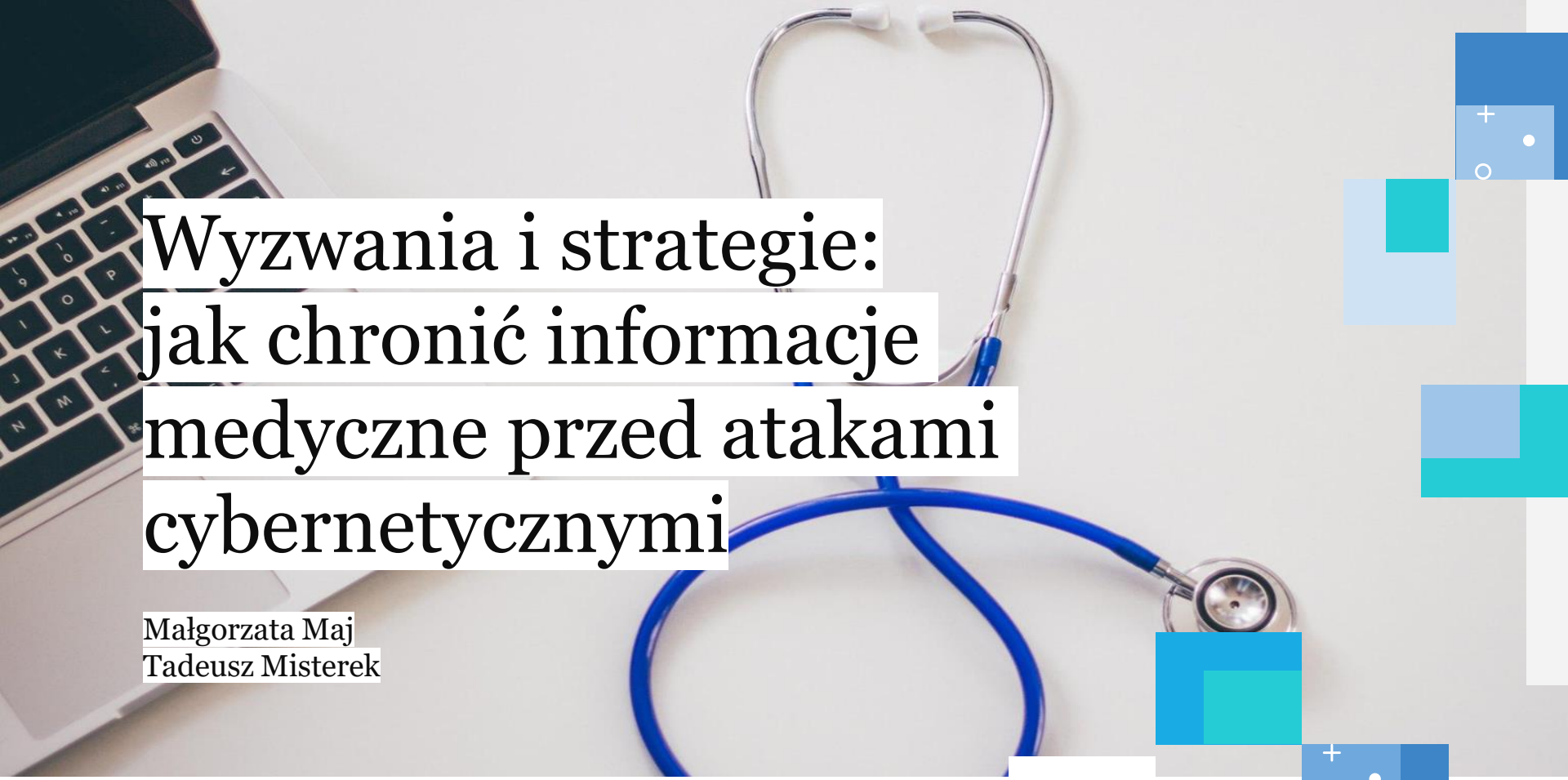


Wyzwania i strategie: jak chronić informacje medyczne przed atakami cybernetycznymi

Małgorzata Maj
Tadeusz Misterek

Fundusz Sprawiedliwości
fundacja instytut CYBERBEZPIECZEŃSTWA

Czym jest cyberbezpieczeństwo w ochronie zdrowia, dlaczego jest tak ważne i jakie obszary są kluczowe? (uwarunkowania prawne i praktyka)

Bezpieczeństwo cybernetyczne to nie tylko ochrona danych i systemów, ale także cały proces zapobiegania i reagowania na cyberataki. Wymaga to zarówno odpowiedniej technologii, jak i skutecznych strategii kontrolowania i zabezpieczania sieci, programów oraz urządzeń.

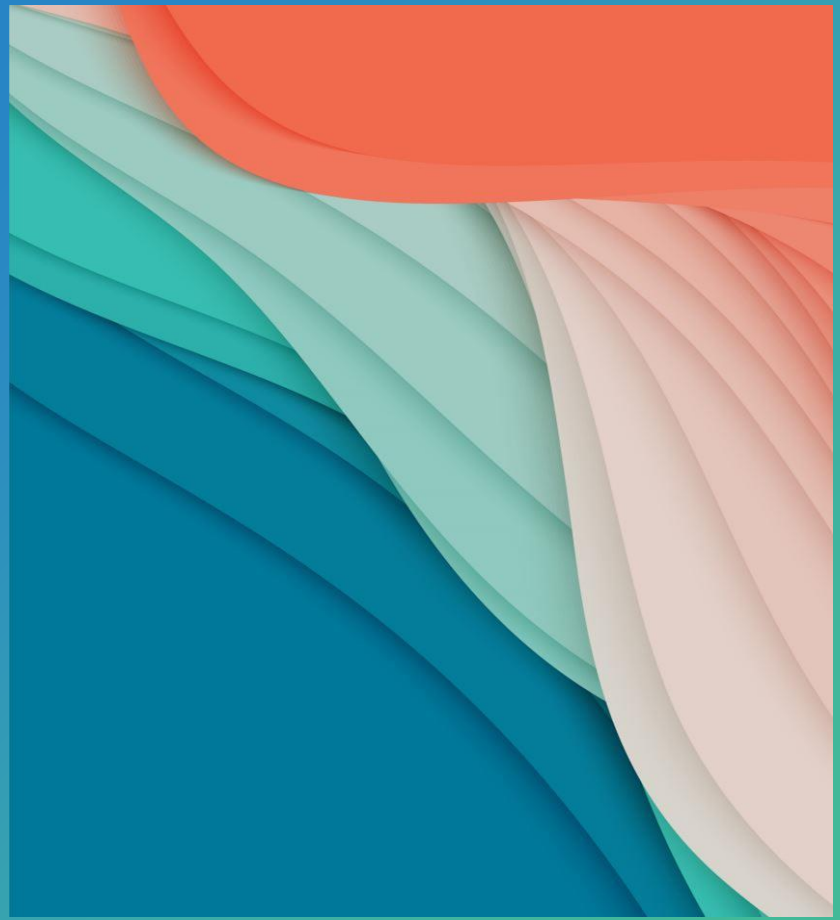
Najważniejszym celem zapewnienia bezpieczeństwa w sieci jest minimalizacja ryzyka ataków oraz zapewnienie efektywnej ochrony przed wykorzystaniem danych i programów przez osoby nieuprawnione.

Czym jest cyberbezpieczeństwo w ochronie zdrowia, dlaczego jest tak ważne i jakie obszary są kluczowe? (uwarunkowania prawne i praktyka)

Jednostki ochrony zdrowia są atrakcyjnym celem dla cyberprzestępców.

- Gromadzą cenne dane osobowe, medyczne i finansowe.
- Stosowane są na co dzień różne technologie i rozwiązania cyfrowe.
- Sektor zdrowia jest bardzo dochodowym celem dla cyberprzestępców.
- Cyberataki mogą mieć charakter podważenia zaufania publicznego.
- Przez ograniczone budżety na rozwiązania IT znalezienie luk bezpieczeństwa jest łatwiejsze w porównaniu do innych branż.

W raporcie opracowanym przez ECRI dotyczącym 10 największych zagrożeń związanych z technologią medyczną w roku 2022, pierwsze miejsce zajęły cyberataki mogące zakłócić realizację świadczeń opieki zdrowotnej i zagrozić bezpieczeństwu pacjenta.



Czym jest cyberbezpieczeństwo w ochronie zdrowia, dlaczego jest tak ważne i jakie obszary są kluczowe?
(uwarunkowania prawne i praktyka)

Kluczowe dla kwestii cyberbezpieczeństwa było wprowadzenie w 2018 roku ustawy o krajowym systemie cyberbezpieczeństwa (KSC) nawiązującej do tzw. Dyrektywy UE NIS.

Wprowadzenie KSC ma na celu zapewnienie odpowiedniego poziomu cyberbezpieczeństwa w kraju, w szczególności u operatorów usług kluczowych, do których zalicza się m.in. sektor zdrowotny.

Wprowadzona ustawa narzuca obowiązek wdrożenia właściwych zabezpieczeń, kontrolowania incydentów i szacowania ryzyka, co pozwala zachować ciągłość działania poszczególnych sektorów.

Czym jest cyberbezpieczeństwo w ochronie zdrowia, dlaczego jest tak ważne i jakie obszary są kluczowe? (uwarunkowania prawne i praktyka)

- 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.).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2023 r. poz. 913 z późn. zm.).
- Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz. U. z 2017 r. poz. 2247).
- 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.).

KSO za cyberbezpieczeństwo uznała odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych w nich danych lub związanych z nimi usług.

Problemy z bezpieczeństwem cyfrowym w branży healthcare - jakie są kluczowe zagrożenia? Innowacje medyczne, AI i medtech a obecne uwarunkowania sektora. (krótkie case study przypadków naruszeń w Polsce)

Cyberatak:

- rejestracja pacjentów
- obsługa pacjentów
- prowadzenie i wykorzystanie EDM
- ujawnienie danych pacjentów
- realizowanie zaplanowanych świadczeń zdrowotnych
- działanie systemów administracyjnych.

Problemy z bezpieczeństwem cyfrowym w branży healthcare - jakie są kluczowe zagrożenia? Innowacje medyczne, AI i medtech a obecne uwarunkowania sektora. (krótkie case study przypadków naruszeń w Polsce)

Oprócz konsekwencji finansowych z tytułu niewypełnienia obowiązków z zakresu cyberbezpieczeństwa, **skutki cyberataku mogą być naprawdę daleko idące.**

Możliwe skutki:

- roszczenia pacjenta z tytułu naruszenia jego praw,
- roszczenia pacjenta z tytułu poniesionej szkody na skutek nieudzielenia świadczenia zdrowotnego w terminie,
- skargi pacjentów do Rzecznika Praw Pacjenta,
- naruszenie zbiorowych praw pacjentów,
- kary finansowe NFZ z tytułu nieprawidłowej realizacji umowy o udzielanie świadczeń zdrowotnych,
- odpowiedzialność karna, zawodowa oraz cywilna szpitala i personelu medycznego,
- sankcje za naruszenie RODO.

Problemy z bezpieczeństwem cyfrowym w branży healthcare - jakie są kluczowe zagrożenia? Innowacje medyczne, AI i medtech a obecne uwarunkowania sektora. (krótkie case study przypadków naruszeń w Polsce)

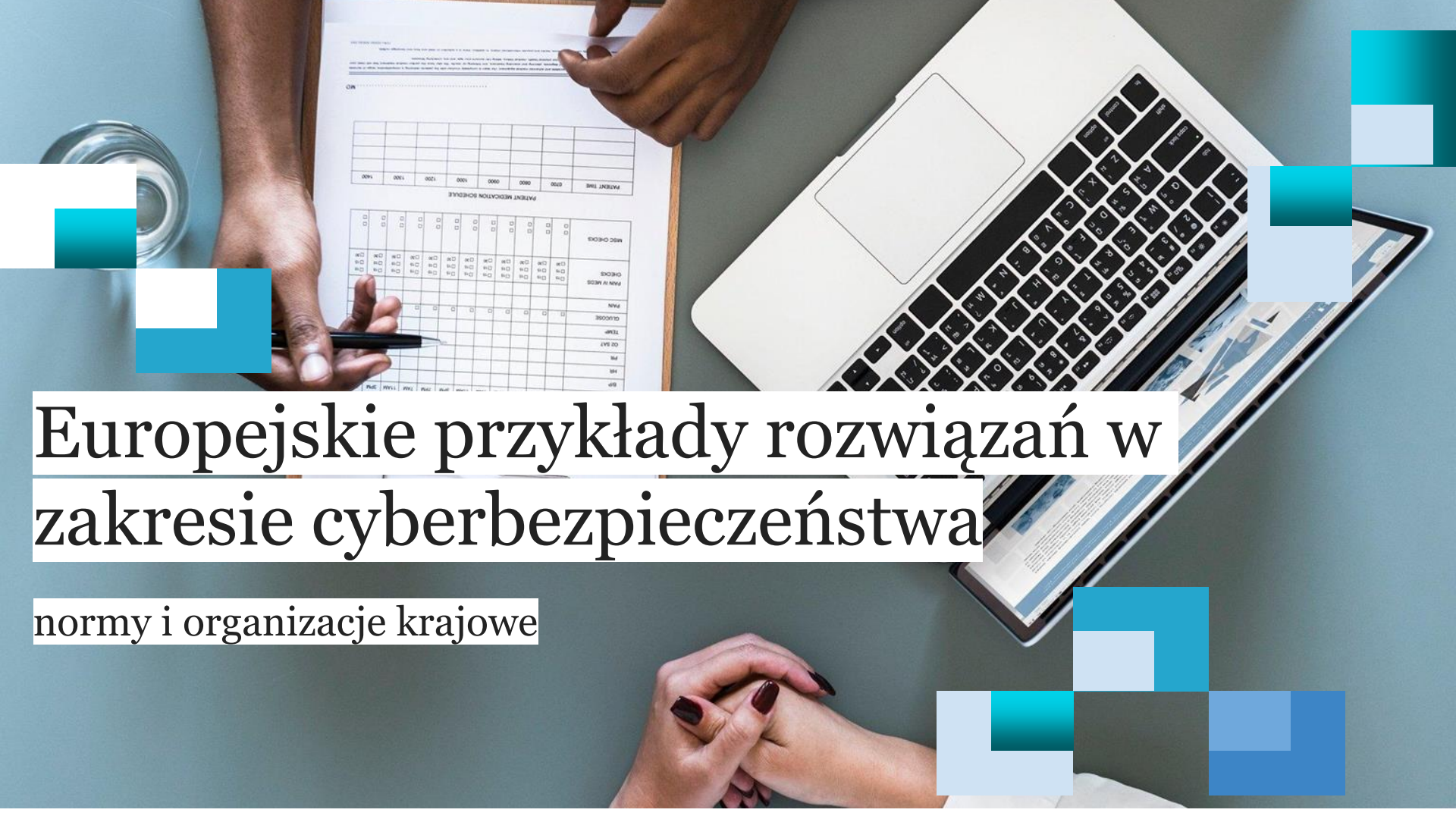
- Wyciek danych z ALAB Laboratoria w wyniku ataku hackerów (ransomware);
- Atak ransomware na Centrum Zdrowia Matki Polki i próba podobnego ataku na Centralny Szpital Kliniczny w Łodzi;
- Atak hackerski na klinikę "Budzik„ przy Centrum Zdrowia Dziecka (uniemożliwienie sporządzenie raportu dla NFZ do rozliczenia);
- Atak na szpital Pirogowa w Łodzi (straty finansowe na prawie pół miliona złotych);
- Lotnicze Pogotowie Ratunkowe – próba zaburzenia pracy Śmigłowcowej Służby Ratownictwa Medycznego oraz lotniczego transportu sanitarnego.

Problemy z bezpieczeństwem cyfrowym w branży healthcare - jakie są kluczowe zagrożenia? Innowacje medyczne, AI i medtech a obecne uwarunkowania sektora. (krótkie case study przypadków naruszeń w Polsce)

Wg. analizy Fortinet, najczęściej ataki na szpitale są realizowane za pomocą metod socjotechnicznych: phishingu (54%), ataków typu DDoS (15%) oraz z użyciem oprogramowania szpiegującego (8%). W 31% prób ataków doszło do włamań na konta personelu.

Zgodnie z wynikami badania Veeam w ochronie zdrowia wciąż widoczna jest tzw. luka dostępności i ochrony danych. Aż 77% placówek dostrzega tzw. protection gap, czyli lukę między tym, ile danych mogą stracić bez negatywnych skutków dla działalności, a tym jak często tworzone są kopie zapasowe informacji. W 2023 r. spodziewano się zwiększania budżetów na ochronę danych o prawie 8%.

Na świecie opieka zdrowotna jest uznawana za najczęściej atakowany sektor z blisko 1800 atakami tygodniowo, a w roku 2022 ta branża zanotowała wzrost liczby ataków o 74 % w stosunku do poprzednich lat.



Europejskie przykłady rozwiązań w zakresie cyberbezpieczeństwa

normy i organizacje krajowe

Normy i organizacje międzynarodowe

1. Międzynarodowe Standardy Bezpieczeństwa Informacji w Ochronie Zdrowia (ISO/IEC 27001 i ISO/IEC 27002):

Organizacje w sektorze ochrony zdrowia mogą wdrożyć te standardy, aby zapewnić skuteczną ochronę danych pacjentów i systemów informatycznych.

2. Europejska Dyrektywa o Ochronie Danych Osobowych (RODO):

RODO nakłada surowe wymagania dotyczące ochrony danych osobowych, w tym danych medycznych, co wymaga od organizacji zdrowotnych stosowania odpowiednich środków bezpieczeństwa.

3. ENISA:

Agencja Unii Europejskiej odpowiedzialna za zapewnienie wysokiego i efektywnego poziomu bezpieczeństwa w sieciach i systemach informatycznych w Unii Europejskiej.

Normy i organizacje międzynarodowe

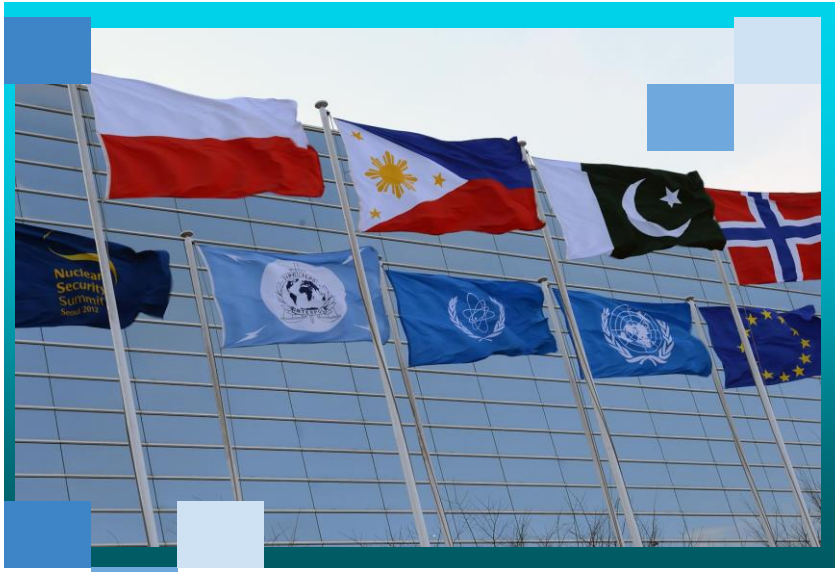
4. Rozporządzenie o Bezpieczeństwie Sieci i Systemów Informacyjnych (NIS 2) z 2022 r.:

Wprowadzone przez Unię Europejską, to prawodawstwo nakłada obowiązki na dostawców usług zdrowotnych w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa sieci i systemów informatycznych.

5. Międzynarodowa Agencja Energii Atomowej (IAEA) - Program Bezpieczeństwa Jądrowego w Ochronie Zdrowia (NUSEC):

IAEA współpracuje z państwami członkowskimi w zakresie zapewnienia bezpieczeństwa informacji medycznej i ochrony przed cyberzagrożeniami w sektorze opieki zdrowotnej.

6. Inne ustawy na poziomach krajowych regulujące branżę medyczną



Europejskie podmioty zajmujące się krajowymi systemami cyberbezpieczeństwa

1. National Health Service (NHS) Digital Security Centre (Wielka Brytania):

NHS Digital Security Centre jest odpowiedzialny za zarządzanie ryzykiem cybernetycznym i zapewnienie bezpieczeństwa informacji w brytyjskim systemie ochrony zdrowia. Centrum prowadzi działania mające na celu identyfikację zagrożeń, wdrażanie środków bezpieczeństwa, szkolenia personelu oraz reagowanie na incydenty związane z bezpieczeństwem informacji medycznej.

2. Centre for Cyber Security in Healthcare (Holandia):

Holenderskie centrum bezpieczeństwa cybernetycznego w sektorze ochrony zdrowia monitoruje i reaguje na zagrożenia cybernetyczne oraz dostarcza wskazówek dotyczących bezpieczeństwa dla placówek medycznych. Centrum działa jako centralny punkt kontaktowy w przypadku incydentów związanych z bezpieczeństwem informacji medycznej oraz wspiera organizacje w wdrażaniu skutecznych środków obronnych.

Europejskie podmioty zajmujące się krajowymi systemami cyberbezpieczeństwa

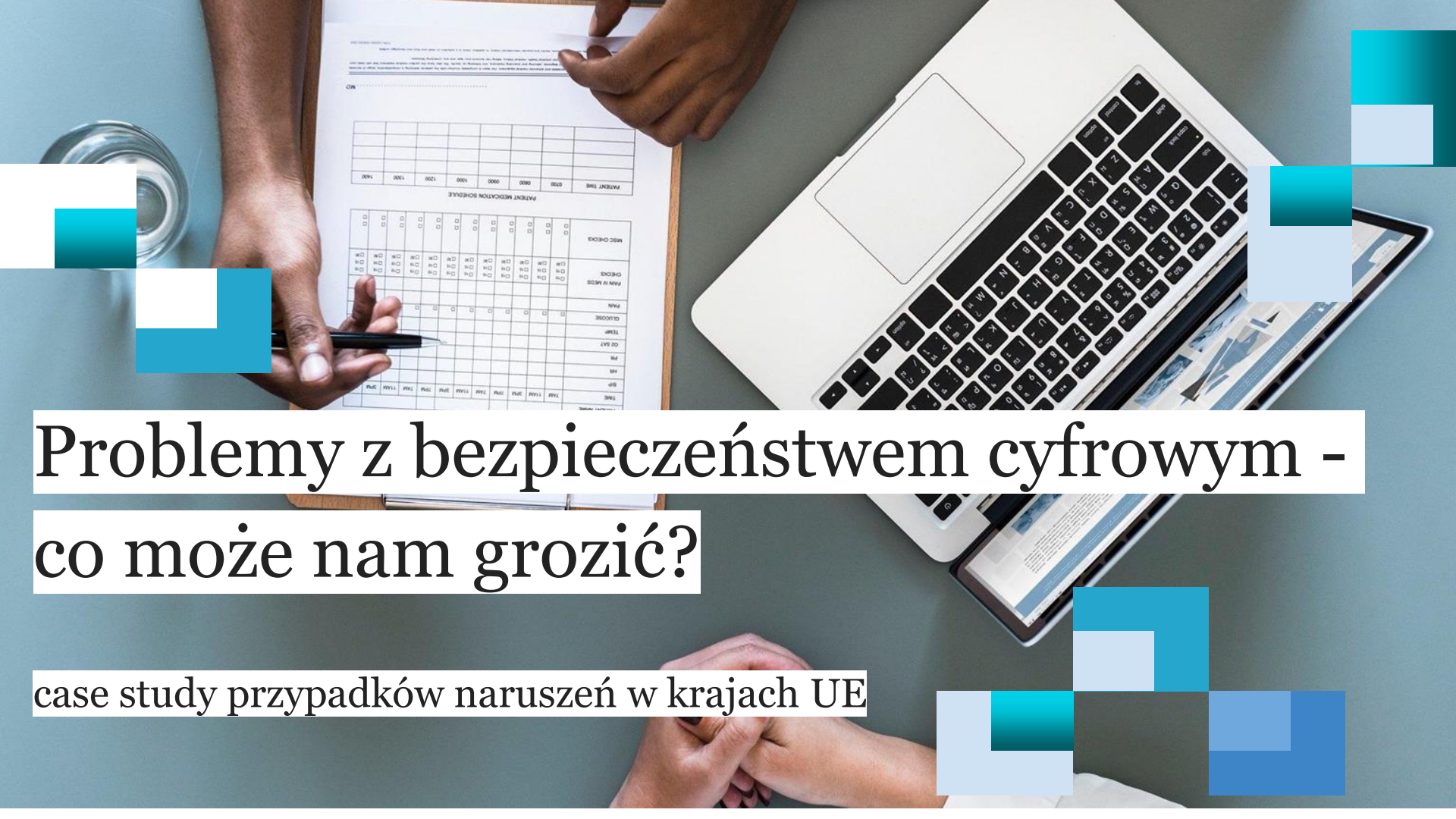
3. Agence eSanté (Luksemburg):

Luksemburska agencja eSanté zajmuje się zarządzaniem infrastrukturą e-zdrowia i zapewnianiem bezpieczeństwa systemów informatycznych w sektorze ochrony zdrowia. Agencja eSanté opracowuje i wdraża środki bezpieczeństwa informatycznego, monitoruje zagrożenia oraz prowadzi działania mające na celu zapobieganie incydentom związanym z bezpieczeństwem informacji medycznej.

4. Agencia de Calidad del Sistema Nacional de Salud (Hiszpania):

Hiszpańska agencja ds. jakości systemu opieki zdrowotnej opracowuje i wdraża środki bezpieczeństwa informatycznego, aby zapewnić bezpieczeństwo danych pacjentów i systemów medycznych. Agencia de Calidad del Sistema Nacional de Salud działa jako organ regulacyjny, który nadzoruje i wspiera organizacje w sektorze ochrony zdrowia w zapewnianiu zgodności z wymogami bezpieczeństwa cyfrowego.

W Polsce odpowiednikiem jest CSIRT, czyli Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, pełni rolę Zespołu CSIRT poziomu krajowego odpowiadającego za koordynację procesu reagowania na incydenty komputerowe



Problemy z bezpieczeństwem cyfrowym - co może nam grozić?

case study przypadków naruszeń w krajach UE

Case study przypadków naruszeń w krajach UE

1. Wielka Brytania (2017):

W 2017 roku NHS England doświadczyło poważnego wycieku danych, w wyniku którego zaginęło około 500 000 rekordów medycznych pacjentów. Wyciek był wynikiem błędu ludzkiego, a dane zostały przypadkowo usunięte z głównej bazy danych.

2. Dania (2018):

W 2018 roku duńska agencja zdrowia (Region Hovedstaden) doświadczyła wycieku danych dotyczących ponad miliona pacjentów. Wyciek ten był spowodowany błędem w konfiguracji systemu informatycznego, który umożliwił nieuprawniony dostęp do danych medycznych.

Case study przypadków naruszeń w krajach UE

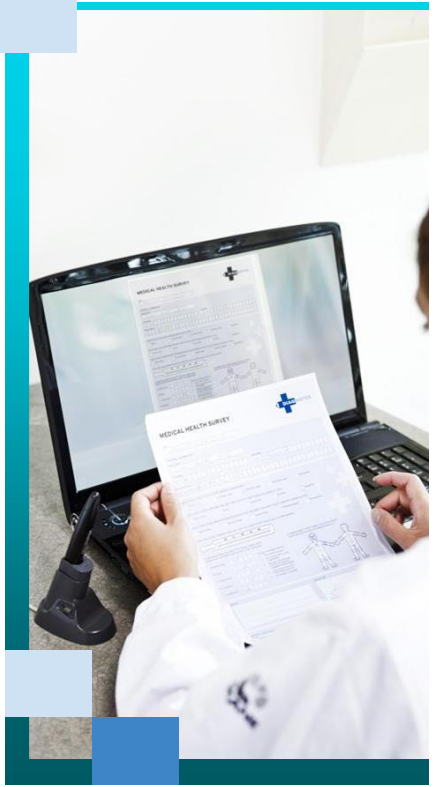
3. Szwecja (2020):

W 2020 roku Szwedzki Urząd ds. Danych Osobowych wszczął śledztwo w sprawie wycieku danych medycznych, który dotknął ponad 2,7 miliona pacjentów. Wyciek ten nastąpił w wyniku naruszenia zabezpieczeń wewnętrznych systemu IT przez jednego z podwykonawców.

4. Niemcy (2021):

W 2021 roku niemiecki operator sieciowy, który obsługuje ponad 13 000 placówek opieki zdrowotnej, doświadczył wycieku danych, w wyniku którego dane medyczne około 13 milionów pacjentów znalazły się w Internecie. Wyciek ten był wynikiem błędu w oprogramowaniu w systemie zarządzania danymi.

Te przykłady pokazują, jak wrażliwe dane medyczne mogą być narażone na wycieki z powodu błędów ludzkich, słabych zabezpieczeń IT i ataków cybernetycznych.



Trendy i dobre praktyki z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia - z punktu widzenia podmiotów leczniczych, zawodów medycznych i pacjentów.

Plan działania
w zakresie cyberbezpieczeństwa
w ochronie zdrowia

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

Ministerstwo
Cyfryzacji

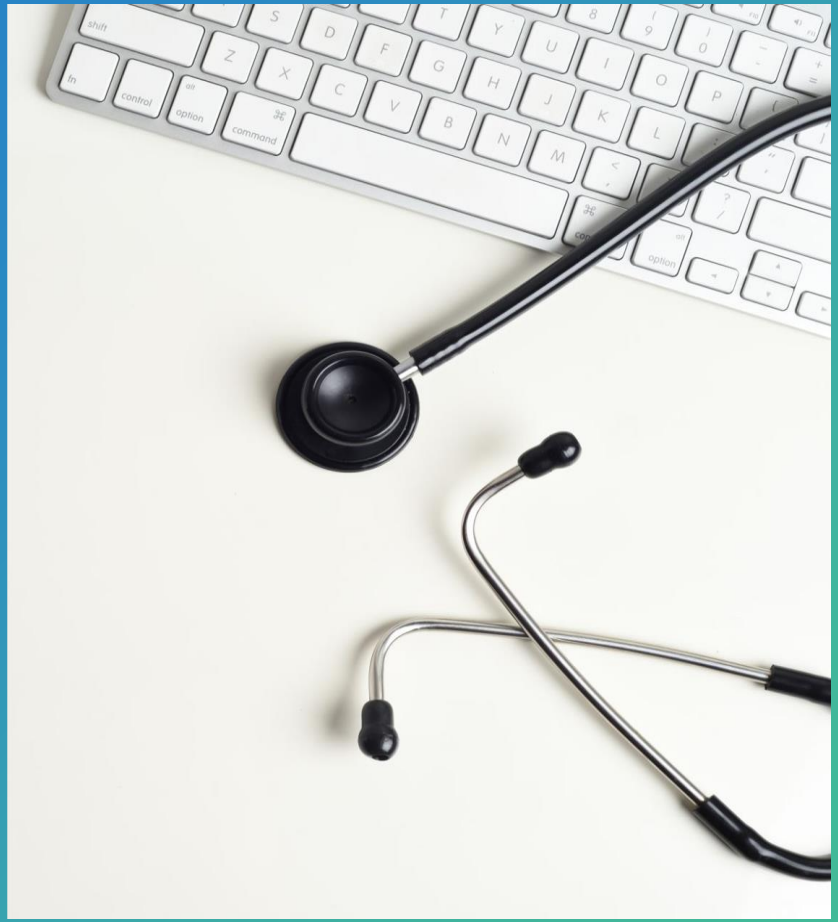
Rekomendacje cyberbezpieczeństwa

dla podmiotów sektora ochrony zdrowia

(Kwiecień 2020 r.)

Krajowy Plan
Odbudowy i Zwiększania
Odporności

fundacja instytut
CYBERBEZPIECZEŃSTWA



Trendy i dobre praktyki z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia - z punktu widzenia podmiotów leczniczych, zawodów medycznych i pacjentów.

Najlepsze praktyki w zakresie cyberbezpieczeństwa dla ochrony zdrowia – szpital:

- Wdrożenie systemu zarządzania bezpieczeństwem;
- Wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo;
- Zabezpieczenie bezpieczeństwa dokumentacji;
- Wdrożenie wewnętrznych regulacji;
- Powołanie wewnętrznej struktury cyberbezpieczeństwa;
- Regularne przeprowadzanie audytów.

Trendy i dobre praktyki z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia - z punktu widzenia podmiotów leczniczych, zawodów medycznych i pacjentów.

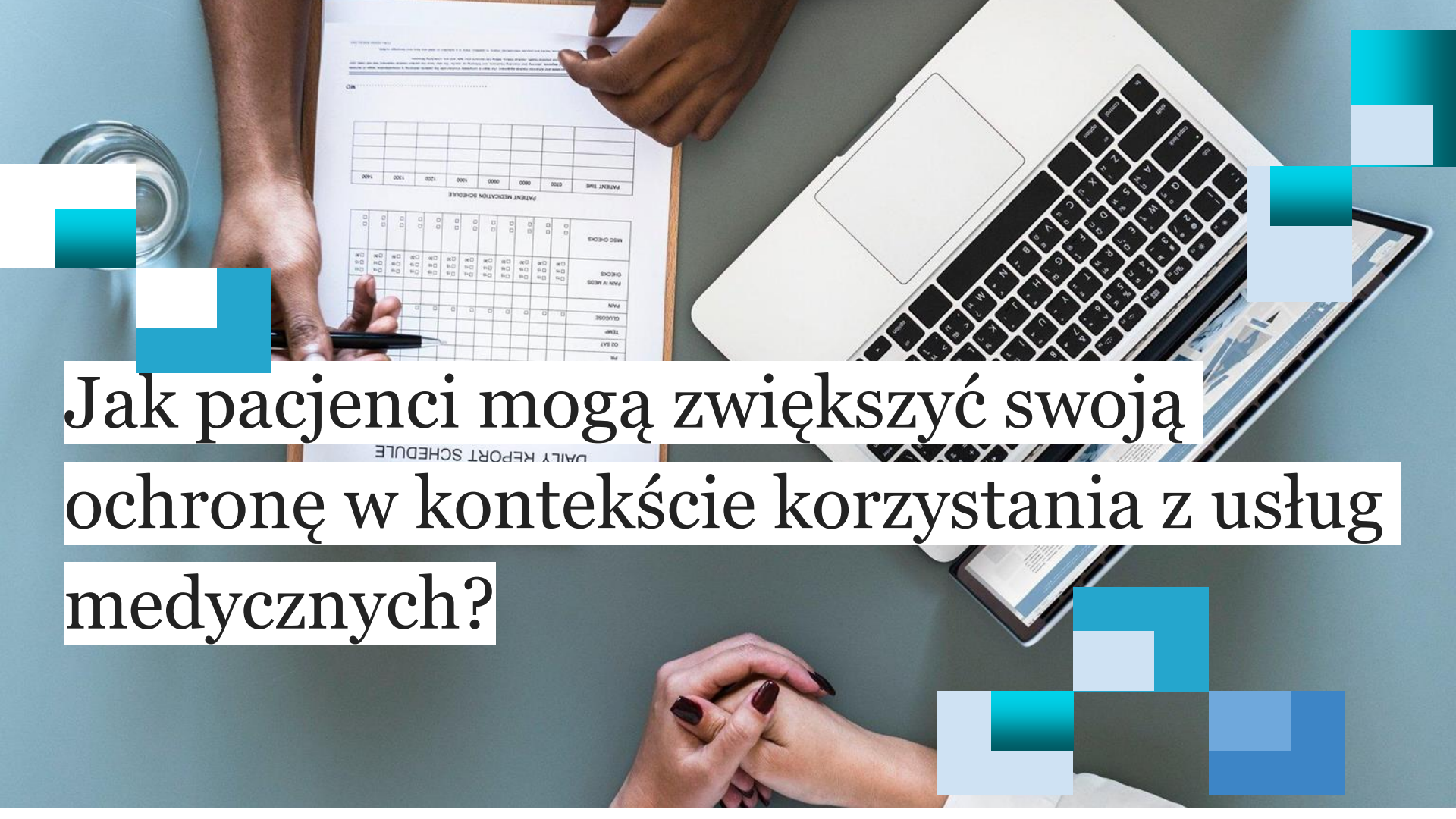
Top 4 praktyki w zakresie cyberbezpieczeństwa dla ochrony zdrowia – pracownicy:

1. Tworzenie kopii zapasowych;
2. Zabezpieczenie poczty elektronicznej i systemów wewnętrznych używanych np. do EDM;
3. Zabezpieczenie sprzętu;
4. Regularne aktualizowanie umiejętności i wiedzy.

Trendy i dobre praktyki z zakresu cyberbezpieczeństwa w sektorze ochrony zdrowia - z punktu widzenia podmiotów leczniczych, zawodów medycznych i pacjentów.

Rekomendacje – pacjenci:

- Ustawianie trudnych haseł i uwierzytelniania dwuetapowego;
- Założenie konta w systemie informacji kredytowej i gospodarczej w celu monitorowania swojej aktywności kredytowej;
- Zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- W razie naruszenia danych – zgłaszanie właściwym organom;
- Zastrzeżenie numeru PESEL.



Jak pacjenci mogą zwiększyć swoją ochronę w kontekście korzystania z usług medycznych?

Jak pacjenci mogą zwiększyć swoją ochronę w kontekście korzystania z usług medycznych?

1. Stosowanie silnych haseł:

Ważne jest, aby stosować unikalne i silne hasła do swoich kont medycznych online, unikając łatwych do odgadnięcia kombinacji

2. Uważne korzystanie z komunikacji elektronicznej:

Unikaj wysyłania wrażliwych informacji medycznych za pośrednictwem nieszyfrowanych e-maili lub wiadomości tekstowych, a także ograniczaj udostępnianie takich informacji za pośrednictwem komunikatorów społecznościowych.

3. Zachowanie ostrożności wobec próśb o dane osobowe:

Nie udostępniaj wrażliwych informacji medycznych osobom lub instytucjom, które nie mają odpowiednich uprawnień lub nie są potwierdzone jako wiarygodne.Ponadto, uważaj na linki przesyłane za pośrednictwem SMS lub e-maili.

4. Regularne sprawdzanie swoich danych medycznych:

Regularnie sprawdzaj swoje dane medyczne, aby wykryć ewentualne nieprawidłowości lub nieuprawnione dostępy do Twoich informacji.

Jak pacjenci mogą zwiększyć swoją ochronę w kontekście korzystania z usług medycznych?

5. Korzystanie z bezpiecznych sieci Wi-Fi:

Podczas korzystania z aplikacji lub stron internetowych związanych z opieką zdrowotną, upewnij się, że jesteś połączony z bezpieczną siecią Wi-Fi, aby uniknąć przechwytywania danych przez osoby trzecie.

6. Rzetelne zarządzanie aplikacjami medycznymi:

Przed pobraniem i korzystaniem z aplikacji medycznych, upewnij się, że są one zaufane, a ich dostawca zapewnia odpowiednie zabezpieczenia danych - przykłady zaufanych platform: IKO, Luxmed, Medicover

7. Regularne aktualizacje oprogramowania:

Regularnie aktualizuj oprogramowanie swoich urządzeń, aby korzystać z najnowszych poprawek zabezpieczeń.