11 000 stron: Opublikowano nowe tajne dokumenty firmy Pfizer

Nowa partia działań prawnych ze strony firmy Pfizer w sprawie szczepionki Comirnaty mRNA została opublikowana 1 kwietnia. W rzeczywistości dokumenty powinny zniknąć z oczu opinii publicznej na 77 lat.

Żaden żart primaaprilisowy: kolejna partia tych dokumentów firmy Pfizer, które powinny pozostać tajne przez ponad 70 lat, została opublikowana 1 kwietnia. Istnieją inne 11043 strony, które zostały pozwane z amerykańskiej FDA. W nowej partii dokumentów znajduje się również niezredagowana wersja raportu popremierowego.

Pfizer potrzebował więcej personelu
Podobnie jak w przypadku pierwszej, jeszcze obszerniejszej partii dokumentów, również ocena nowych dokumentów zajmie dużo czasu i wysiłku. Ale są już pierwsze przebłyski.

Na przykład firma musiała zatrudnić dodatkowy personel, ponieważ najwyraźniej nie była przygotowana na dużą liczbę zgłaszanych spontanicznych i niepożądanych zdarzeń.

- Among adverse event reports received into the Pfizer safety database during the cumulative period, only those having a complete workflow cycle in the safety database (meaning they progressed to Distribution or Closed workflow status) are included in the monthly SMSR. This approach prevents the inclusion of cases that are not fully processed hence not accurately reflecting final information. Due to the large numbers of spontaneous adverse event reports received for the product, the MAH has prioritised the processing of serious cases, in order to meet expedited regulatory reporting timelines and ensure these reports are available for signal detection and evaluation activity. The increased volume of reports has not impacted case processing for serious reports, and compliance metrics continue to be monitored weekly with prompt action taken as needed to maintain compliance with expedited reporting obligations. Non-serious cases are entered into the safety database no later than 4 calendar days from receipt. Entrance into the database includes the coding of all adverse events; this allow for a manual review of events being received but may not include immediate case processing to completion. Non-serious cases are processed as soon as possible and no later than 90 days from receipt. Pfizer has also taken a multiple actions to help alleviate the large increase of adverse event reports. This includes significant technology enhancements, and process and workflow solutions, as well as increasing the number of data entry and case processing colleagues. To date, Pfizer has onboarded approximately 600 additional full-time employees (FTEs). More are joining each month with an expected total of more than 1,800 additional resources by the end of June 2021.

Można to znaleźć w nieprzeredagowanym raporcie popremierowym. Dokument ma 38 stron i jest z pewnością bardzo wybuchowy. A także pokazuje, ile luk miała terapia mRNA po rozpoczęciu kampanii szczepień. Brakuje informacji nie tylko o „skuteczności szczepień”, ale także o „stosowaniu w czasie ciąży i karmienia piersią”. Anafilaksja, reakcja alergiczna, została już przynajmniej zidentyfikowana jako „ważne ryzyko”.

3.1.2. Summary of Safety Concerns in the US Pharmacovigilance Plan

Table 3. Safety concerns

Important identified risks	Anaphylaxis
Important potential risks	Vaccine-Associated Enhanced Disease (VAED), Including Vaccine-associated Enhanced Respiratory Disease (VAERD)
Missing information	Use in Pregnancy and lactation Use in Paediatric Individuals <12 Years of Age Vaccine Effectiveness

38-stronicowy raport:

reissue_5.3.6-postmarketing-experiencePobierz

Pojawiły się więc obawy dotyczące bezpieczeństwa „zaostrzonych chorób związanych ze szczepionką, w tym chorób układu

oddechowego związanych ze szczepionką.” Może to wskazywać na większą podatność na inne patogeny. Osłabienie układu odpornościowego w wyniku szczepienia, przed którym ostrzegało wiele osób.

Zwycięstwo w sądzie

Dokumenty musiały zostać ujawnione po tym, jak FDA przegrała w sądzie okręgowym w Teksasie. Organizacja non-profit, która wygrała proces, podszywając się pod pracowników służby zdrowia i medycyny na rzecz przejrzystości, natychmiast opublikowała dokumenty firmy Pfizer na swojej stronie internetowej. Jednak nie ma informacji ani wyjaśnień na temat tego, co pokazują (jeszcze). Rzecznik organizacji powiedział: *„Naszym zadaniem było pozyskanie dokumentów. Analizę pozostawiamy naukowcom i innym.”*

Być może nie była to ostatnia partia dokumentów, które miały być ukrywane przez 77 lat.

Nowo opublikowane dokumenty można znaleźć tutaj.

Źródło: Lega Artis

Indyjska aplikacja do śledzeniea COVID ujawnia lokalizację obozów wojskowych

Ekspert GIS ostrzegł, że indyjska aplikacja do śledzenia COVID, Aarogya Setu, może udostępniać lokalizacje obozów wojskowych i może być wykorzystywana przez wrogów do inwigilacji i do śledzenia ruchów żołnierzy we wrażliwych obszarach, takich jak Pangong Tso w Ladakh.

Aarogya Setu ujawnia lokalizację obozów wojskowych

Wrażliwe informacje o rozmieszczeniu żołnierzy i ich ruchu w bazach wojskowych lub placówkach szpiegowskich wzdłuż granicy z Chinami mogły zostać naruszone przez aplikację mobilną Aarogya Setu do śledzenia COVID-19 w Indiach.

Aarogya Setu został zaprojektowany przez rząd w celu gromadzenia danych o lokalizacji i odniesienia ich do bazy danych testów COVID-19 należącej do Indian Council of Medical Research, aby ostrzec użytkownika, jeśli w pobliżu znajduje się zarażona osoba.

„Dzięki aplikacji można sprawdzić, czy żołnierz używający Arogya Setu znajduje się w konkretnym obozie, czy też wyjeżdża do innego obozu, czy jest przenoszony, czy coś w tym rodzaju. Przez stały pomiaru, można zobaczyć, jak wiele osób zostało przeniesionych z obozu i ile osób zjnaduje się w obozie w danej chwili" Raj Bhagat Palanichamy, niezależny system informacji geograficznej (GIS) – napisał Sputnik.

Ostrzegając władze, Raj podzielił się przykładem wykorzystania Arogya Setu do z grubsza wykrywania liczby osób korzystających z aplikacji (co może być zbieżne z liczbą żołnierzy) we wrażliwych obszarach, takich jak Pangong Tso, gdzie wojska Indii i Chin były zaangażowane w ostry konflikt od kwietnia

tego roku.

„Dzięki fałszywej aplikacji GPS możesz przenieść swoją lokalizację w dowolne miejsce. Możesz po prostu wpisać cokolwiek do Wagah Border, Pangong Tso, Galwan Valley. To nic wielkiego. A potem możesz po prostu otworzyć aplikację Arogya Setu, która pokaże, ilu zwykłych ludzi (dotkniętych COVID) jest tam itp.”- powiedział Raj, dodając, *„że chińscy agenci mogą nie uzyskać dokładnej liczby żołnierzy w określonej lokalizacji, ale „Będą wiedzieć, czy ludzie się poruszają i czy idą w jakim kierunku, w jakim czasie itp.”*

„Jeśli mówisz o miejscu, w którym znajduje się tylko baza wojskowa, nie jest wymagana żadna wiedza techniczna ani hakowanie. Ale jeśli chcesz dowiedzieć się czegoś o konkretnym budynku itp., trzeba trochę pokombinować ”- powiedział Raj Bhagat Sputnikowi.

Armia indyjska, wydając poradnik w kwietniu tego roku, poprosiła żołnierzy o zainstalowanie aplikacji Arogya Setu i włączenie usług lokalizacyjnych i bluetooth podczas odwiedzania miejsc publicznych, w ośrodkach izolacyjnych, powołując się na pomoc władzom cywilnym w związku z COVID-19 podczas podczas opuszczania kwater lub stacji wojskowych. W kwietniu personel armii został ostrzeżony, aby nie ujawniał swojej tożsamości służbowej, w tym rangi, stanowiska i listy kontaktów użytkowników podczas korzystania z takich aplikacji.

Jaki pogląd na Aarogya Setu ma Armia Indyjska?

Według wyższego rangą oficera armii, aplikacja Aarogya Setu mogłaby służyć do śledzenia lokalizacji żołnierzy, a żołnierze rozmieszczeni na wysuniętych posterunkach w ogóle nie powinni używać telefonów komórkowych.

„Zadbaliśmy o to, aby żołnierze rozmieszczeni na wysuniętych posterunkach nie korzystali z telefonów komórkowych. Komunikują się za pośrednictwem wojskowych urządzeń komunikacyjnych. Tak więc ich ruch ani lokalizacja

nie zostaną ujawnione przeciwnikom za pośrednictwem aplikacji Aarogya Setu ”- powiedział w poniedziałek generał armii indyjskiej Sputnikowi.

Urzędnik armii indyjskiej przyznał jednak, że ruch z posterunków pokojowych i miejsc innych niż posterunki wysunięte może być śledzony. *„Nasze oddziały patrolujące wrażliwe obszary nie używają telefonów komórkowych”* – stwierdził urzędnik.

Przejęty kod źródłowy Aarogya Setu

12 sierpnia firma zajmująca się bezpieczeństwem cybernetycznym z siedzibą w Bombaju opublikowała szczegółowy blog wyjaśniający, w jaki sposób odkryła kod źródłowy całej platformy Aarogya Setu, w tym jej infrastruktury zaplecza udostępnionej publicznie w Internecie.

W blogu stwierdzono, że przy otwartych danych dostępowych firma była w stanie „pobrać kod źródłowy witryny internetowej Aarogya Setu, portalu Swaraksha, wewnętrznych interfejsów API, usług internetowych i wewnętrznej analizy”.

Sprawa została skierowana do Indian Computer Emergency Response Team, który po cichu załątałł lukę.

Następnie rząd zagroził Shadow Map podjęciem kroków prawnych w związku z blogiem opisującym zagrożenia bezpieczeństwa Aarogya Setu.

Chociaż dużo uwagi poświęcono Aarogya Setu, kilka rządów stanowych uruchomiło własne aplikacje COVID-19. Badanie bezpieczeństwa tych aplikacji przez Centrum Internet and Society (CIS) okazało się, że większość z tych aplikacji nie mają konkretnej polityki prywatności.

Źródło:

BlacklistedNews.com