Nr specjalny 14
LUTY–KWIECIEŃ 2023
ISSN 2545-3297

WYDANIE SPECJALNE

RODO
W OCHRONIE ZDROWIA

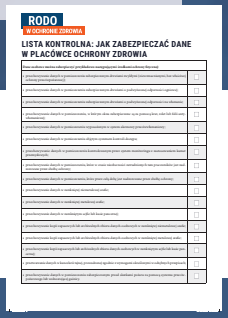
CYBERBEZPIECZEŃSTWO W PLACÓWKACH LECZNICZYCH

- Jak wykonać analizę ryzyka w placówce ochrony zdrowia
- Jakie są rekomendacje w zakresie cyberbezpieczeństwa placówek medycznych
- Jak zapobiegać atakom ransomware w placówce
- Jak zapewnić bezpieczne oprogramowanie oraz pocztę elektroniczną

WZORY DOKUMENTÓW

- Lista kontrolna: Co powinna zawierać Dokumentacja SZBI
- Lista kontrolna: Jakie są zasady bezpiecznego użytkowania sprzętu IT
- Ewidencja czynności w systemie informatycznym

PREZENT!
Jak zabezpieczać dane w placówce


RODO
W OCHRONIE ZDROWIA
LISTA KONTROLNA: JAK ZABEZPIECZAĆ DANE W PLACÓWCE OCHRONY ZDROWIA

Wydanie online magazynu czytaj na www.RODOmed24.pl

BEZPŁATNE WEBINARIA

DLA NASZYCH PRENUMERATORÓW **Bez rejestracji!**

Patron merytoryczny webinariów

F/K LEGAL

NOWE TERMINY I TEMATY JUŻ WKRÓTCE

1

Webinarium:
27.02.2023
12.00–13.15

Ustawa o jakości w ochronie zdrowia – przegląd zmian dla świadczeniodawców

Maciej Mrożewski – radca prawny/lawyer w Kancelarii F/K Legal

JAK WZIĄĆ UDZIAŁ? Nie musisz się rejestrować!

1. Wejdź na **rodomed24.pl**, do zakładki Szkolenia i Konferencje.
2. Wybierz webinarium, które Cię interesuje.
3. Kliknij w podany link w terminie webinarium.

Prelegent:

Maciej Mrożewski – lawyer, radca prawny. Specjalizuje się w prawie cywilnym procesowym i materialnym. Zajmuje się sprawami o błąd w sztuce medycznej oraz tymi z zakresu odszkodowań majątkowych i osobowych, sprawami windykacyjnymi oraz z zakresu prawa pracy i prawa rodzinnego. W trakcie studiów doświadczenie zdobywał jako wolontariusz Kliniki Prawa WPiA UŁ. Pracę magisterską poświęconą przestępstwu nieudzielenia pomocy przez lekarza obronił w Katedrze Prawa Karnego pod kierunkiem prof. dr hab. Agnieszki Liszewskiej. Doświadczenie zawodowe zdobywał, pracując w kancelariach prawnych w Łodzi oraz odbywając praktykę w sądach. Włada językami angielskim i francuskim. Odbył aplikację radcowską przy Okręgowej Izbie Radców Prawnych w Łodzi. Współpracuje z Kancelarią Fortak & Karasiński Radcowie Prawni od 2021 roku.

RODO
W OCHRONIE ZDROWIA

Wiedza i Praktyka
ul. Łotewska 9A, 03-918 Warszawa
NIP: 526-19-92-256
Redaktor:
Anna Śmigulska-Wojciechowska
Kierownik grupy tematycznej:
Alina Sulgostowska
Wydawca: Klaudia Bogumił
Koordynacja produkcji:
Mariusz Jezierski, Magdalena Huta
Korekta: Zespół
Projekt graficzny publikacji:
Piotr Fedorczyk
Skład i łamanie: Raster studio
Drukarnia: KRM Druk
Nakład: 550 egz.
Nr rejestrowy BDO: 000008579
E-mail do redakcji: rodomed24@wip.pl
Informacje o prenumeracie:
tel.: 22 518 29 29
faks: 22 617 60 10
e-mail: cok@wip.pl
Czynne pon.–pt. w godz. 8.00–16.00
Poza godzinami pracy można pozostawić wiadomość w skrzynce głosowej.

W numerze:

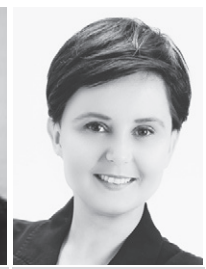
CYBERBEZPIECZEŃSTWO W PLACÓWKACH LECZNICZYCH

Piszą dla Ciebie nasi eksperci:

Agnieszka Sztuwe
radca prawny, Kancelaria Radców Prawnych i Adwokatów Naworska Marszałek sp. p. w Toruniu

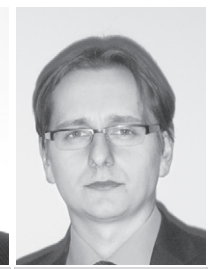
Marzena Pytlarz
radca prawny, specjalizuje się w ochronie danych osobowych i prawie medycznym

Michał Grabiec
radca prawny, kancelaria GW Legal Grabiec & Wójcik sp. p.



Marta Bogusiak
radca prawny, partner w Kancelarii BOGUSIAK UZDROWSKA KOWALCZYK Radcowie prawni sp. p.

Maciej Lipka
specjalista w zakresie ochrony danych osobowych



Łukasz Siudak
radca prawny, specjalista z prawa medycznego

Anna Śmigulska-Wojciechowska
redaktor prowadząca

Zapraszam do zadawania pytań.
Odpowiadamy na najczęściej pojawiające się pytania. Wyślij e-mail:
rodomed24@wip.pl

Szanowna Czytelniczko, Szanowny Czytelniku!

Bieżące wydanie numeru specjalnego czasopisma „RODO w Ochronie Zdrowia" poświęcone zostało niezwykle ważnemu tematowi, a mianowicie kwestii cyberbezpieczeństwa w placówkach ochrony zdrowia. Nasi eksperci wskazują i podpowiadają m.in., jakie należy stosować zabezpieczenia danych osobowych przetwarzanych w systemach teleinformatycznych, aby uniknąć np. ataku ransomware. Przeczytaj ten przewodnik zawierający aktualne wskazówki, przykłady, praktyczne porady. Z opracowania dowiesz się m.in.:

- *jak interpretować przepisy prawa dotyczące zabezpieczenia danych osobowych,*
- *jakie stanowisko zajmuje UODO,*
- *co w praktyce oznacza analiza ryzyka,*
- *jakie są techniczne aspekty zabezpieczenia danych osobowych przetwarzanych w systemach teleinformatycznych,*
- *jak bezpiecznie pobierać oprogramowanie oraz bezpiecznie korzystać z poczty elektronicznej,*
- *jak zarządzać podatnościami,*
- *jak monitorować sieć lokalną.*

Nasi eksperci przygotowali również wiele pomocnych dokumentów, jak np.:

- *Lista kontrolna: Co powinna zawierać Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji (str. 17),*
- *Lista kontrolna: jakie są zasady bezpiecznego użytkowania sprzętu IT (str. 18),*
- *Lista kontrolna: jakie są reguły korzystania z oprogramowania (str. 19),*
- *Ewidencja czynności w systemie informatycznym oraz ewidencja napraw systemu informatycznego (str. 20).*

Przypominam, iż całe wydanie czasopisma „RODO w Ochronie Zdrowia" dostępne jest w wersji online na stronie www.rodomed24.pl.

Życzę miłej lektury!

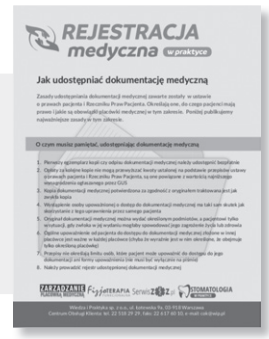
Anna Śmigulska-Wojciechowska

PS Jeśli masz problem, wyślij zapytanie na adres naszej redakcji rodomed24@wip.pl. Przekażemy je naszym ekspertom, a oni przygotują dla Ciebie gotowe rozwiązanie.

Drogi Czytelniku,

czekamy na opinie na temat naszej publikacji. Zależy nam na Twoim zdaniu dotyczącym przydatności porad naszych ekspertów w codziennej pracy.

Każdą opinię przesłaną na adres: rodomed24@wip.pl nagrodzimy niezbędnikiem pt. „Jak udostępniać dokumentację medyczną".



PARTNER MERYTORYCZNY: Kancelaria Adwokacka APDK w Warszawie

Z wydawnictwem „Wiedza i Praktyka" współpracujemy od kilku lat. Wszystkie publikacje są rzetelne i niezwykle pomocne. Nowy tytuł dotyczący RODO w sektorze ochrony zdrowia jest doskonałym miejscem na przedstawienie praktycznych aspektów ochrony danych osobowych w placówkach medycznych.

Gorąco polecamy!

Dominika Kołodziejska-Koza
adwokat

Agnieszka Pietrzak
adwokat

REKOMENDACJE W ZAKRESIE ARCHITEKTURY CYBERBEZPIECZEŃSTWA PLACÓWEK MEDYCZNYCH

Tworząc podstawy bezpieczeństwa infrastruktury informatycznej, należy skoncentrować się na obszarach objętych największym ryzykiem wycieku danych i ataku z zewnątrz na infrastrukturę wewnątrz jednostki. Niniejsza rekomendacja dotyczy typowych zagadnień cyberbezpieczeństwa (nie skupia się na wątku zasilania gwarantowanego) oraz zagadnień związanych z ciągłością działania i dokumentacji procesów oceny ryzyka i polityk w tym zakresie.

Poniższe rekomendacje opierają się na następujących priorytetach.

Priorytet pierwszy

Konieczność ochrony danych medycznych w przypadku skutecznego ataku ransomware. Nie ma możliwości zapewnienia 100% ochrony przed atakami. Dlatego największy nacisk należy położyć na działania zapewniające zachowanie jak najbardziej aktualnych danych w kopiach zapasowych. Kopie zapasowe w celu zapewnienia ich prawidłowego odczytania (odtworzenia danych) muszą być wykonywane regularnie, zgodnie z przestrzeganą polityką tworzenia kopii, muszą być regularnie weryfikowane w celu sprawdzenia ich możliwości odczytania, muszą być odmiejscowione dla uzyskania pewności, iż w momencie ataku kopie nie będą narażone na skasowanie.

Priorytet drugi

Ochrona poczty elektronicznej jako usługi własnej lub dzierżawionej. Atak typu ransomware opiera się na wykorzystaniu podatności serwerów pocztowych lub na metodzie polegającej na przesłaniu infekującego załącznika w poczcie elektronicznej. Konieczne jest zatem aktywne weryfikowanie treści załączników oraz linków zawartych w poczcie, a także ochrona dostępu do skrzynek poprzez wprowadzenie dodatkowych faktorów uwierzytelniania.

Priorytet trzeci

Ochrona brzegu sieci. Braki finansowe i niedostatek kadr wielokrotnie powodują brak aktualizacji, podatności w urządzeniach brzegowych. Konieczne jest uaktualnienie bądź zakup nowych urządzeń typu firewall. Urządzenia tego typu stanowią pierwszą i główną zaporę zasobów przed rekonesansem i atakiem cyberprzestępców. Podatności i niedostatki konfiguracyjne tych urządzeń powinny być likwidowane w celu ochrony zasobów danych.

Priorytet czwarty

Ochrona stacji roboczych. Atak typu ransomware polega na stopniowej infekcji wszystkich dostępnych stacji roboczych. Możliwość wykrycia i zablokowania aktywności polegającej na szyfrowaniu stacji roboczych powinna stanowić swoistą „drugą linię obrony" w przypadku zainfekowania sieci LAN. Segmentacja sieci lokalnych oraz stałe monitorowanie stacji roboczych będzie czynnikiem podnoszącym odporność zasobów na atak. Segmentacja sieci dodatkowo wspiera proces „oddzielenia" systemów kopii zapasowych od reszty systemów produkcyjnych (część priorytetu pierwszego).

PODSTAWOWE DZIAŁANIA W CELU REALIZACJI PRIORYTETÓW

W ramach podstawowych struktur systemu cyberbezpieczeństwa rekomendowane są działania w zakresie:

1. Audytu bezpieczeństwa na podstawie rozporządzenia KRI (w przypadku otrzymania decyzji OUK audyt musi obejmować obowiązki wynikające z ustawy o Krajowym Systemie Cyberbezpieczeństwa – informacje w tym miejscu https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-)
2. Instalacji urządzeń typu FIREWALL;
3. Skutecznej ochrony antywirusowej;
4. Skutecznej kopii zapasowej;
5. Bezpiecznej poczty elektronicznej;
6. Przygotowania dokumentacji Zintegrowanego Systemu Zarządzania Bezpieczeństwem w jednostce;
7. Przygotowania i przeprowadzenia cyklicznych szkoleń całej załogi w zakresie bezpieczeństwa.

Źródło:
- „Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia", Centrum e-Zdrowia