
      a) monitorowanie dostępu do informacji,
      b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
      c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
   8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
   9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

System zarządzania bezpieczeństwem informacji

10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
    a) dbałości o aktualizację oprogramowania,
    b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    e) zapewnieniu bezpieczeństwa plików systemowych,
    f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.

3. **Wymagania 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 27002 - w odniesieniu do ustanawiania zabezpieczeń;
    2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem.

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

Normy ISO

- PN-EN ISO/IEC 27001 promuje holistyczne podejście do bezpieczeństwa informacji przez wskazanie strategicznych obszarów w budowaniu bezpieczeństwa takich jak: ludzie, procesy i technologie.

- Dokument stanowi referencyjny zestaw ogólnych zabezpieczeń informacji wraz z wytycznymi dotyczącymi ich wdrażania. Niniejszy dokument jest opracowany w celu używania przez organizacje:
  a) w kontekście systemu zarządzania bezpieczeństwem informacji (ISMS) na podstawie ISO/IEC 27001;
  b) do wdrażania zabezpieczeń informacji, na podstawie uznanych na całym świecie najlepszych praktyk;
  c) do opracowywania specyficznych dla danej organizacji wytycznych dotyczących zarządzania bezpieczeństwem informacji.

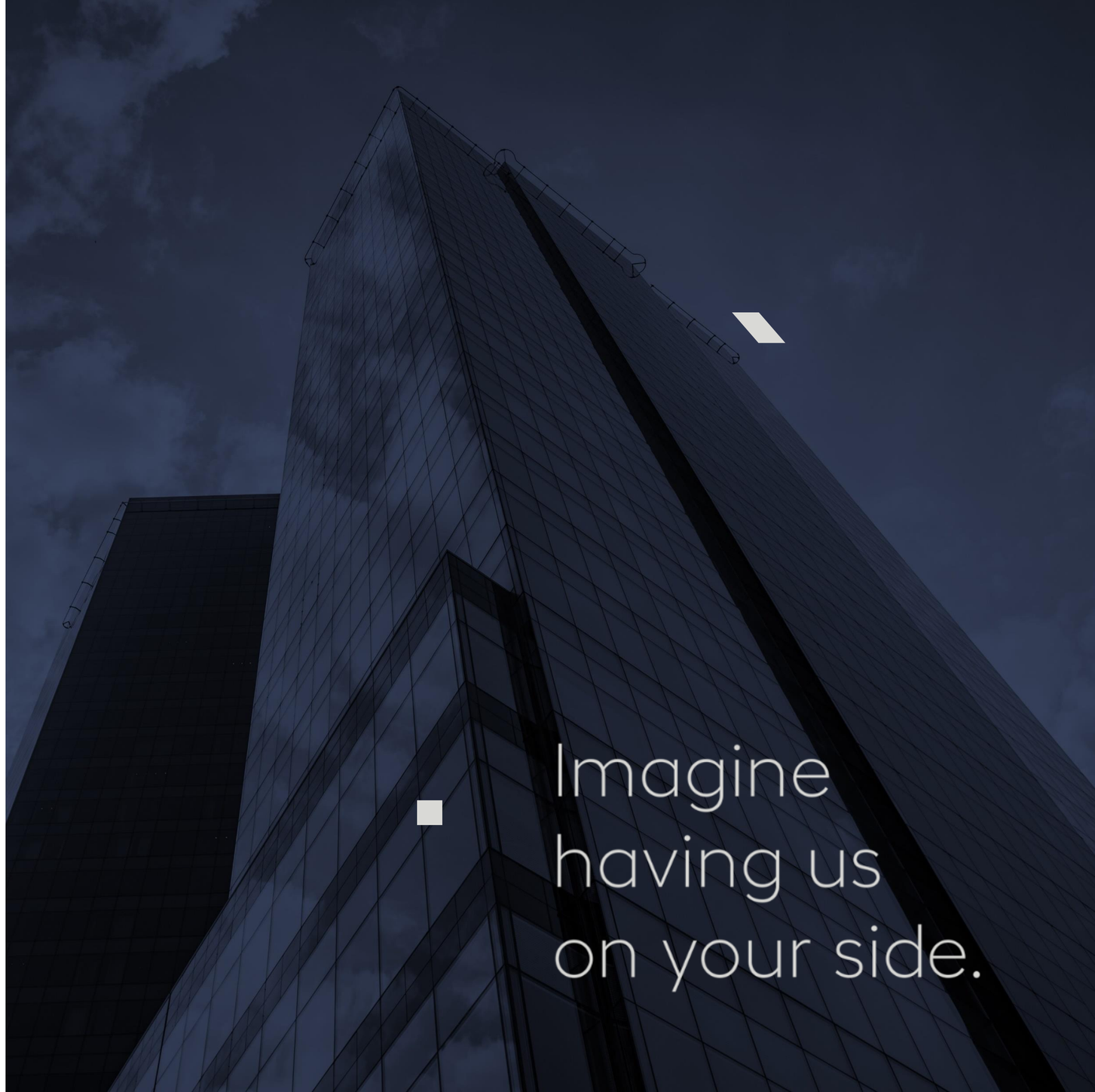
- ISO 27005 (lub ISO/IEC 27005) to międzynarodowa norma zawierająca najlepsze praktyki i wytyczne w zakresie zarządzania ryzykiem bezpieczeństwa informacji. Norma wspiera wymagania dotyczące Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001.

Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 773).

RYMARZ ▪ ZDORT ◥ MARUTA

Krajowy System Cyberbezpieczeńswa

RZMLAW.COM



Kto jest operatorem usług kluczowych?

- **Art. 5. [Uznanie podmiotu za operatora usługi kluczowej]**

1. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, **wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej**. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

2. Organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli:
   1) podmiot świadczy usługę kluczową;
   2) świadczenie tej usługi zależy od systemów informacyjnych;
   3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

Ochrona zdrowia		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2022 r. poz. 633, z późn. zm).
		Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia.
		Narodowy Fundusz Zdrowia.
		Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301).
		Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.
		Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. - Prawo farmaceutyczne.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.).

Obowiązki operatorów usług kluczowych

Art. 8. [Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej]

Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
    a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
    b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
    c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
    d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
    e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;
3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
    a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
    b) dbałość o aktualizację oprogramowania,
    c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
    d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

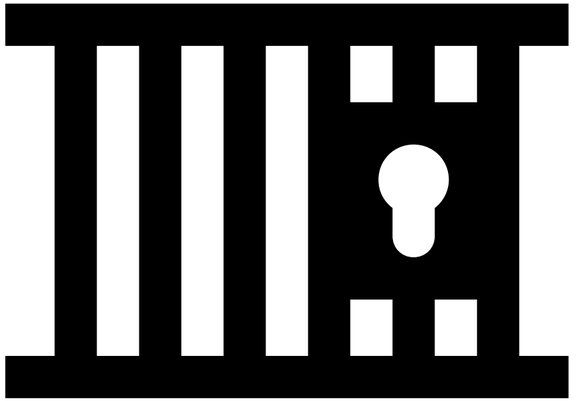
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.).

Co grozi za nieprzestrzeganie przepisów?

- Stwierdzenie przez Rzecznika Praw Pacjenta, że dana praktyka narusza zbiorowe prawa pacjentów i wydanie **decyzji o zaniechaniu jej stosowania lub usunięcia skutków tego naruszenia**. Brak usunięcia naruszeń lub niepodjęcie działań określonych w decyzji = **kara pieniężna do 500 000 zł** (ustawa o Prawach Pacjenta i Rzeczniku Praw Pacjenta).

- Naruszenia przepisów z zakresu ochrony danych osobowych (RODO) – **kary pieniężne** do wysokości do 20 000 000 EUR lub 4% od rocznego światowego obrotu z poprzedniego roku obrotowego. W przypadku podmiotów publicznych limit do 100 tys. zł.

- **Kary pieniężne** do 100 000 zł za zaniechania na gruncie przepisów ustawy o Krajowym systemie cyberbezpieczeństwa (kary dla operatora usługi kluczowej).



+ **Ryzyko odpowiedzialności cywilnej,** szczególnie istotne w przypadku np. wycieku dużych baz danych pacjentów. Potencjalnie odpowiedzialność karna.

Nowelizacja Ustawy o krajowym systemie cyberbezpieczeństwa

- WDROŻENIE DYREKTYWY NIS2 W SEKTORZE OCHRONY ZDROWIA

Kogo dotyczy?

- Dotychczasowe przepisy obejmowały swoim zakresem tylko podmioty, wobec których wydano decyzje o uznaniu ich za tzw. operatorów usług kluczowych (ok. 270 podmiotów).

- Co istotne, nowe przepisy dotyczyć będą nie tylko wybranych organizacji, ale „podmiotów kluczowych” i „podmiotów ważnych”, czyli w kontekście sektora ochrony zdrowia - **podmiotów publicznych** oraz **placówek zatrudniających co najmniej 50 osób** lub mających co najmniej 10 mln EUR rocznego przychodu, czyli m.in. większość szpitali.

- **Nowe przepisy mają wejść w życie w ciągu 1 miesiąca od opublikowania w dzienniku ustaw. Podmioty objęte zakresem przepisów będą miały 6 miesięcy na dostosowanie swojej działalności do nowych wymogów.**

Obowiązki – kluczowe zmiany

Art. 8. [Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej]

Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
   d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
   e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

Art. 8 **Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający**:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających **najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka**, w szczególności:
   a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
   b) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
   e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie,
   f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
   g) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
   h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny,
   i) polityki i procedury stosowania kryptografii, w tym szyfrowania;

UWAGA! Dla każdego sektora Rada Ministrów może określić, w drodze rozporządzenia, szczegółowe wymagania odrębnie dla danego rodzaju działalności

Obowiązki – kluczowe zmiany c.d.

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) dbałość o aktualizację oprogramowania,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

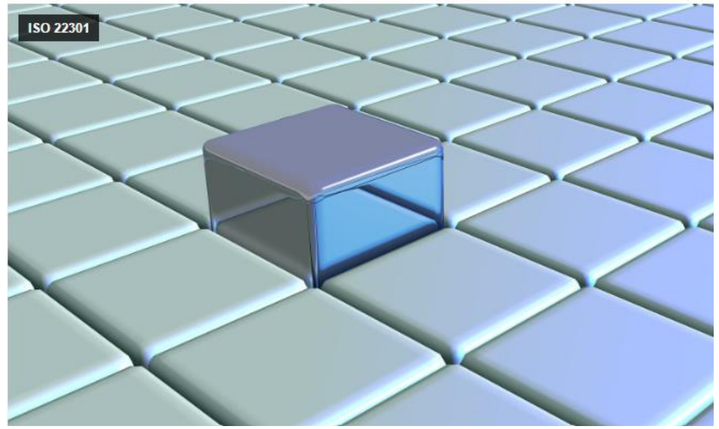
3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń;
6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, **uwzględniających uwierzytelnianie wieloskładnikowe**.

Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarzadzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.

UWAGA! Dla każdego sektora Rada Ministrów może określić, w drodze rozporządzenia, szczegółowe wymagania odrębnie dla danego rodzaju działalności

Normy ISO

- PN-EN ISO/IEC 27001 promuje holistyczne podejście do bezpieczeństwa informacji przez wskazanie strategicznych obszarów w budowaniu bezpieczeństwa takich jak: ludzie, procesy i technologie.



- Norma ISO 22301 zawiera wymagania dotyczące systemu zarządzania ciągłością działania (BCM). Stanowi ona ramy dla identyfikacji kluczowych czynników ryzyka mających wpływ na organizację oraz na utrzymanie jej działań w najtrudniejszych warunkach

Podsumowanie zmian – praktyczny wymiar obowiązków

1. **Samoocena i zgłoszenie do ewidencji:**
   a) Obowiązek oceny, czy podmiot spełnia wymagania ustawy KSC
   b) Obowiązek zgłoszenia, że dany podmiot podlega pod przepisy

2. **Obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji**

a) Zapewnienie zgodności z systemem zarzadzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301 (art. 8 ust. 2)

3. **Obsługa incydentów**
   a) Obowiązek systematycznego szacowania ryzyka wystąpienia incydentu
   b) Obowiązek zarządzania ryzykiem wystąpienia incydentu
   c) Obowiązek zapewnienia dostępu do informacji o incydentach na rzecz właściwego CSIRT
   d) Dokonywanie zgłoszeń nt. incydentów (wczesne ostrzeżenie w terminie 12h/24h, zgłoszenie w ciągu 72h)
   e) Przekazywanie sprawozdań nt. incydentów poważnych
   f) Współdziałanie podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT
   g) Informowanie swoich użytkowników o incydentach

4. **Wdrożenie zabezpieczeń:**
   a) Zapewnienie bezpieczeństwa IT (wdrożenie środków zabezpieczenia)
   b) Zapewnienie bezpieczeństwa fizycznego i środowiskowego
   c) Wdrożenie wewnętrznych polityk i procedur
   d) Opracowanie planów ciągłości działania i planów awaryjnych, polityka poufności informacji, monitorowanie systemów IT w trybie ciągłym, polityka oceny skuteczności zabezpieczeń, edukacja z zakresu cyberbezpieczeństwa i cyberhigieny
5. **Prowadzenie dokumentacji**
   a) Opracowanie, stosowanie i aktualizowanie dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego oraz przechowywanie jej przez co najmniej 2 lata po wycofaniu jej przedmiotu (systemu, usługi); dokumentowanie protokołem jej niszczenia
   b) Ustanowienie nadzoru nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi
6. **Zarządzanie łańcuchem dostaw**

a) Konieczność uwzględnienia podatności związanych z dostawcą sprzętu lub oprogramowania, ogólnej jakości produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania oraz wyników skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 dyrektywy NIS2
b) Konieczność wycofania na własny koszt z użytkowania zakupionych produktów, usług i procesów ICT dostarczanych przez podmiot, który został uznany za dostawcę wysokiego ryzyka

Podsumowanie zmian – praktyczny wymiar obowiązków

7. **Działania edukacyjne i szkoleniowe**
   a) Przeprowadzanie szkoleń dla kierownika podmiotu kluczowego (min. raz w roku) z zakresu wykonywania obowiązków wynikających z przepisów ustawy
   b) Zapewnienie użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej

8. **Odpowiedzialność osób kierujących organizacją**
   a) Wyznaczenie kierownika, który odpowiada za zgodność, i który nie może być skazany prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji
   b) Wyznaczenie dwóch osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi i podmiotami ważnymi
   c) Odpowiedzialność kierownika podmiotu kluczowego lub ważnego – a gdy jest to organ wieloosobowy (np. zarząd) i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu

9. **Audyty zgodności**
   a) Przeprowadzenie audytu wstępnego
   b) Przeprowadzenie nie rzadziej niż co 2 lata na własny koszt audytu bezpieczeństwa systemu informacyjnego oraz przedstawienie w postaci elektronicznej sprawozdania z przeprowadzonego audytu właściwemu organowi w terminie 3 dni roboczych od dnia jego otrzymania
   c) Przeprowadzanie audytu i przekazywanie wniosków z audytu na każde żądanie organu ds. cyberbezpieczeństwa

10. **Zbieranie informacji o cyberzagrożeniach i cyberincydentach**
    a) Stosowanie środków zapobiegających incydentom i ograniczających ich wpływ na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi
    b) Stosowanie bezpiecznych środków komunikacji elektronicznej
    c) Wdrożenie i korzystanie z systemu s46

Sankcje finansowe

- Wysokość kary pieniężnej **nie może przekroczyć 10 000 000 euro** lub **2% przychodów** osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł.”,

- Wysokość kary pieniężnej nie może przekroczyć **7 000 000 euro lub 1,4%** przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż **15 000 zł**.

- Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:

1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi;
2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług

– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do **100 000 000 zł.**

Karze pieniężnej może podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, niezależnie od kary nałożonej na podmiot.

Kara pieniężna może być wymierzona w kwocie **nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia.**

Kara pieniężna może zostać nałożona nawet jeżeli naruszenie obowiązków miało charakter jednorazowy.

Projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa

- Certyfikacja produktów ICT, usług ICT i procesów ICT będzie odbywać się dobrowolnie, na podstawie umowy zawartej między dostawcą, a jednostką oceniającą zgodność.

- Krajowe programy certyfikacji cyberbezpieczeństwa będą tworzone w drodze rozporządzeń ministra. Celem krajowych programów certyfikacji cyberbezpieczeństwa będzie zapewnienie, by produkty ICT, usługi ICT lub procesy ICT, certyfikowane zgodnie z takimi programami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług.

- Obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji.

- Projektowana ustawa wejdzie w życie po upływie miesiąca od dnia jej ogłoszenia.

Zestaw rekomendacji w zakresie cyberbezpieczeństwa w ochronie zdrowia

- **Rekomendacje Centrum E-Zdrowia**

Centrum e-Zdrowia

19.06.2024

Cyberbezpieczeństwo w ochronie zdrowia – nowe szkolenia Akademii CeZ

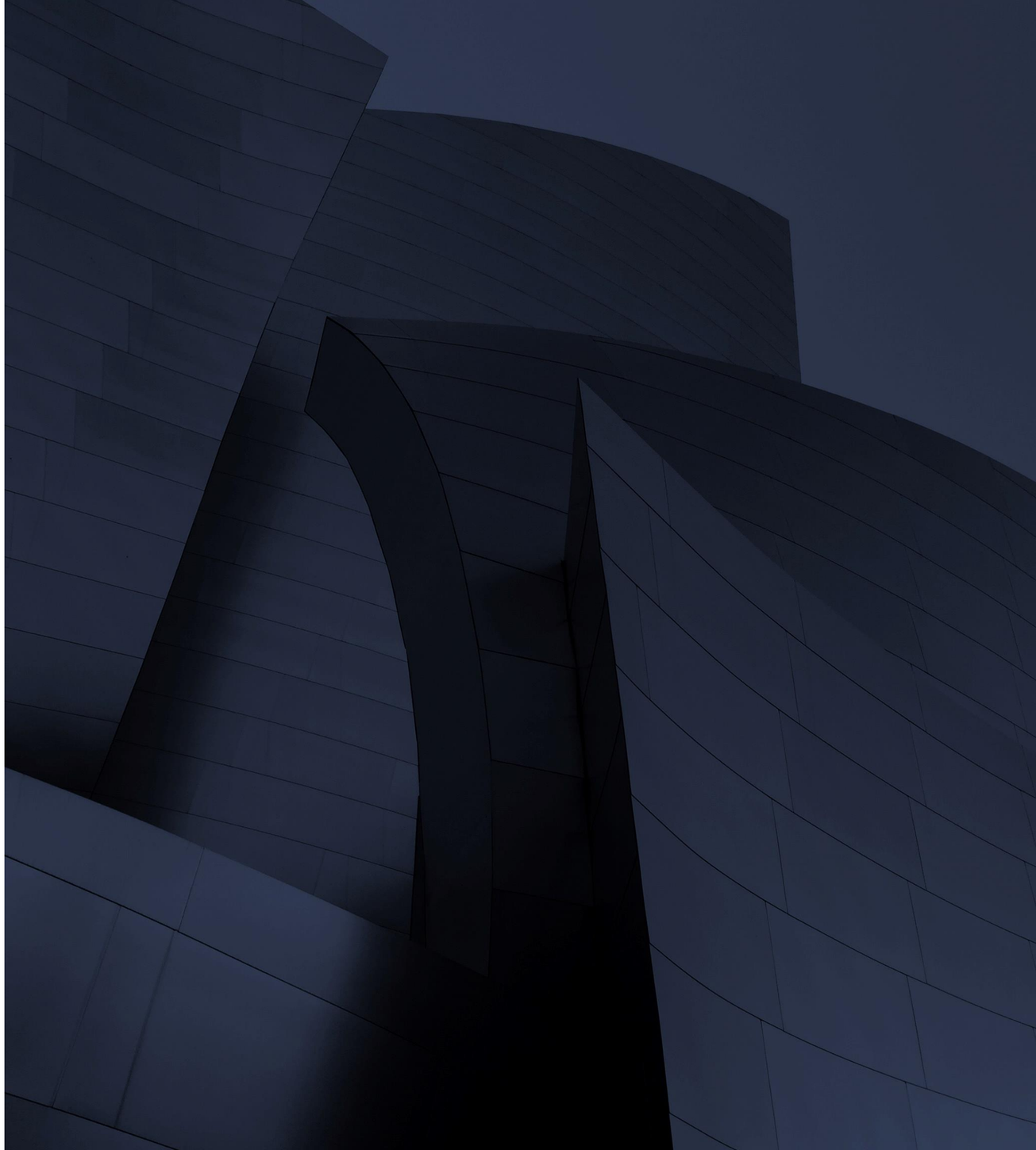
Zakres rekomendacji Centrum e-Zdrowia

Jak sfinansować cyberbezpieczeństwo w ochronie zdrowia?

Finansowanie

408 mln zł będzie miał do dyspozycji Narodowy Fundusz Zdrowia na zwiększanie odporności placówek medycznych wobec ataków hakerskich. Dostawcy usług IT pozytywnie oceniają tę informację. Jednocześnie z niecierpliwością czekają na doniesienia o pieniądzach z Krajowego Planu Odbudowy.

- Ministerstwo Zdrowia zapowiedziało pierwsze duże konkursy na dofinansowanie reform i inwestycji w polskiej ochronie zdrowia ze środków Krajowego Planu Odbudowy (KPO).



https://www.portalsamorzadowy.pl/ochrona-zdrowia/ruszaja-konkursy-na-duze-pieniadze-z-kpo-dla-zdrowia-wiemy-kto-najbardziej-skorzysta,548429.html

https://www.rynekzdrowia.pl/E-zdrowie/To-moze-byc-dobry-rok-dla-e-zdrowia-W-grze-miliardy-zlotych-na-cyfryzacje-i-cyberbezpieczenstwo,253658,7.html

Na co zwracać uwagę przy wyborze dostawcy?

Rekomendacje Centrum e-Zdrowia

Zarządzanie bezpieczeństwem i ciągłością działania łańcucha usług	– Polityka bezpieczeństwa w relacjach z dostawcami – Standardy i wymagania nakładane na dostawców w umowach w zakresie cyberbezpieczeństwa – Dostęp zdalny – Metody uwierzytelnienia

- Zakres oferowanego bezpieczeństwa;
- Możliwości innowacji i potencjał doskonalenia;
- Kompetencje dostawcy i jego pracowników;
- Certyfikacja oraz wykorzystywane technologie;
- Doświadczenie i renoma;
- Zasady zarządzania kryzysowego;
- Zakres spełniania norm ISO;
- Wywiązywanie się z obowiązków prawnych, w tym RODO.

RYMARZ · ZDORT ⟍ MARUTA

Thank you

RZMLAW.COM

RYMARZ · ZDORT · MARUTA

Michał Czarnuch
PARTNER, PRAKTYKA LIFE SCIENCES

michal.czarnuch@rzmlaw.com
+48 887 092 062

FOR FURTHER INFORMATION DO NOT HESITATE TO CONTACT US.