pacjent.gov.pl

Nie przekazuj AI swoich danych

Czy zdarzyło Ci się szukać diagnozy w internecie? Wrzucasz swoje wyniki badań w narzędzia sztucznej inteligencji? Dowiedz się, jakie mogą być skutki

W internecie pojawia się coraz więcej narzędzi opartych na sztucznej inteligencji. Mogą one odpowiadać na pytania, przeszukiwać sieć, a nawet analizować przesłane dokumenty.

Kiedy dostajesz wyniki badań, możesz chcieć skorzystać z podpowiedzi AI lub z wyszukiwarki internetowej. Jednak zaufanie poradom sztucznej inteligencji nie jest pozbawione ryzyka. Narzędzia te nie mogą zastąpić pracowników medycznych. Nie muszą też przestrzegać tajemnicy lekarskiej, nie obowiązuje ich RODO ani żadne zasady etyki zawodowej.

Uważaj, co udostępniasz w sieci

Wszystko, co raz trafi do internetu, może w nim pozostać już na zawsze. Ta sama zasada dotyczy narzędzi sztucznej inteligencji. To, co do nich wpisujesz, może zostać zapisane, powielone lub wykorzystane do ich uczenia się.

Trenowanie sztucznej inteligencji polega na uczeniu się na przykładach. Systemy AI analizują ogromne ilości danych, aby lepiej rozumieć pytania i poprawnie na nie odpowiadać. Dlatego nie wysyłaj tam danych osobowych, poufnych informacji ani szczegółów, których nie przekazałbyś/abyś obcej osobie. Nie przesyłaj dokumentów, które zawierają nie tylko wyniki badań, ale także Twoje dane wrażliwe takie jak np. PESEL.

Ochrona danych zdrowotnych zaczyna się od ostrożności: nie przekazuj ich, jeśli nie masz pełnej kontroli nad tym, co później stanie się z informacjami o Twoim zdrowiu.

Chroń informacje o sobie

Dane zdrowotne należą do najbardziej wrażliwych informacji o Tobie. Zawierają historię leczenia, informacje o chorobach, przyjmowanych lekach i badaniach. W niepowołanych rękach mogą zostać nieuczciwie wykorzystane do wyłudzeń, szantażu, kradzieży tożsamości czy wyłudzenia recept.

Nigdy nie przekazuj:

- wyników badań, opisów wizyt i kart informacyjnych zawierających dane osobowe
- numeru PESEL, numeru dowodu czy danych kontaktowych
- zdjęć dokumentacji medycznej zawierających dane osobowe
- loginów i haseł do portali medycznych, a także profilu zaufanego
- informacji o stanie zdrowia swoim lub bliskich wraz z danymi osobowymi.

Nie rób tego, jeśli nie chcesz:

- przeczytać gdzieś na publicznym portalu o swoich chorobach
- udostępnić swoją diagnozę medyczną osobom, które wykorzystają to przeciwko Tobie
- otrzymywać fałszywych i niepokojących informacji o stanie swojego zdrowia, na podstawie których podejmiesz złe decyzje
- dostawać oferty magicznych leków
- paść ofiarą wyłudzenia, bo ktoś poznał Twoje słabości.

Nie możesz procesować się z AI o naruszenie tajemnicy lekarskiej ani w sprawie błędnej diagnozy. **Narzędzia AI nie są osobami ani nie mają osobowości prawnej.** Jednym słowem – są bezkarne, cokolwiek zrobią z Twoimi danymi.

W regulaminach narzędzi sztucznej inteligencji jest często informacja, by porad sztucznej inteligencji nie traktować jak diagnoz lekarskich. To zabezpieczenie właściciela narzędzia przed odpowiedzialnością karną.

> **Sztuczna inteligencja jest narzędziem, z którego lepiej korzystać rozważnie.**

Ludzie mają skłonność uczłowieczania różnych elementów otaczającego ich świata. Nic dziwnego, że dzieje się to w przypadku narzędziAI, które są do tego stworzone, by udawać ludzi.

Tymczasem AI:

- nie odróżnia dobrych i złych źródeł wiedzy
- korzysta z ograniczonych źródeł informacji, ale mogą to być także opinie czy oceny nieakceptowane przez medycynę
- jeśli nie znajduje odpowiedzi, może zacząć halucynować, czyli wymyślać coś, co jest niezgodne z prawdą

- może sprawiać wrażenie, że jest empatyczna, wspierająca Cię w decyzjach, ale jej algorytmom chodzi tylko o to, żeby jak najdłużej utrzymać Twoją uwagę.

Może to spowodować, że podejmiesz złe decyzje w sprawie swojego zdrowia.

Jak zadbać o bezpieczeństwo swoich danych

- Swoje dane udostępniaj tylko w oficjalnych narzędziach systemu ochrony zdrowia, takich jak mojeIKP czy Internetowe Konto Pacjenta.
- Nie przesyłaj do narzędzi AI żadnych dokumentów zawierających dane osobowe – jeżeli chcesz skorzystać z tego narzędzia, udostępniaj tylko te treści, które ich nie zawierają.
- Jeżeli możesz, wyłącz (domyślnie włączone) w używanych przez Ciebie narzędziach AI udostępnianie danych do trenowania modeli.
- Jeśli masz wątpliwości co do bezpieczeństwa aplikacji, nie używaj jej w ogóle.

Gdzie zgłaszać podejrzane sytuacje

Jeśli podejrzewasz, że mogło dojść do naruszenia danych lub widzisz próbę wyłudzenia informacji, zgłoś to do **CERT Polska**

Jeśli chcesz lepiej chronić swoje dane zdrowotne, skorzystaj z bezpłatnej publikacji **„Podstawy bezpieczeństwa i ochrony danych w sektorze ochrony zdrowia”**. To praktyczny przewodnik przygotowany przez CSIRT CeZ z myślą o osobach korzystających z systemów ochrony zdrowia. W prosty sposób wyjaśnia, jak rozpoznawać próby oszustw w internecie, jak bezpiecznie korzystać z aplikacji i usług medycznych oraz jak chronić swoje dane przed phishingiem, kradzieżą tożsamości czy innymi cyberatakami.

Z AI warto korzystać świadomie i ostrożnie, tak samo jak z innych usług w internecie.

Przeczytaj też: Twoje bezpieczne IKP

O czym warto pamiętać, korzystając z Internetowego Konta Pacjenta lub aplikacji mojeIKP? Co robić, gdy na swoim koncie znajdujesz błędne dane lub cudze informacje?