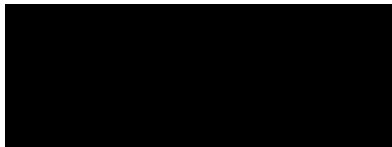




Ministerstwo Zdrowia

Departament
e-Zdrowia

EZDW.055.24.2026 [REDACTED]
Warszawa, 20 maja 2026



Szanowny Panie,

w odpowiedzi na petycję dotyczącą funkcjonowania Systemu Informacji Medycznej (P1), w szczególności w obszarze ochrony prywatności pacjentów oraz zasad raportowania danych medycznych, proszę o przyjęcie poniższego.

Ad.1.

„Dobrowolność raportowania usług prywatnych – świadczenia zdrowotne, badania laboratoryjne i diagnostyczne finansowane prywatnie nie powinny być automatycznie raportowane do P1. Dane mogą być przekazywane wyłącznie za świadomą zgodą pacjenta.”

Zgodnie z art. 56 ust. 2a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U.2026.208 t.j. dalej: „ustawa o SIOZ”), usługodawcy są obowiązani przekazywać do SIM dane zdarzenia medycznego przetwarzanego w systemie informacji od dnia 1 lipca 2021 r. Celem ustanowienia tego przepisu było umożliwienie wymiany elektronicznej dokumentacji medycznej (dalej: EDM) między podmiotami leczniczymi, a także stworzenie pełnej, elektronicznej historii leczenia pacjenta, poprawa bezpieczeństwa danych i pacjenta oraz automatyzacja procesów sprawozdawczych. Z uwagi na powyższe cele, postanowiono uznać za konieczne obligatoryjne raportowanie do systemu przez usługodawców z sektora publicznego i prywatnego, wzbogacając tym system informacji w ochronie zdrowia i usprawniając jego funkcjonalności, z pożytkiem dla samego pacjenta. Zatem raportowanie zdarzeń medycznych przez usługodawców (tj. publiczne i prywatne podmioty wykonujące działalność leczniczą) odbywa się na podstawie przepisów ustawy nie zaś na podstawie zgody pacjenta. Tym samym działanie takie jest w pełni legalne i zgodne z przepisami rangi ustawowej. Przywołany przepis ustawy korzysta z domniemania zgodności z Konstytucją RP. Zatem w tym kontekście zarzut o ewentualnej niezgodności z art. 47 Konstytucji RP należy uznać za nieuprawniony.

W związku z powyższym brak jest podstaw do zmiany zasad raportowania danych ze względu na źródło finansowania świadczenia., z uwagi na pozytywny ich wpływ na cały sektor ochrony zdrowia.

Ad.2.

„Prawo do bycia zapomnianym – stworzenie możliwości trwałego usunięcia wybranych danych z IKP, o ile nie są one wymagane do celów rozliczeniowych lub medycznych.”

Podstawę prawną do przetwarzania danych osobowych przez Ministra Zdrowia jako administratora danych osobowych stanowią przepisy ustawy o systemie, w związku z art. 9 ust. 1 lit. h Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz. Urz. UE L 119 z 04.05.2016 r., s. 1, z późn. zm.), dalej: RODO: przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego (...). W odniesieniu do dokumentu Polityki Prywatności zamieszczonego na stronie internetowej pacjent.gov.pl i prawa do usunięcia danych zgodnie z art. 17 RODO, uprzejmie informuję, że w świetle samego RODO prawo do zapomnienia nie ma zastosowania, gdy przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa krajowego oraz z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego (art. 17 ust. 3 lit. b i c RODO). We wspomnianym dokumencie Polityka prywatności wskazano: Każdej osobie, której dane są przetwarzane, przysługuje prawo do usunięcia danych (prawo do zapomnienia), o ile żądanie to nie dotyczy usunięcia danych medycznych, których przetwarzanie jest określone w odrębnych przepisach. Dla danych medycznych nie stosuje się prawa do zapomnienia. W myśl standardów europejskich dane medyczne to szczególny typ danych osobowych, które dotyczą zdrowia. Informacje zgromadzone w ramach Platformy P1 są bezpieczne, a ich wykorzystanie przez administratora danych oparte jest o zasady przetwarzania danych osobowych wynikających z RODO oraz innych przepisów prawa krajowego. Mając na uwadze te przepisy, brak jest możliwości trwałej likwidacji danych na Platformie P1, w tym w Internetowym Koncie Pacjenta. Dane te nie są przetwarzane wyłącznie w celu umożliwienia dostępu do nich pacjentowi, ale również innym podmiotom, w szczególności podmiotom wykonującym działalność leczniczą w związku z zapewnieniem ciągłości leczenia oraz Narodowemu Funduszowi Zdrowia.

Ad.3.

„Samodzielne zarządzanie danymi – zapewnienie pacjentowi narzędzi umożliwiających usuwanie lub ukrywanie danych w systemie P1 bez pośrednictwa personelu medycznego”.

Wprowadzenie funkcjonalności tj. samodzielne zarządzanie danymi wymagałoby decyzji kierunkowych, zmian technicznych oraz przepisów prawa. Niemniej z uwagi na założenia systemu P1 i szerszej systemu informacji w ochronie zdrowia, którego elementy określa ustawa o SIOZ, spełnienie takiego postulatu prawdopodobnie mogłoby prowadzić do wypaczenia istoty jego funkcjonowania i w ogóle istnienia Systemu Informacji Medycznej (SIM), który jest systemem teleinformatycznym służącym przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców.

Ad.4.

„Odpowiedzialność placówek – wprowadzenie skutecznych sankcji wobec podmiotów medycznych naruszających zasady przetwarzania danych.”

Postulat wprowadzenia dodatkowych sankcji wobec podmiotów medycznych wykracza poza kompetencje Ministra Zdrowia. Wprowadzenie dodatkowych sankcji wobec podmiotów wykonujących działalność leczniczą i występujących w roli administratorów w rozumieniu art. 4 pkt 7 RODO wymagałoby zmiany przepisów o ochronie danych osobowych. Właściwym w tym zakresie jest Minister Cyfryzacji, bowiem w strukturach Ministerstwa Cyfryzacji funkcjonuje Departament Zarządzania Danymi, do którego zadań należy m.in. kształtowanie polityki państwa w zakresie zarządzania danymi i ochrony danych osobowych oraz tworzenie otoczenia regulacyjnego w tym obszarze. Ponadto, należy podkreślić, że w obecnym porządku prawnym to Prezes Urzędu Ochrony Danych Osobowych posiada instrumenty nadzorcze i sankcyjne wobec administratorów nieprzestrzegających przepisów o ochronie danych osobowych. Zgodnie z przepisami RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Prezes Urzędu Ochrony Danych Osobowych posiada m.in. prawo do prowadzenia postępowań w sprawie naruszenia przepisów o ochronie danych osobowych oraz nakładania decyzją administracyjną administracyjnych kar pieniężnych, a także prowadzenia planowych lub doraźnych kontroli przestrzegania przepisów o ochronie danych osobowych. Przepisy te przewidują trzy rodzaje odpowiedzialności administratorów za uchybienia przepisom o ochronie danych osobowych, tj. odpowiedzialność administracyjną, cywilną oraz karną.

Podsumowując, obecne rozwiązania:

- są zgodne z przepisami krajowymi i unijnymi (w tym RODO),
- zapewniają bezpieczeństwo danych,
- służą poprawie jakości i dostępności świadczeń zdrowotnych.

W związku z powyższymi postulatami zawarte w petycji nie mogą zostać uwzględnione w obecnym stanie prawnym.

Z wyrazami szacunku

