

Petycja

Wdrożenie państwowego mechanizmu autoryzacji dostępu do danych medycznych, zintegrowanego z Internetowym Kontem Pacjenta, aplikacją mojeIKP oraz aplikacją mObywatel.

Jeżeli lekarz, placówka, farmaceuta lub inny podmiot chciałby uzyskać dostęp do dokumentacji medycznej pacjenta poza zakresem wynikającym bezpośrednio z ustawy albo poza dokumentacją wytworzoną przez ten podmiot, pacjent otrzymywałby w aplikacji powiadomienie zawierające:

1. nazwę placówki;
2. imię, nazwisko i numer prawa wykonywania zawodu osoby występującej o dostęp;
3. zakres żądanych danych;
4. cel uzyskania dostępu;
5. okres, na jaki dostęp ma zostać udzielony;
6. informację, czy dane mogą zostać jedynie wyświetlone, czy również pobrane albo przekazane dalej.

Pacjent mógłby jednym działaniem:

1. wyrazić zgodę;
2. odmówić dostępu;
3. ograniczyć zakres danych;
4. skrócić czas udostępnienia;
5. udzielić zgody jednorazowej;
6. udzielić określonej placówce dostępu na czas leczenia;
7. później cofnąć udzielone uprawnienie.

Autoryzacja mogłaby odbywać się przez powiadomienie w mObywatelu, zeskanowanie kodu QR wyświetlonego przez lekarza albo inną bezpieczną metodę potwierdzenia tożsamości.

Trzy tryby dostępu

Wprowadzenie takiego systemu powinno zostać poprzedzone szczegółową analizą prawną określającą, które podmioty i w jakich sytuacjach mogą uzyskiwać dostęp bez dodatkowej zgody pacjenta, a kiedy dostęp powinien wymagać jego świadomego działania.

Proponuję rozważenie trzech podstawowych trybów:

1. Dostęp wynikający bezpośrednio z przepisów

Bez dodatkowej zgody pacjenta dostęp powinien przysługiwać wyłącznie w zakresie rzeczywiście koniecznym, w szczególności:

- placówce i osobie wykonującej zawód medyczny w odniesieniu do dokumentacji wytworzonej podczas udzielania świadczeń;
- wybranemu przez pacjenta lekarzowi, pielęgniarce i położnej podstawowej opieki zdrowotnej – w zakresie wynikającym z ustawy;
- podmiotom publicznym wykonującym ustawowe zadania, ale tylko w zakresie niezbędnym do konkretnego celu;
- osobom upoważnionym przez pacjenta do działania w jego imieniu;

- opiekunom ustawowym, z uwzględnieniem praw małoletniego pacjenta.

Każdy taki dostęp powinien pozostawiać trwały ślad w rejestrze widocznym dla pacjenta.

2. Dostęp wymagający zgody pacjenta

Zgoda pacjenta powinna być wymagana w szczególności, gdy:

- nowa placówka chce poznać dokumentację wytworzoną przez inne podmioty;
- lekarz specjalista chce uzyskać dostęp do pełnej historii leczenia, która nie jest niezbędna do aktualnej konsultacji;
- dostęp ma obejmować szczególnie szeroki zakres dokumentacji;
- dane mają zostać udostępnione integratorowi, zewnętrznemu dostawcy systemu lub innemu podmiotowi niewykonującemu bezpośrednio świadczenia zdrowotnego;
- dane mają zostać wykorzystane w celu innym niż bezpośrednie leczenie, o ile odrębne przepisy nie ustanawiają innej podstawy prawnej.

Zgoda powinna być szczegółowa, ograniczona czasowo i możliwa do łatwego wycofania.

3. Dostęp awaryjny

W przypadku bezpośredniego zagrożenia życia lub zdrowia dostęp powinien być możliwy bez oczekiwania na zgodę pacjenta. Nie może to jednak oznaczać dostępu anonimowego i niekontrolowanego.

Osoba korzystająca z trybu awaryjnego powinna:

- uwierzytelnić się za pomocą silnego mechanizmu;
- wskazać przyczynę użycia trybu awaryjnego;
- uzyskać dostęp tylko do danych potrzebnych w konkretnej sytuacji;
- podlegać późniejszej kontroli zasadności dostępu.

Pacjent albo jego przedstawiciel powinien otrzymać niezwłoczne powiadomienie, kto, kiedy, z jakiej placówki i z jakiego powodu użył trybu awaryjnego.

Rejestr dostępu dostępny dla pacjenta

Każdy pacjent powinien mieć w IKP i mObywatelu dostęp do czytelnego rejestru obejmującego:

- datę i godzinę dostępu;
- nazwę placówki;
- dane osoby korzystającej z dokumentacji;
- podstawę dostępu;
- zakres wyświetlonych danych;
- informację o pobraniu lub wyeksportowaniu dokumentów;
- informację o dalszym udostępnieniu danych;
- możliwość zgłoszenia dostępu, którego pacjent nie rozpoznaje.

Powiadomienia powinny być przekazywane natychmiast w przypadku:

- pierwszego dostępu nowej placówki;
- dostępu do pełnej historii leczenia;
- skorzystania z trybu awaryjnego;
- pobrania większej liczby dokumentów;
- próby masowego eksportu danych;
- dostępu nietypowego ze względu na miejsce, czas albo zakres.

Pacjent powinien móc ustawić, czy chce otrzymywać powiadomienie o każdym dostępie, czy tylko o operacjach podwyższonego ryzyka.

Ograniczenie technicznych możliwości masowego wycieku

Sama autoryzacja pacjenta nie wystarczy, jeżeli dostawcy oprogramowania nadal będą mogli przechowywać i eksportować kompletne kopie dokumentacji milionów osób.

Dlatego wnoszę o rozważenie w szczególności:

1. odejścia od przekazywania dostawcom systemów lokalnych pełnych, zbiorczych kopii dokumentacji, jeżeli nie jest to bezwzględnie konieczne;
2. udostępniania danych przez kontrolowane interfejsy, na podstawie krótkotrwałych i ograniczonych uprawnień;
3. oddzielenia kluczy szyfrujących od podmiotów przechowujących dane;
4. uniemożliwienia dostawcy oprogramowania samodzielnego odszyfrowania pełnych zbiorów danych;
5. stosowania segmentacji danych poszczególnych placówek i pacjentów;
6. blokowania masowych eksportów i automatycznego wykrywania nietypowych operacji;
7. obowiązkowego wieloskładnikowego uwierzytelniania pracowników medycznych i administratorów;
8. okresowej certyfikacji systemów przetwarzających elektroniczną dokumentację medyczną;
9. regularnych, niezależnych testów bezpieczeństwa i odporności na włamania;
10. ograniczenia uprawnień technicznych administratorów systemów zgodnie z zasadą minimalnych uprawnień;
11. prowadzenia nieusuwalnych dzienników dostępu podlegających niezależnej kontroli;
12. stosowania zasady, że dostęp do danych musi być ograniczony do konkretnego pacjenta, konkretnego celu i konkretnego czasu.

Celem powinno być stworzenie systemu, w którym przełamanie zabezpieczeń jednego podmiotu nie otwiera automatycznie dostępu do całej bazy danych, a każda próba uzyskania szerokiego dostępu jest blokowana albo wymaga dodatkowej, niezależnej autoryzacji.

Istniejące rozwiązania jako punkt wyjścia

Internetowe Konto Pacjenta i aplikacja mojeIKP pozwalają już pacjentowi udostępnić dane wybranemu lekarzowi, pielęgniarce, farmaceucie lub placówce oraz określić zakres i czas upoważnienia. Dziwić może jednak to, że w aplikacji nie mam upoważnionych ośrodków czy instytucji, a odnoszę wrażenie, że odwiedzani lekarze mają dostęp do tych danych. Być może widzą wyłącznie swoje dane, ale to nadal są moje dane.

Oznacza to, że część niezbędnej infrastruktury i mechanizmów prawnych już istnieje. Może jest w planach, testach, ale skoro widać w aplikacji, to oznacza, że projektanci tych aplikacji dostrzegając

problem pragną się z nim zmierzyć. Nie chodzi obecnie o roztrząsanie dlaczego mimo braku zgody z mojej strony dane te są widoczne. Ale jak widać proponowane rozwiązanie nie wymaga więc tworzenia całkowicie nowego systemu, lecz dopracowania obecnych i rozszerzenia istniejących funkcji o:

- aktywne występowanie o dostęp przez osobę lub placówkę;
- autoryzację za pośrednictwem mObywatela;
- natychmiastowe powiadomienia o wykorzystaniu danych;
- powszechny i czytelny rejestr dostępu;
- kontrolowany tryb awaryjny;
- techniczne ograniczenie możliwości kopiowania danych;
- jednolite stosowanie tych zasad przez wszystkie systemy gabinetowe i medyczne.

Należy również zapewnić rozwiązania dla osób, które nie korzystają ze smartfona, osób małoletnich, ubezwłasnowolnionych, czasowo niezdolnych do wyrażenia zgody oraz pozostających pod opieką innych osób.

Przy okazji zwrócę uwagę na powszechny w takich aplikacjach problem - drobnych liter w niemal wszystkich funkcjach aplikacji, których nie da się w ustawieniach aplikacji powiększyć. Można przypuszczać, iż większość korzystający to osoby w jakimś stopniu chore, często w wieku wymagającym wsparcia czy jakichś form dostosowania narzędzi do ich możliwości, a sama zmiana koloru tła raczej jest zbyt małą paletą ustawień systemu.

Wnioski

Zwracam się do Ministra Zdrowia o:

1. przeprowadzenie, we współpracy z Ministerstwem Cyfryzacji, Centrum e-Zdrowia, UODO, Rzecznikiem Praw Obywatelskich i Rzecznikiem Praw Pacjenta, analizy prawnej oraz technicznej proponowanego rozwiązania;
2. opracowanie katalogu podmiotów i sytuacji, w których dostęp do danych medycznych:
 - następuje z mocy prawa,
 - wymaga autoryzacji pacjenta,
 - może nastąpić w trybie awaryjnym;
3. przygotowanie projektu rozwiązań prawnych i technicznych;
4. przeprowadzenie pilotażu mechanizmu autoryzacji i powiadomień w ramach IKP, mojeIKP i mObywatela;
5. przedstawienie harmonogramu możliwego wdrożenia.

Zwracam się do Prezesa Urzędu Ochrony Danych Osobowych o:

1. ocenę przedstawionej koncepcji z punktu widzenia zasad ochrony danych w fazie projektowania i domyślnej ochrony danych;
2. ocenę, czy obecny model przetwarzania dokumentacji przez zewnętrznych dostawców systemów medycznych zapewnia wystarczające ograniczenie dostępu i możliwość rozliczenia wszystkich operacji;
3. przygotowanie rekomendacji dotyczących powiadamiania pacjentów o dostępie do ich danych;
4. rozważenie wydania wytycznych ograniczających możliwość tworzenia przez podmioty przetwarzające zbiorczych kopii dokumentacji wielu administratorów.

Zwracam się do Rzecznika Praw Obywatelskich o:

1. analizę problemu w świetle konstytucyjnego prawa do prywatności i autonomii informacyjnej;
2. podjęcie wystąpienia generalnego do właściwych ministrów;
3. monitorowanie prac zmierzających do zapewnienia pacjentom rzeczywistej kontroli nad wykorzystywaniem ich danych medycznych.

Proszę również o udzielenie informacji:

1. czy opisany mechanizm jest obecnie przedmiotem prac któregoś z organów państwa;
2. czy planowane jest wprowadzenie powiadomień o dostępie do dokumentacji medycznej;
3. czy pacjent będzie mógł sprawdzić pełną historię dostępu do swoich danych;
4. jakie rozwiązania mają zapobiec możliwości przejęcia zbiorczych danych milionów pacjentów wskutek naruszenia zabezpieczeń pojedynczego dostawcy;
5. czy planowana jest obowiązkowa certyfikacja systemów przetwarzających elektroniczną dokumentację medyczną;
6. w jakim terminie możliwe byłoby uruchomienie pilotażu przedstawionego rozwiązania.

Incydent dotyczący MyDr powinien stać się impulsem do zmiany sposobu myślenia o bezpieczeństwie dokumentacji medycznej. Nie wystarczy nakładać obowiązki na podmioty przechowujące dane i reagować dopiero po wycieku. System powinien być skonstruowany w taki sposób, aby masowe przejęcie dokumentacji było technicznie niemożliwe albo wymagało przełamania wielu niezależnych zabezpieczeń, zostało natychmiast wykryte i nie mogło nastąpić bez pozostawienia jednoznacznego śladu.

Pacjent powinien wiedzieć, kto korzysta z jego danych, w jakim celu i w jakim zakresie. Tam, gdzie dostęp nie wynika bezpośrednio z przepisów ani z nagłego zagrożenia życia lub zdrowia, pacjent powinien móc świadomie o nim zdecydować.