

## **Procedura Anonimizacji Danych Medycznych**

Celem niniejszego dokumentu jest określenie zasad anonimizacji danych medycznych, zgodnie z obowiązującymi przepisami prawa (RODO, HIPAA) oraz najlepszymi praktykami w zakresie ochrony prywatności pacjentów.

### **1. Definicje**

Anonimizacja – proces przetwarzania danych osobowych w taki sposób, aby osoby, których one dotyczą, nie mogły zostać zidentyfikowane w żadnym przypadku.

Pseudonimizacja – przetwarzanie danych w taki sposób, że nie można ich przypisać konkretnej osobie bez użycia dodatkowych informacji przechowywanych oddzielnie.

### **2. Zakres danych do anonimizacji**

Dane bezpośrednio identyfikujące np:

- Imię i nazwisko
- PESEL, numer dokumentu tożsamości
- Adres zamieszkania, e-mail, telefon
- IP, ID użytkownika

Dane pośrednio identyfikujące np.:

- Data urodzenia (redukowana do roku)
- Miejscowość (redukowana do województwa)
- Nietypowe cechy medyczne

### **3. Metody anonimizacji**

- Usuwanie pól zawierających dane osobowe
- Agregacja danych (np. wiek w przedziałach)
- Redukcja precyzji (np. data do miesiąca lub roku)
- Maskowanie (np. \*\*\* zamiast imienia)
- Tokenizacja/pseudonimizacja (losowy identyfikator)

### **4. Anonimizacja plików DICOM**

- Usunięcie tagów: PatientName, PatientID, InstitutionName, StudyDate
- Redakcja warstwy graficznej (OCR i zamazanie danych na obrazach)
- Użycie narzędzi: DicomCleaner, pydicom, GDCM

### **5. Dokumentacja procesu**

- Każda sesja anonimizacji powinna być dokumentowana
- Należy zapisać: datę, osobę odpowiedzialną, zakres usuniętych danych
- Dane nie mogą być odtworzone – brak klucza odwrotnego

## **6. Ocena skuteczności anonimizacji**

- Przeprowadzenie testów deanonimizacji
- Ocena ryzyka przy danych rzadkich lub szczególnych
- Zastosowanie normy ISO/TS 25237:2017

## **7. Przepisy i normy**

- RODO (art. 4, 9, 89)
- HIPAA Safe Harbor
- ISO/TS 25237:2017