

SPIS TREŚCI

| | |
|---|------------|
| ROZDZIAŁ 1. E-ZDROWIE | 5 |
| 1.1. Technologie wspierające poprawę jakości usług medycznych | 5 |
| 1.2. Najważniejsze aspekty telemedycyny | 9 |
| 1.3. Aktualne wymogi związane z przekazywaniem informacji do Systemu Ewidencji Zasobów Ochrony Zdrowia | 13 |
| 1.4. Centralna e-rejestracja | 17 |
| 1.5. Polski System Weryfikacji Leków | 21 |
| 1.6. Kody kreskowe na wyrobach medycznych | 23 |
| 1.7. Kody kreskowe wykorzystywane do identyfikacji pacjentów | 25 |
| 1.8. Zabezpieczanie pacjenta przed podaniem niewłaściwego leku, wykorzystując kody kreskowe z opasek | 26 |
| 1.9. Wykorzystanie sztucznej inteligencji w placówce medycznej | 27 |
| 1.10. Zrobotyzowana Automatyzacja Procesów w placówce medycznej | 31 |
| 1.11. Aplikacje mobilne w placówce medycznej | 34 |
| 1.12. Elektroniczny domowy stetoskop bazujący na sztucznej inteligencji | 37 |
| 1.13. Nowe technologie w medycynie – przegląd najciekawszych polskich rozwiązań | 39 |
| 1.14. Wykorzystanie ChatGPT w placówce medycznej | 41 |
| 1.15. Nadzór telemetryczny | 45 |
| ROZDZIAŁ 2. BEZPIECZEŃSTWO DANYCH PRZETWARZANYCH W PLACÓWCE MEDYCZNEJ | 49 |
| 2.1. Polska Implementacja Krajowa HL7 CDA | 49 |
| 2.2. Zasady zabezpieczania dokumentacji elektronicznej | 51 |
| 2.3. Bezpieczeństwo serwerów | 54 |
| 2.4. Wpisy w dokumentacji | 71 |
| 2.5. Pomyłka w dokumentacji | 74 |
| 2.6. Zasady udostępniania elektronicznej dokumentacji medycznej | 76 |
| 2.7. Przekazywanie informacji o pacjentach do innych placówek | 96 |
| 2.8. Bezpieczne dane pacjenta na smartfonie | 100 |
| 2.9. Przechowywanie danych pacjentów na poczcie e-mail | 103 |
| 2.10. Wykonywanie kopii zapasowych danych | 105 |
| 2.11. Pierwszy zatwierdzony kodeks postępowania dla sektora medycznego | 109 |
| 2.12. Bezpieczeństwo sieci lokalnej w placówce medycznej | 114 |
| ROZDZIAŁ 3. CYBERBEZPIECZEŃSTWO | 119 |
| 3.1. Cyberbezpieczeństwo w placówkach medycznych | 119 |
| 3.2. Rekomendacje w zakresie architektury cyberbezpieczeństwa placówek medycznych | 127 |
| 3.3. Rozwiązania informatyczne stosowane w placówce dla bezpieczeństwa przetwarzanych danych | 129 |
| 3.4. Analiza ryzyka w placówce ochrony zdrowia | 135 |

| | |
|--|------------|
| 3.5. Zabezpieczenie danych przetwarzanych w systemach teleinformatycznych od strony technicznej | 137 |
| 3.6. Bezpieczne oprogramowanie oraz poczta elektroniczna | 141 |
| 3.7. Analiza ryzyka w zakresie ataku ransomware w placówce | 146 |
| PODSTAWA PRAWNA | 152 |