Telemedycyna w świetle przepisów o ochronie danych osobowych ze szczególnym uwzględnieniem telepsychiatrii

Telemedicine, with the emphasis on telepsychiatry, in the light of the regulations of personal data protection

Anna Nycz, Radosław Tworus

Klinika Psychiatrii, Stresu Bojowego i Psychotraumatologii CSK MON WIM w Warszawie;
kierownik: płk dr n. med. Radosław Tworus

Streszczenie. Unijne rozporządzenie dotyczące przetwarzania danych osobowych, które weszło w życie 25 maja 2018 r., rzuca nowe światło na aspekt bezpieczeństwa danych w nowoczesnej medycynie, nakładając szereg wymogów na administratorów oraz podmioty przetwarzające dane osobowe. W publikacji przedstawiono wybrane zagadnienia bezpieczeństwa medycznych danych osobowych z uwzględnieniem newralgicznego obszaru ochrony danych, tj. pacjentów leczonych psychiatrycznie. W pracy podkreślono, że zapewnienie prawidłowego i skutecznego przetwarzania danych osobowych jest uwarunkowane współdziałaniem zespołów interdyscyplinarnych, tj. środowiska medycznego, specjalistów z zakresu informatyki medycznej, specjalistów zajmujących się wdrażaniem polityki ochrony systemów medycznych i przetwarzania danych oraz prawników.
Słowa kluczowe: telemedycyna, telepsychiatria, dane osobowe, bezpieczeństwo informacji, cyberprzestępczość, RODO

Abstract. European Union Data Protection Directive, which came into force on 25th May 2019, casts new light on the aspect of data security in modern medicine and imposes a range of requirements on the administrators and subjects involved in personal data processing. This study discusses selected issues of personal medical data security with an emphasis on the area as sensitive as data security of psychiatric patients. The study underlines that the correctness and efficiency of personal data processing relies heavily on the cooperation of interdisciplinary teams i.e. medical staff, health informatics specialists, specialists responsible for the implementation of the policy of medical systems security and personal data processing, and lawyers.
Key words: cybercrime, GDPR (General Data Protection Regulation), information security, personal data, telemedicine, telepsychiatry

Nadesłano: 19.02.2019. Przyjęto do druku: 6.09.2019
Nie zgłoszono sprzeczności interesów.
Lek. Wojsk., 2019; 97 (4): 341–344

Adres do korespondencji
mgr Anna Nycz
Klinika Psychiatrii, Stresu Bojowego
i Psychotraumatologii CSK MON WIM
ul. Szaserów 128, 04-141 Warszawa
tel. +48 261 816 450
e-mail: anycz@wim.mil.pl

Wstęp

Odpowiedzialność za bezpieczeństwo danych zawartych w dokumentacji medycznej pacjenta – czy to prowadzonej w sposób tradycyjny, tj. papierowy, czy elektroniczny – powinna być dla systemu ochrony priorytetowym zadaniem. W dobie ciągłego i szybkiego rozwoju technologicznego zapewnienie bezpieczeństwa danych, zwłaszcza w nowoczesnej telemedycynie, może stanowić duże wyzwanie. Postęp technologiczny oraz proces globalizacji spowodowały, że znacząco zwiększyły się skala i zakres danych, zarówno w aspekcie ich zbierania, jak i wymiany. Wyzwaniem jest również to, że regulacje prawne dotyczące przetwarzania danych z użyciem

nowoczesnych rozwiązań telemedycznych powstają wolniej niż same rozwiązania. Dodatkowo nowo powstające technologie należy każdorazowo wnikliwie analizować pod kątem potencjalnych zagrożeń dla prywatności danych oraz ich ochrony. W myśl dokumentu RODO dane dotyczące zdrowia określane są mianem szczególnej kategorii danych osobowych, a co za tym idzie wymagają szczególnej ochrony.

Bezpieczeństwo przetwarzania danych, czyli art. 32 RODO

Podstawowym wyznacznikiem zabezpieczenia danych osobowych przy stosowaniu rozwiązań telemedycznych są prawidłowo i z należytą starannością zaprojektowane systemy teleinformatyczne służące do przesyłania danych medycznych. Mowa tu nie tylko o samych systemach komputerowych oraz oprogramowaniu obsługującym obszar szpitalny i lecznictwo ambulatoryjne, ale również o nowoczesnych aplikacjach medycznych, portalach pacjenta, czatach lekarz–pacjent czy systemach wideokonferencji. Warto, by bezpieczeństwem danych osobowych przetwarzanych z użyciem narzędzi telemedycznych zajmowały się profesjonalne firmy, posiadające długoletnie doświadczenie w powyższym zakresie, które przy projektowaniu i aktualizacji systemów będą wdrażały środki techniczne według art. 32 RODO [1]:

- pseudonimizację, czyli przetwarzanie danych osobowych w taki sposób, by niemożliwe było zidentyfikowanie, do kogo one należą, bez dostępu do informacji przechowywanych bezpiecznie w innym miejscu (np. szyfrowanie za pomocą klucza, tokenizacja, skracanie),
- szyfrowanie danych osobowych,
- możliwość ciągłego zapewnienia poufności, integralności, dostępności oraz odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych oraz organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Wszystkie wymienione powyżej elementy mają na celu maksymalne wykorzystanie sprawdzonych rozwiązań organizacyjno-technicznych w celu zmniejszenia ryzyka niewłaściwego przetwarzania danych. Co ważne, niewystarczające jest wprowadzenie danych rozwiązań raz na zawsze – administratorzy na bieżąco powinni analizować potencjalne ryzyka i dostosowywać swoje rozwiązania do zmieniającego się otoczenia.

Organizacyjne i techniczne rozwiązania w przetwarzaniu danych osobowych w usługach telemedycznych

Przepisy RODO nie dostarczają konkretnych rozwiązań – technicznych ani organizacyjnych – jakie powinien zastosować administrator w celu zapewnienia właściwej ochrony w procesie przetwarzania danych osobowych. RODO wskazuje jedynie, że przy ocenie ryzyka i ustanawianiu zabezpieczeń należy uwzględnić stan wiedzy technicznej, koszty wdrożenia oraz realne skutki wynikające z błędów w procesie przetwarzania danych osobowych [2]. Przy wyborze środków technicznych wykorzystywanych w rozwiązaniach z zakresu telemedycyny warto korzystać z międzynarodowych norm bezpieczeństwa, tj.:

- w zakresie rozwiązań kryptograficznych – szyfrowanie, techniki uwierzytelniania (ISO/IEC 29192),
- w zakresie rozwiązań związanych z naruszeniem ochrony danych medycznych – zarzadzanie, dokumentowanie, wyjaśnianie incydentów (ISO/IEC 27001),
- w zakresie rozwiązań pozwalających zabezpieczyć rozwiązania sprzętowe do przetwarzania danych medycznych (ISO/IEC 15408, 20243, 27036),
- w zakresie rozwiązań oceniających bezpieczeństwo systemów IT (ISO/IEC 15408, 17825, 18367 itp.).

Wszystkie opisane powyżej standardy mają na celu minimalizację ryzyka związanego z przetwarzaniem medycznych danych osobowych oraz ochronę przed głównymi zagrożeniami cybernetycznymi związanymi ze świadczeniami typu e-Health, do których zaliczyć należy:

- nieautoryzowaną modyfikację danych medycznych,
- nieautoryzowany dostęp do danych medycznych i związane z tym ryzyko ich ujawnienia,
- atak złośliwych oprogramowań typu ransomware, polegający na zaszyfrowaniu osobowych danych medycznych, a następnie żądanie okupu w zamian za przywrócenie dostępu do nich,
- przyłączenie elementu systemu wykorzystywanego do e-Health do botnetu, czyli maszyny – botmastera, która w sposób nieuprawniony wykonuje operacje i polecenia,
- odmowę realizacji usługi wynikającą z jej niedostępności z powodu przeciążenia elementu infrastruktury systemu [3,4].

Każde z powyższych zagrożeń stanowi nie tylko naruszenie artykułu 5. RODO, mówiącego o przetwarzaniu danych zgodnie z prawem, ograniczeniu celu przetwarzania, integralności, poufności i rozliczalności, ale może stanowić realne zagrożenie dla życia i zdrowia pacjenta [5]. Sytuacja taka miała już miejsce w historii. Warto przypomnieć sobie chociażby 12 maja 2017 r., w którym doszło do potężnego cyberataku, który zaszyfrował około

75 tys. systemów w niemal 100 krajach, a około 25 londyńskich szpitali pozbawił dostępu do danych pacjentów, powodując kompletny chaos w ich funkcjonowaniu.

Warto dodać, że w przypadku kradzieży danych medycznych konsekwencje są dużo poważniejsze niż na przykład w przypadku wycieku danych finansowych. Dane medyczne mogą stać się przedmiotem wielokrotnego przestępczego przetwarzania i analizowania, a w efekcie długotrwałego wykorzystywania, co uniemożliwia przywrócenie stanu sprzed kradzieży. Wszystkie podmioty wykonujące działalność leczniczą powinny mieć świadomość aktualnego zagrożenia cybernetycznego, którego zakładanym celem może być realny paraliż funkcjonowania państwa w zakresie zapewnienia obywatelom opieki medycznej [6].

Ochrona danych szczególnie wrażliwych, czyli RODO w telepsychiatrii

Poruszając zagadnienie przetwarzania danych osobowych w telefonicznych liniach interwencyjnych, należy wziąć pod uwagę kilka aspektów, m.in. rodzaj i zakres gromadzonych danych, wielkość zbioru danych, zespół osób uprawnionych do przetwarzania uzyskanych danych oraz możliwe zabezpieczenia i rozwiązania techniczno-organizacyjne mające na celu ich zabezpieczenie. Rodzaj i zakres gromadzonych danych osobowych zależy od specyfiki linii interwencyjnej oraz charakteru udzielanej pomocy.

Z pewnością linia interwencyjna dla osób z problemami zdrowia psychicznego wpisuje się w działalność związaną z przetwarzaniem ogromnej liczby danych o charakterze medycznym, szczególnie wrażliwych, ponieważ związanych z obszarem szeroko rozumianego zdrowia psychicznego. Wielkość takiego zbioru danych jest ściśle uzależniona od intensywności działania linii, natomiast biorąc pod uwagę szczegółowość i wnikliwość konieczną podczas zbierania wywiadu klinicznego, liczba danych wrażliwych uzyskanych podczas pojedynczej interwencji jest ogromna. Mowa tu nie tylko o danych ściśle medycznych, tj. przebiegu choroby, zażywanych lekach, ale również całej linii życiowej pacjenta. Podczas zbierania wywiadu psychiatrycznego przekazywane są również dane dotyczące światopoglądu, wyznawanej religii czy preferencji seksualnych. Są to dane, które standardowo nie wchodzą w zakres wywiadu w przypadku chorób somatycznych, natomiast stanowią nieodłączny element leczenia psychiatrycznego. W konsekwencji skłania to w sposób szczególny do dokładania najwyższej staranności w zakresie ochrony tych danych.

Kolejnym aspektem, który warto podkreślić w kontekście bezpieczeństwa informacji, jest sposób rejestrowania danych, czy to w systemie komputerowym, czy dokumentowanym w wersji papierowej, oraz związany z tym aspekt bezpieczeństwa przechowywania danych. Warto poza tym zadbać o ograniczenie dostępu do danych jedynie do osób, które są do nich uprawnione w wyniku podjętej interwencji, tj. konsultantów linii, koordynatorów, psychologów i psychiatrów podejmujących decyzję o dalszych działaniach wobec osoby telefonującej. Wobec zasady dobrowolności i anonimowości osób telefonujących do linii interwencyjnych warto zastosować pseudonimizację, która uniemożliwi w sposób bezpośredni identyfikację danej osoby, ale pozwoli na odtworzenie historii zgłoszeń, np. w przypadku powtarzających się, wielokrotnie ponawianych interwencji.

Aktualne wytyczne i zalecenia

Do najważniejszych standardów postępowania w zakresie przetwarzania danych osobowych można zaliczyć następujące dokumenty będące instrumentami miękkiego prawa:

- Rekomendacja Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej – 28.09.2017 r.,
- normy ISO,
- Ramy Bezpieczeństwa Cybernetycznego NIST, opracowane przez amerykański Krajowy Instytut Standaryzacji i Technologii,
- Kodeks Branżowy w Ochronie Zdrowia – projekt został złożony do Prezesa Urzędu Ochrony Danych Osobowych 13.11.2018 r. [7]

Podsumowanie

Pełne wykorzystywanie nowoczesnych technologii medycznych musi ściśle korelować z zapewnianiem najwyższego poziomu bezpieczeństwa przetwarzanych danych medycznych. Największe zagrożenia w zakresie świadczenia usług e-Health dotyczą wadliwych systemów informatycznych oraz cyberprzestępczości.

Piśmiennictwo

1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych. Dz. U. 2018 poz. 1000
2. Prawo.pl. RODO nie wskazuje środków i metod zabezpieczania danych, jedynie daje wskazówki [online]. https://www.prawo.pl/zdrowie/rodo-nie-wskazuje-srodkow-i-metod-zabezpieczania-danych-jedynie-daje-wskazowki,238269.html (dostęp: 3.11.2018)
3. Najbuk P, Kaźmierczyk P, Dziomdziora W, eds. Cyberbezpieczeństwo w sektorze ochrony zdrowia. Dziennik Gazeta Prawna, 2017; 159 (4558): 2–5
4. Jackowski M, ed. Ochrona danych medycznych. RODO w ochronie zdrowia. Wolters Kluwer, Warszawa 2018: 234–253

5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Dziennik Urzędowy Unii Europejskiej
6. Czubkowska S. Samorządy i szpitale lekceważą hakerów. A mogą za to słono zapłacić. Dziennik Gazeta Prawna, 2017; 213 (4612): 8–12
7. Najbuk P, Stępniowski J, Kaźmierczyk P. Branża medyczna już pisze własny kodeks ochrony danych osobowych. Dziennik Gazeta Prawna, 2017; 159 (4558): 2–5