

Jak zabezpieczyć cyfrowe dane medyczne

59 porad i 38 dokumentów
dla placówki

stan prawny na czerwiec 2022 r.

SERWIS **ZOZ**.PL

ZARZĄDZANIE W OCHRONIE ZDROWIA

NOWOŚĆ! BEZPIECZEŃSTWO EPIDEMIOLOGICZNE - PROCEDURY

Zarządzaj placówką efektywnie i skutecznie

BEZPŁATNE KONTO TESTOWE

na SerwisZOZ.pl 24h/7 do pełnych zasobów portalu!



Możesz z niego korzystać na swoim laptopie, tablecie czy telefonie



Jesteś zainteresowany płatną subskrypcją? Zadzwoń do nas lub napisz e-mail.

Nasi konsultanci dopasują najlepszą ofertę dla Ciebie.

SerwisZOZ.pl dostępny jest 24h/7 dni w tygodniu na laptopie, telefonie i tablecie.

Korzystaj wygodnie z wiedzy gdziekolwiek jesteś!

Zamówienia przyjmuje Centrum Obsługi Klienta: **22 518 29 29**, e-mail: **cok@wip.pl**.

Jak zabezpieczyć cyfrowe dane medyczne

**59 porad i 38 dokumentów
dla placówki**

Autorzy:

Marta Bogusiak

radca prawny, partner w Kancelarii prawnej Bogusiak Uzdrawska Kowalczyk Radcowie Prawni sp. p.

Michał Grabiec

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

Patrycja Krótka

aplikant radcowski, Kancelaria Naworska Marszałek sp. k. w Toruniu

Maciej Lipka

prawnik i specjalista ds. danych osobowych, były pracownik departamentów skarg, legislacji i prasowego w Urzędzie Ochrony Danych Osobowych; na bazie swojego doświadczenia doradza, jak dostosować organizację do aktualnych przepisów oraz zdarzeń mających wpływ na przetwarzanie danych

Karolina Polowczyk

aplikant radcowski, Kancelaria Fortak & Karasiński Radcowie Prawni sp. p.

Marzena Pytlarz-Pietraszko

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

Agnieszka Sienko

radca prawny, specjalista prawa ochrony zdrowia, jest także pracownikiem naukowo-dydaktycznym Uniwersytetu Medycznego im. Piastów Śląskich we Wrocławiu. Doświadczenia zawodowe zdobywała jeszcze w Branżowej Kasie Chorych dla Służb Mundurowych, w Departamencie Polityki Zdrowotnej Urzędu Marszałkowskiego Województwa Dolnośląskiego, wreszcie w publicznych i niepublicznych zakładach opieki zdrowotnej

Anna Słowińska

prawnik, absolwentka Wydziału Prawa Uniwersytetu Szczecińskiego i studiów podyplomowych „Prawa i Wolności człowieka” zorganizowanych przez Instytut Nauk Prawnych PAN i Helsińską Fundację Praw Człowieka. Autorka i współautorka kilkuset artykułów i kilku publikacji książkowych z zakresu tematyki prawa pracy, bhp, ochrony zdrowia, praw człowieka. Założycielka Fundacji Lepsze Prawa Człowieka działającej w obszarze ochrony praw człowieka, która m.in. monitoruje przestrzeganie bhp przez podmioty lecznicze

Agata Starecka-Dembek

radca prawny w Kancelarii Fortak & Karasiński Radcowie Prawni sp. p.

Agnieszka Sztuwe

radca prawny w Kancelarii Adwokatów Naworska Marszałek sp. k. w Toruniu; w praktyce zawodowej zajmuje się obsługą przedsiębiorców, przede wszystkim w zakresie ochrony danych osobowych (z uwzględnieniem RODO)

Dariusz Wójcik

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

Redaktor: **Michał Kowalski**

Menedżer produktu: **Aleksandra Świder**

Segment manager: **Alina Sulgostowska**

Projekt graficzny okładki: **Piotr Fedorczyk**

Korekta: **Zespół**

Koordynator produkcji: **Magdalena Huta**

Druk: **KRM Druk**

Skład i łamanie: **Dariusz Ziach**

ISBN 978-83-8276-565-6

Copyright by Wiedza i Praktyka sp. z o.o.

Warszawa 2022

Wiedza i Praktyka sp. z o.o.

ul. Łotewska 9a, 03-918 Warszawa,

tel. 22 518 29 29, faks 22 617 60 10, e-mail: cok@wip.pl

NIP: 526-19-92-256, KRS: 0000098264 – Sąd Rejonowy dla m.st. Warszawy w Warszawie,

XIII Wydział Gospodarczy Krajowego Rejestru Sądowego,

wysokość kapitału zakładowego 200.000 zł,

nr rejestrowy BDO: 000008579.

Publikacja „Jak zabezpieczać cyfrowe dane medyczne. 59 porad i 38 dokumentów dla placówki” została przygotowana z zachowaniem najwyższej staranności i wykorzystaniem wysokich kwalifikacji, wiedzy oraz doświadczenia jej twórców. Zaproponowane w niej wskazówki, porady i interpretacje dotyczą sytuacji typowych. Ich zastosowanie w konkretnym przypadku może wymagać dodatkowych, pogłębionych konsultacji. Opublikowane rozwiązania nie mogą być traktowane jako oficjalne stanowisko organów i urzędów państwowych. W konsekwencji autorzy, konsultanci oraz redakcja nie mogą ponosić odpowiedzialności prawnej za zastosowanie zawartych w publikacji „Jak zabezpieczać cyfrowe dane medyczne. 59 porad i 38 dokumentów dla placówki” wskazówek, przykładów, informacji itp. do konkretnych przypadków.

Szanowny Czytelniku!

Oddajemy w Twoje ręce drugie wydanie publikacji „Jak zabezpieczać cyfrowe dane medyczne”. Znajdziesz w niej praktyczne wskazówki dotyczące przede wszystkim prowadzenia dokumentacji medycznej w postaci elektronicznej. Właśnie w takiej dokumentacji przetwarzane są bowiem cyfrowe dane medyczne. Zabezpieczenie tej dokumentacji powinno być więc priorytetem każdej placówki medycznej. W publikacji znajdziesz przede wszystkim wyjaśnienie, kiedy należy prowadzić dokumentację medyczną w postaci elektronicznej, a kiedy w grę wchodzi jeszcze papierowa. Dużą uwagę poświęcamy oczywiście metodom zabezpieczenia dokumentacji medycznej. Jak zabezpieczyć serwery? Czy należy stosować szyfrowanie? Czym jest SZBI? Czy konieczne są audyty bezpieczeństwa? Kogo upoważnić do dostępu do dokumentacji medycznej? Na te pytania odpowiedź znajdziesz w książce. Oprócz tego w przystępny sposób przedstawione zostały reguły udostępniania dokumentacji medycznej.

Z kolei w drugiej części znajdziesz wyjaśnienie, jak bezpiecznie i zgodnie z przepisami udzielać teleporad. Do tego będziesz mógł skorzystać z pakietu aż 38 wzorów dokumentów i checkliście przydatnych dla każdej placówki medycznej.

W stosunku do pierwszego wydania przedstawiliśmy wiele nowych zagadnień, takich jak np. forma prowadzenia list oczekujących, stosowanie skanów, pobieranie opłat o firm ubezpieczeniowych, czy też dostęp do dokumentacji medycznej dziecka. Warto dodać, że kolejne wydanie publikacji uwzględniła stan prawny z czerwca 2022 r. Wzięto w nim pod uwagę zmiany prawne m.in. w zakresie informowania o teleporadach.

Życzę owocnej lektury

Michał Kowalski

radca prawny, redaktor publikacji

SPIS TREŚCI

ROZDZIAŁ I. ELEKTRONICZNA DOKUMENTACJA MEDYCZNA	7
1.1. Czym jest elektroniczna dokumentacja medyczna	7
1.2. Dlaczego forma elektroniczna	8
1.3. Co wchodzi w skład dokumentacji	8
1.4. Kiedy forma papierowa	10
1.5. Obowiązki w związku z wdrożeniem dokumentacji elektronicznej	17
1.6. Kiedy upoważnienie, a kiedy powierzenie przetwarzania	18
1.7. Jak zabezpieczyć dokumentację elektroniczną	19
1.8. Bezpieczeństwo serwerów	21
1.8.1. Model klasyczny: wytwarzanie i przechowywanie	21
1.8.2. Obszary bezpieczeństwa	21
1.8.3. Zabezpieczenie pomieszczeń tzw. krytycznych	22
1.8.4. Szyfrowanie danych medycznych	23
1.8.5. Audyty bezpieczeństwa	23
1.8.6. Ograniczenia w serwerowni	23
1.8.7. Bezpieczeństwo fizyczne gabinetu	24
1.8.8. Dwa źródła zasilania i UPS	24
1.8.9. Niszczenie nośników danych	25
1.9. Polska Implementacja Krajowa HL7 CDA	25
1.10. Czy konieczne szyfrowanie	26
1.11. Dokumentacja a SZBI w placówce publicznej	29
1.12. Dlaczego należy przeprowadzać audyty	34
1.13. Konieczne szkolenia w placówkach publicznych	37
1.14. Zgoda pacjenta na zabieg – czy także w formie elektronicznej	39
1.15. Kto dokonuje wpisów w dokumentacji	41
1.16. Jak postąpić w przypadku pomyłki w dokumentacji	43
1.17. Jak udostępniać elektroniczną dokumentację medyczną	45
1.17.1. Upoważnienia do odbioru dokumentacji	48
1.17.2. Udostępnianie dokumentacji w formie skanów	49
1.17.3. Udostępnianie dokumentacji w czasie pandemii	53
1.17.4. Udostępnianie a opłaty	55
1.17.5. Jak uregulować dostęp do dokumentacji medycznej małoletniego	57
1.17.6. Co z udostępnianiem dokumentacji na żądanie Policji i innych organów	60
1.18. Jak zorganizować obieg dokumentacji	63
1.19. Podpisywanie dokumentacji medycznej	67
1.20. Przekazywanie informacji o pacjentach do innych placówek	70
1.21. Jakie są konsekwencje utraty dokumentacji medycznej?	74

ROZDZIAŁ II. ZASADY UDZIELANIA TELEPORAD	77
2.1. Czym jest teleporada	77
2.2. Jakie uprawnienia ma lekarz udzielający teleporady	78
2.3. Standardy organizacyjne teleporady	79
2.4. Jak zarejestrować pacjenta na teleporadę	81
2.5. W jaki sposób rejestrować pacjentów gabinetu stomatologicznego na teleporadę	83
2.6. Przebieg teleporady	84
2.7. Teleporady mogą wiązać się z przetwarzaniem danych	85
2.8. Czy można przetwarzać wizerunek pacjenta	85
2.9. Należy unikać podpisywania zdjęć	86
2.10. Czy konieczna zgoda pacjenta	86
2.11. Karta teleporady	87
2.12. Przekazanie dokumentacji z teleporady pacjentowi	88
2.13. Jak długo przechowywać dokumentację medyczną z teleporady	89
2.14. Teleporada a obowiązek informacyjny	92
2.15. Dane pacjenta muszą być bezpieczne	93
2.16. Jak komunikować się zdalnie w zgodzie z RODO	93
2.17. Bezpieczne dane pacjenta na smartfonie	95
2.18. System do udzielania teleporad	97
2.19. Finansowanie teleporad przez NFZ	99
2.20. Internetowe Konto Pacjenta	100
2.21. Przechowywanie danych pacjentów na poczcie e-mail	101
2.22. Zlecenie testów na COVID-19 w ramach teleporady	104
2.23. Konieczna umowa powierzenia z dostawcą teleporady	107
ROZDZIAŁ III. WZORY DOKUMENTÓW I LISTY KONTROLNE	109
Wzór 1. Wykaz udostępnianej dokumentacji medycznej	109
Wzór 2. Plan całodobowego zabezpieczenia dokumentacji medycznej	110
Wzór 3. Arkusz analizy ryzyka – przed wdrożeniem elektronicznej dokumentacji medycznej	114
Wzór 4. Procedura odtwarzania systemów po awarii i ich testowania	117
Wzór 5. Protokół odtwarzania systemu po awarii i testowania	118
Wzór 6. Karta teleporady	119
Wzór 7. Regulamin udzielania świadczeń zdrowotnych za pomocą środków porozumiewania się na odległość	120
Wzór 8. Analiza technicznych i informatycznych środków bezpieczeństwa informacji	124
Wzór 9. Dokumenty związane z bezpieczeństwem danych cyfrowych – zestawienie	135
Wzór 10. Plan audytu ochrony danych osobowych	137
Wzór 11. Procedura odtwarzania systemów po awarii i ich testowania	139
Wzór 12. Procedura reagowania na incydenty bezpieczeństwa informacji	140
Wzór 13. Wniosek o udzielenie dofinansowania na rozwój informatyzacji świadczeń opieki zdrowotnej	143
Lista kontrolna 1. 5 elementów do sprawdzenia w elektronicznej dokumentacji medycznej	145

Lista kontrolna 2. Jakie zabezpieczenia stosujesz w odniesieniu do elektronicznych nośników informacji – lista kontrolna	146
Lista kontrolna 3. Łączenie dokumentacji papierowej z dokumentacją w postaci elektronicznej	147
Lista kontrolna 4. Czy oprogramowanie w podmiocie spełnia najważniejsze warunki bezpieczeństwa	148
Lista kontrolna 5. Jak zapewnić bezpieczeństwo danych osobowych przetwarzanych w EDM	149
Lista kontrolna 6. Udostępnianie dokumentacji medycznej	151
Lista kontrolna 7. Jak prowadzić dokumentację medyczną wizyt zdalnych	152
Lista kontrolna 8. Jak chronić dane osobowe, udzielając teleporad	153
Lista kontrolna 9. Prawo pacjenta do informacji o stanie zdrowia (komunikacja z osobami uprawnionymi na odległość)	154
Lista kontrolna 10. Jak prowadzić dokumentację medyczną wizyt zdalnych	155
Lista kontrolna 11. Bezpieczna wideokonferencja (wskazówki przydatne także w przypadku teleporad)	156
Lista kontrolna 12. Jakie rozwiązania możesz zastosować w przypadku prywatnych urządzeń mobilnych	159
Lista kontrolna 13. Jak zabezpieczyć dane przekazywane za pośrednictwem poczty elektronicznej	160
Lista kontrolna 14. Bezpieczeństwo danych przechowywanych w aplikacjach klasy EDM	161
Lista kontrolna 15. Co zawrzeć w procedurze rozpatrywania skarg i wniosków – lista kontrolna	163
Lista kontrolna 16. Czy możesz podać telefonicznie kod niezbędny do realizacji e-recepty – lista kontrolna	165
Lista kontrolna 17. Jak przeprowadzić ocenę skutków przetwarzania danych osobowych w EDM	166
Lista kontrolna 18. Jak szacować ryzyko związane z przetwarzaniem danych osobowych w EDM	169
Lista kontrolna 19. Jak sprawdzić procesora przed zawarciem umowy powierzenia przetwarzania danych osobowych	172
Lista kontrolna 20. Jak usuwać dane osobowe na żądanie	173
Lista kontrolna 21. Oświadczenia pacjenta w formie papierowej i elektronicznej – jak je przechowywać – lista kontrolna	174
Lista kontrolna 22. Przekazywanie informacji o stanie zdrowia pacjenta na odległość zgodnie z wytycznymi RPP i prezesa UODO – lista kontrolna	175
Lista kontrolna 23. Sprawdź, czym się kierować przy wyborze audytora	177
Lista kontrolna 24. Sprawdź, czy jesteś przygotowany do kontroli UODO	179
Lista kontrolna 25. W jaki sposób możesz podpisywać e-dokumentację	181
ROZDZIAŁ IV. WYKAZ AKTÓW PRAWNYCH, NA KTÓRE POWOŁANO SIĘ W PUBLIKACJI	183

ROZDZIAŁ I. ELEKTRONICZNA DOKUMENTACJA MEDYCZNA

1.1. Czym jest elektroniczna dokumentacja medyczna

Zgodnie z ustawą o systemie informacji w ochronie zdrowia **elektroniczna dokumentacja medyczna (EDM)** to określone poniżej dokumenty, które:

- wytworzono w postaci elektronicznej oraz
- opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo uwierzytelniono z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych (ZUS).

Ponadto dokumenty te muszą być dokumentami wskazanymi w poniższej tabeli.

Elektronicznej dokumentacji medycznej nie możemy całkowicie utożsamiać z dokumentacją medyczną prowadzoną w postaci elektronicznej, gdyż ta ostatnia ma szerszy zakres niż opisany powyżej. Innymi słowy, **każda EDM jest dokumentacją medyczną, natomiast nie każda dokumentacja medyczna ma status EDM**. Poza tym EDM podlega w przypadkach określonych w ustawie o systemie informacji o ochronie zdrowia elektronicznej wymianie pomiędzy usługodawcami w ramach wdrażanych systemów takich jak np. Elektroniczna Platforma Gromadzenia, Analiz i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych. Można też zakładać, że katalog dokumentów zaliczanych do EDM będzie się stale powiększać.