Sztuczna inteligencja a dane medyczne (bezpieczeństwo danych) - część I

Badania kliniczne opierają się na coraz bardziej zaawansowanych systemach informatycznych, które umożliwiają gromadzenie i analizowanie dużych ilości danych. Wykorzystanie technologii cyfrowych nie tylko zwiększa efektywność badań, ale także umożliwia dokładniejsze podejmowanie decyzji medycznych oraz szybszy rozwój nowych terapii. Aby dane te mogły być wykorzystywane w sposób bezpieczny i zgodny z wymaganiami prawnymi, konieczne jest wdrożenie odpowiednich rozwiązań zapewniających ich ochronę.

Sztuczna inteligencja (ang. Artificial Intelligence – AI) zyskuje na znaczeniu jako kluczowe narzędzie wspierające zarządzanie bezpieczeństwem danych w badaniach klinicznych. Dzięki wykorzystaniu algorytmów uczenia maszynowego czy automatycznych mechanizmów reagowania na potencjalne zagrożenia, AI umożliwia nie tylko monitorowanie danych w czasie rzeczywistym, ale także przewidywanie ryzyka i podejmowanie działań zapobiegawczych. AI zapewnia integralność danych, minimalizując ryzyko błędów i niezgodności, a także wspomaga zgodność z regulacjami, takimi jak na przykład RODO.

W Polsce większość placówek posiada system IT, który pozwala na gromadzenie i przetwarzanie danych w postaci elektronicznej. Oprócz danych administracyjnych, dane z badań klinicznych przechowywane są w różnych systemach, zarówno krajowych, jak i międzynarodowych, które spełniają odpowiednie standardy ochrony danych (RODO). Są to między innymi lokalne systemy przechowywania w ośrodkach badawczych, systemy elektronicznej dokumentacji medycznej, usługi chmurowe czy inne specjalistyczne systemy zarządzania danymi z badań klinicznych.

Czy dane z badań klinicznych są bezpieczne?

W systemie ochrony zdrowia szczególne znaczenie ma zapewnienie bezpieczeństwa systemów, szczególnie w placówkach medycznych, które przetwarzają wrażliwe dane pacjentów. Postęp cyfryzacji w polskim systemie ochrony zdrowia, mimo licznych korzyści, wymaga wdrożenia skutecznych rozwiązań zapewniających bezpieczeństwo przed cyberatakami. Dzięki zaawansowanym technologiom i współpracy z ekspertami, możliwe jest bezpieczne przechowywanie danych medycznych. Aby dane medyczne nie były wykorzystywane w niepożądany sposób, istotne jest, aby zapewnić placówkom odpowiednie zabezpieczenia techniczne i organizacyjne, a także przygotować je do ewentualnych incydentów związanych z bezpieczeństwem danych.

W Polsce obowiązują przepisy, które nakładają na placówki medyczne obowiązki dotyczące cyberbezpieczeństwa. Najważniejsze z nich to Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która wprowadza m.in. obowiązki dotyczące wdrożenia systemu zarządzania bezpieczeństwem informacji i odpowiedniego zabezpieczenia infrastruktury teleinformatycznej.

Zgodnie z Ustawą, placówki medyczne są traktowane jako tzw. "operatorzy usług kluczowych", co oznacza, że muszą podjąć szczególne działania w zakresie zapewnienia bezpieczeństwa danych i systemów. W praktyce oznacza to konieczność wdrożenia działań, takich jak prowadzenie systematycznej oceny ryzyka, zapewnienie ochrony przed nieautoryzowanym dostępem do systemów informacyjnych, bieżące aktualizowanie oprogramowania, a także tworzenie kopii zapasowych danych.

W przypadku wystąpienia cyberataku, placówka medyczna powinna niezwłocznie podjąć działania w celu minimalizacji szkód, w tym zgłoszenie incydentu do odpowiednich służb, takich jak CERT[1], a także podjęcie działań naprawczych. Dodatkowo, w przypadku naruszenia ochrony danych osobowych, należy zgłosić to do organu nadzorczego – Prezesa Urzędu Ochrony Danych Osobowych.

Dane z badań klinicznych są bezpieczne, o ile są odpowiednio przechowywane i zabezpieczone. Konsekwencje cyberataków mogą być poważne, w związku z czym ośrodki powinny podejmować kompleksowe działania w celu ochrony danych i systemów informacyjnych.

Bibliografia:

- AI in Protecting Clinical Trial Data from Cyber Threats. (2024). International Journal of Advanced Engineering Technologies and Innovations, 1(2), 567-592.
- https://www.thoughtful.ai/blog/safeguarding-patient-data-ais-role-in-healthcare-cybersecurity
- https://www.termedia.pl/mz/Cyberbezpieczenstwo-placowek-medycznych-aspekty-prawne,50463.html
- https://www.rynekzdrowia.pl/E-zdrowie/Samorzad-lekarski-zaprezentowal-raport-o-danych-medycznych-w-pracy-lekarza,255096,7.html

Autorka: Martyna Słowik

---

[1] CERT Polska to zespół reagowania na incydenty, jeden z trzech CSIRT-ów (z ang. Computer Security Incident Response Team) poziomu krajowego, odpowiedzialny m.in. za ochronę polskiej cyberprzestrzeni przed zagrożeniami i udział w międzynarodowych projektach naukowo-badawczych.

Poprzedni Strona