

Rekomendacje w zakresie architektury cyberbezpieczeństwa placówek medycznych	4
Jak stosować przepisy dotyczące zabezpieczenia danych osobowych	5
Analiza ryzyka w placówce ochrony zdrowia – o czym należy pamiętać	8
Zabezpieczenie danych przetwarzanych w systemach teleinformatycznych od strony technicznej	9
Jak zapewnić bezpieczne oprogramowanie oraz pocztę elektroniczną	11
Jak wdrażać analizę ryzyka w zakresie ataku ransomware w placówce	13
Czy przystąpić do stosowania kodeksu postępowania dla sektora medycznego	16
Lista kontrolna: Co powinna zawierać Dokumentacja Systemu Zarządzania Bezpieczeństwem Informacji	18
Lista kontrolna: Jakie są zasady bezpiecznego użytkowania sprzętu IT	19
Lista kontrolna: Jakie są reguły korzystania z oprogramowania	20
Ewidencja czynności w systemie informatycznym oraz ewidencja napraw systemu informatycznego	21
Jak uchronić placówkę medyczną przed cyberatakiem – wskazówki dla administratorów	22
Lista kontrolna: Czy przestrzegasz najważniejszych zasad ochrony danych pacjenta	25
Lista kontrolna: Czy nie dopuszczasz się najczęstszych uchybień w prowadzeniu dokumentacji medycznej	26
Lista kontrolna: Jakie zabezpieczenia danych zastosować zgodnie z RODO	27
Procedura nadawania uprawnień w systemie informatycznym	28
Zasady korzystania z poczty elektronicznej	32