Kara za brak wyobraźni. Dokumentacja medyczna w skradzionym aucie lekarza

Kategoria: Polityka Zdrowotna
Opublikowano: środa, 06, sierpień 2025 12:29
Alicja Cisowska

Analiza ryzyka dla ochrony danych przewożonych przez lekarza w dokumentacji pacjenta w czasie wizyt domowych pozwoliłaby ustrzec przed konsekwencjami kradzieży samochodu. Tymczasem niepubliczny ZOZ w Pyskowicach dopiero po takim zdarzeniu zidentyfikował zagrożenie i wyraźnie zakomunikował zakaz pozostawiania dokumentacji medycznej m.in. w prywatnym samochodzie.

Samochód lekarza, który pojechał z wizytą domową do pacjenta, został skradziony. W samochodzie była niezabezpieczona dokumentacja w sumie ośmiorga pacjentów, w tym nazwiska, imiona, daty urodzenia, adresy zamieszkania, numery PESEL, oraz dane dotyczące zdrowia.

Niepubliczny ZOZ, dla którego pracował lekarz, zgłosił ten fakt PUODO. Ten zbadał, jak wyglądały procedury ochrony danych w tym ZOZ. Okazało się, że analiza ryzyka dla danych była niekompletna, przez co nie wdrożono odpowiednich zabezpieczeń dla dokumentacji medycznej przy wizytach domowych. Za to – a nie za utratę danych – Prezes UODO Mirosław Wróblewski nałożył na ZOZ karę finansową w wysokości 32 tys. 832 zł.

ZOZ udzielał świadczeń zdrowotnych pacjentom także w formie wizyt domowych. Lekarze używali do tego swoich prywatnych samochodów, podpisując z ZOZ odpowiednie umowy. Administrator Bezpieczeństwa Informacji ZOZ już w 2017 r. zwrócił uwagę na problemy, jakie się z tym wiążą. Przewożenie niezabezpieczonej dokumentacji jest ryzykowne, bo można ją zgubić albo stracić w wyniku kradzieży. Administrator Bezpieczeństwa alarmował, że powinna być ona odwożona tego samego dnia do placówki, a nie zabierana przez lekarza „na noc”.

Te zalecenia w momencie kradzieży samochodu lekarza nie zamieniły się jednak w procedury ZOZ. Ten, jako administrator danych, nie identyfikował prywatnych aut pracowników jako obszaru przetwarzania danych osobowych, do których odnoszą się postanowienia procedur dotyczących zabezpieczania tych danych. Również same procedury w sposób bardzo ogólny odnosiły się do okoliczności przetwarzania danych poza siedzibą administratora. Nie odpowiadały na realne zagrożenia stwierdzone w audytach bezpieczeństwa. Zmiana nastąpiła dopiero po kradzieży – kiedy załącznik do polityki bezpieczeństwa dotyczący zabezpieczeń fizycznych został zaktualizowany poprzez konkretne wskazanie zasad obowiązujących w razie konieczności transportu dokumentacji medycznej poza siedzibą placówki medycznej. Dopiero wtedy pracownicy przeszli odpowiednie szkolenie, a lekarze jeżdżący do pacjentów dostali na dokumenty medyczne teczki zabezpieczone zamkiem szyfrowym.

Źródło: UODO