

Centralny portal informacyjny ochrony zdrowia

Szansa dla systemu

Dominik Meller



rys. Olga Reszeliska Zx

W marcu 2009 r. Ministerstwo Zdrowia opublikowało „Strategię e-Zdrowie Polska na lata 2009–2015” (<http://csioz.gov.pl/ezdrowie.html>). Jednym z jej głównych celów jest „unowocześnienie systemu informacji medycznej w celu analizy zapotrzebowania na świadczenia zdrowotne”. Oczywiście, poza celami głównymi centralny portal informacyjny (CPI) mógłby pełnić dodatkowe funkcje, np. ułatwiać dostęp do informacji na temat pozamedycznych kosztów choroby.

Skuteczność zarządzania zarówno w skali mikro, jak i makro zależy od dostępu do danych. Dlatego istnienie luki informacyjnej jest tak bardzo niepożądane w systemach zarządzania. Centralny portal informacyjny to odpowiedź na ten problem. Na razie istnieją jedynie koncepcje realizacji technicznej portalu. Dyskusja dotyczy zarówno rozproszenia punktów przechowywania danych, jak i dostępu do zgromadzonych informacji. Abstrahując od rozważań *stricte* technologicznych, w artykule poruszone zostaną kwestie dotyczące użyteczności systemu dla pacjentów i personelu medycznego, a także niebezpieczeństw, jakie może spowodować zastosowanie nieodpowiedniej technologii tworzenia i obsługi CPI. Potencjalne zagrożenia nie

powinny jednak zablokować powstania, a następnie sprawnego funkcjonowania portalu.

Integralna część systemu służby zdrowia

Koncepcja ogólnokrajowego systemu zbierającego i przechowującego informacje o wszystkich obywatelach objętych ubezpieczeniem zdrowotnym doczekała się już pierwszych realizacji. Największe szanse powodzenia ma w krajach rozwiniętych, dlatego pierwsze projekty zrealizowano w Stanach Zjednoczonych. Ich wykonania podjęli się potentaci rynku IT – Google i Microsoft – tworząc konkurencyjne rozwiązania – Google Health, a Microsoft Health Vault. Są one jednak tylko dodatkową warstwą istniejących systemów służby zdrowia. Zgodnie z koncepcją UM II (http://www.nfz-warszawa.pl/download/swiadcze/Koncepcja_systemu_RUMII.pdf), CPI, który będzie działał w Polsce, ma być integralną częścią ogólnokrajowego systemu służby zdrowia.

Podstawową funkcją CPI będzie przechowywanie i zarządzanie informacjami medycznymi o korzystających z usług ochrony zdrowia. Dzięki zastosowaniu elektronicznych kart ubezpieczenia zdrowotnego stanie się możliwa identyfikacja wszystkich kontaktów medycznych i ich powiązanie z konkretnymi osobami. Umożliwi to stworzenie dokładnej historii chorób każdego pacjenta. Dostęp do pełnej informacji medycznej znacznie przyspieszy diagnozowanie i pozwoli obniżyć koszty powstałe wskutek wielokrotnego zlecenia tych samych badań w różnych placówkach.

Dane medyczne przechowywane centralnie zwiększają ponadto mobilność pacjentów. Po wprowadzeniu CPI nie będzie trzeba przenosić papierowych kartotek medycznych. Transfer chorego pomiędzy placówkami stanie się operacją czysto logistyczną.

Kolejną zaletą CPI będzie automatyczne tworzenie druków, co skróci czas obsługi pacjenta w przychodniach. Bardzo często lekarze muszą poświęcać znacznie więcej czasu na przygotowywanie dokumentacji niż na pracę medyczną. Portal umożliwi zmianę tych proporcji. Wszelka dokumentacja będzie wypełniana automatycznie przez system, a następnie drukowana na miejscu. Metoda ta wyeliminuje problem błędów przy wypełnianiu druków wymaganych przez instytucje zewnętrzne, takie jak pracodawcy lub ZUS.

System umożliwi podgląd historii leków zapisywanych chorym oraz statusu wystawianych recept. Dzięki integracji z systemem aptecznym każdy lekarz będzie mógł obserwować, czy pacjent wykupuje leki. Będzie to możliwe między innymi dzięki zastosowaniu technologii elektronicznych kart pacjenta.

Pomoc w profilaktyce

Portal stanie się ponadto nieocenionym źródłem informacji epidemiologicznych. Naukowcy, dzięki do-



„ Potencjalne zagrożenia nie powinny zablokować powstania, a następnie sprawnego funkcjonowania CPI „

stępowi do ciągle aktualizowanych danych o stanie zdrowia Polaków, znacznie wcześniej niż dotychczas będą mogli wykryć ogniska epidemii i podejmować działania mające na celu ochronę reszty społeczeństwa. Natomiast w ujęciu długofalowym CPI będzie mógł zostać wykorzystany jako baza do planowania działań profilaktycznych w całym kraju. Bez wątpienia dostęp danych z kilku lat umożliwi przygotowanie odpowiednich programów profilaktycznych, co pozwoli uwrażliwić osoby szczególnie zagrożone na najbardziej prawdopodobne schorzenia lub nawet wprowadzić określone regulacje prawne.

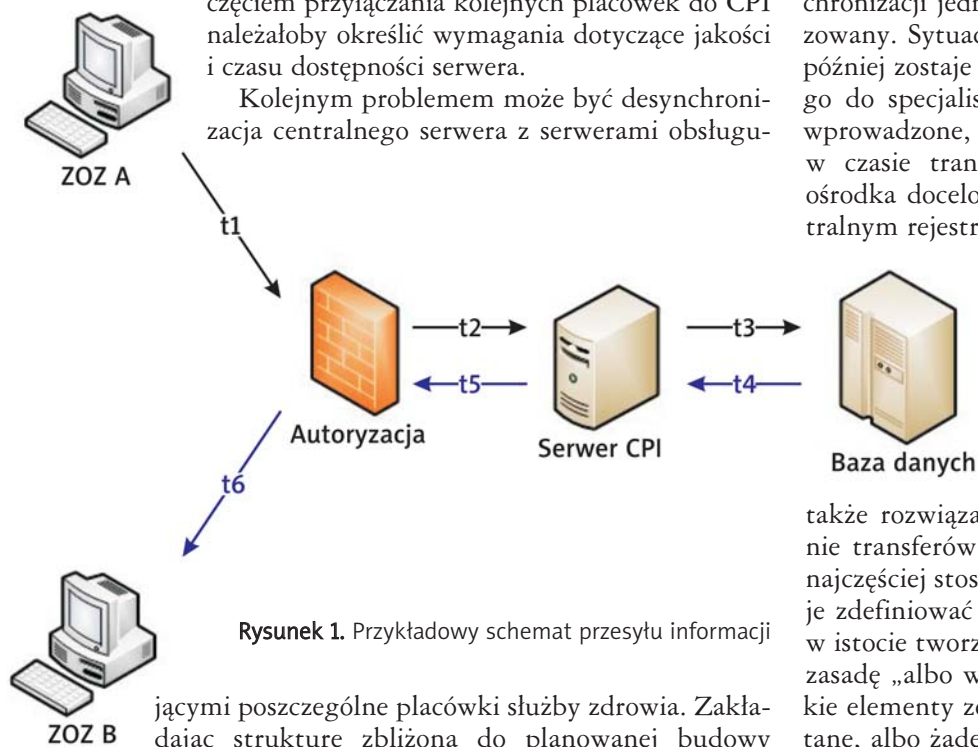
Najpoważniejsze zagrożenia

Mimo niewątpliwych zalet, wprowadzenie CPI może stanowić pewne zagrożenie związane zarówno z wykorzystaną technologią, jak i ze strukturą systemu. Projektując portal, należy wziąć pod uwagę wiele aspektów nie tylko funkcjonalnych, ale i *stricte* informatycznych. Dlatego przygotowywanie CPI musi się opierać na ścisłej współpracy zespołów techników, analityków i praktyków. Bez tej kooperacji portal nie spełni swego zadania.

Podstawową funkcją każdego systemu zbierającego i udostępniającego informacje w sieci jest transfer danych. Strategia „e-Zdrowie” zakłada, że każda placówka medyczna powinna zostać podłączona do internetu. Aby w pełni korzystać z CPI, niezbędna jest jednak odpowiednia przepustowość łącz internetowych. Niestety, nie każdy provider zapewnia wysoką jakość usług. Najważniejszym elementem jest „czas

dostępności”. Parametr ten określa, przez jaki czas – w porównaniu z całkowitym czasem świadczenia usługi – połączenie z Internetem jest sprawne, a transfer danych przebiega bez zakłóceń. Dlatego wraz z rozpoczęciem przyłączania kolejnych placówek do CPI należałoby określić wymagania dotyczące jakości i czasu dostępności serwera.

Kolejnym problemem może być desynchronizacja centralnego serwera z serwerami obsługi



Rysunek 1. Przykładowy schemat przesyłu informacji

jącymi poszczególne placówki służby zdrowia. Zakładając strukturę zbliżoną do planowanej budowy systemu Rejestru Zakładów Opieki Zdrowotnej (rys. 1), należy wziąć pod uwagę, iż zdarzenia medyczne mogą następować po sobie na tyle dynamicznie, że desynchronizacja może mieć bardzo poważne skutki.

Jak widać, synchronizacja lokalnego serwera z serwerami globalnymi odbywa się co określony interwał czasu. W dużych aglomeracjach, gdzie działa wiele specjalistycznych placówek, może się zdarzyć, że chory zostanie przeniesiony z jednego szpitala do drugiego. Nawet gdy założymy w pełni cyfrowy obieg dokumentów, a pacjent będzie miał kartę zawierającą dane o ostatnim kontakcie medycznym, może wystąpić luka informacyjna. Będzie ona na tyle szeroka, jak duża

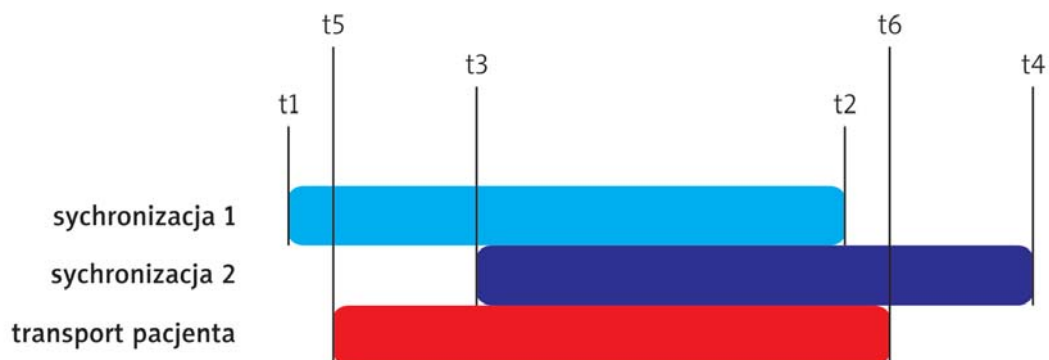
jest różnica pomiędzy momentami synchronizacji z serwerem głównym tych dwóch ośrodków. Problem synchronizacji przedstawia rysunek 2.

Na poniższym wykresie t1 jest momentem synchronizacji jednostki, w której pacjent jest hospitalizowany. Sytuacja jest klarowna. Jednak kilka minut później zostaje podjęta decyzja o przeniesieniu chorego do specjalistycznego ośrodka (t5). Dane zostają wprowadzone, a pacjent przetransportowany. Jednak w czasie transportu mija moment synchronizacji ośrodka docelowego (t3) oraz zapisu danych w centralnym rejestrze z ośrodka źródłowego (t2). Różnica

pomiędzy t6 a t4 wyznacza niebezpieczny przedział czasu, gdy w drugim ośrodku nie ma najnowszych informacji o przyjętym pacjencie.

Niepełne dane

Podczas budowania CPI należy także rozwiązać problem zakończonych niepomysłnie transferów danych. W praktyce informatycznej najczęściej stosuje się mechanizmy transakcji. Można je zdefiniować jako operacje na bazie danych, które w istocie tworzą integralną całość. Stosuje się w nich zasadę „albo wszystko, albo nic”, czyli albo wszystkie elementy zostaną poprawnie zapisane lub odczytane, albo żaden. Przykładem konieczności stosowania transakcji może być internetowa rejestracja pacjenta w ośrodku. Zanotowanie jedynie jego nazwiska, bez wpisania godziny spotkania, mogłoby poważnie zdezorganizować pracę ZOZ. Aby uchronić się przed takimi błędami, należy wprowadzić system monitoringu zapisu i odczytu danych. W wypadku częściowego niepowodzenia operacji wycofywałby on z systemu pozostałe wpisy należące do operacji i informował o tym zlecającego. Konsekwencje powodowane niesfinalizowanymi transakcjami warunkują zastosowanie mechanizmu transakcji lub jego pochodnej jako elementu zabezpieczającego spójność danych.



Rysunek 2. Interwał czasu potrzebny na uaktualnienie danych pacjenta w bazie

Dane „bliżej” odbiorców

Gdy zachowana zostanie spójność danych, należy przeanalizować niebezpieczeństwa wiążące się z ich fizycznym przechowywaniem. Serwery muszą być umieszczone w specjalnie do tego przygotowanych pomieszczeniach. Jednak korzystanie z jednej lub nawet kilku lokalizacji nie gwarantuje całkowitego bezpieczeństwa. Zależność bezpieczeństwa od liczby lokalizacji nie jest funkcją liniową i dlatego należałoby rozważyć alternatywne metody przechowywania danych. Obecnie coraz większe uznanie zyskuje idea *cloud computing* (udostępnianie użytkownikowi funkcjonalności oprogramowania, bez konieczności zajmowania się administracją i sprzętem). Wykorzystując fragment tej metody, można by zdecentralizować przechowywanie danych i odpowiednie informacje „przenieść” bliżej odbiorców, przyspieszając dostęp do nich, a jednocześnie zachowując wspólną platformę informacyjną. Rozproszenie w kraju serwerów przechowujących dane wymagać będzie przygotowania ujednoliconych wytycznych dotyczących bezpieczeństwa. Pociąga to za sobą kolejne koszty, zatem istotnym zagadnieniem stanie się znalezienie odpowiedniej równowagi pomiędzy bezpieczeństwem a rozproszeniem źródeł danych.

Przechowywanie danych nierozzerwalnie wiąże się z archiwizacją i przygotowywaniem kopii zapasowych. Dobrą praktyką jest wczesne wykrywanie nieprawidłowości powstałych podczas pracy systemu. Można do tego wykorzystać mechanizmy monitorujące rejestry zdarzeń zarówno oprogramowania CPI, jak i baz danych. Pozwoli to na szybkie wykrywanie usterek, wychwytnie nieprawidłowości we wczesnym etapie i podjęcie odpowiednich czynności naprawczych. Oczywiście, samo przechowywanie rejestrów wprowadza do systemu dodatkowy element wymagający ochrony, gdyż dostęp do tych informacji osób nieuprawnionych także może spowodować nieautoryzowany wyciek danych.

Równie ważny problem to ryzyko awarii dysków twardych. Prawdopodobieństwo takiego zdarzenia jest nikłe, ale może spowodować nieodwracalne szkody. Dlatego najważniejsze dane powinny być zapisywane równocześnie na dwóch nośnikach, by w momencie awarii jednego z nich można było automatycznie wykorzystać dysk zapasowy. Ze względu na kosztowność rozwiązania należałoby nadać odpowiednie priorytety danym i na tej podstawie podejmować decyzję o stosowaniu równoległego ich zapisu.

Bezpieczeństwo systemu

Ostatnim i zarazem największym niebezpieczeństwem jest ryzyko nieautoryzowanego dostępu do informacji medycznych. Niezbędne jest zatem wprowadzenie wielopoziomowych mechanizmów weryfikacji tożsamości użytkowników. Obecnie weryfikacja za pomocą podpisu na elektronicznej karcie pacjenta jest ekonomicznie

„ Podstawową funkcją CPI będzie przechowywanie i zarządzanie informacjami medycznymi o wszystkich korzystających z usług ochrony zdrowia ”

nieuzasadniona, co więcej, konieczność zakupu czytników kart skutecznie ograniczyłaby liczbę użytkowników CPI. Można by więc wykorzystać modele opracowane w bankowości elektronicznej. Są to rozwiązania przetestowane przez miliony klientów, a co za tym idzie, wszystkie niebezpieczeństwa z nimi związane są znane. Zatem głównym zadaniem związanym z edukacją użytkowników systemu w kwestiach bezpieczeństwa byłoby wyczulenie ich na ataki typu *phishing*, czyli wyludzanie poufnych informacji, jak identyfikatory logowania lub hasła. Nie jest to zjawisko nowe i wiele instytucji, których klienci są zagrożeni takimi atakami, prowadzi akcję edukacyjną, uwrażliwiając użytkowników na spreparowane strony podszywające się pod strony logowania lub wiadomości e-mail fałszywie polecające przesłanie wrażliwych danych w celu weryfikacji.

CPI warte ryzyka

Przedstawione w artykule korzyści przeważają nad zagrożeniami wynikającymi z wprowadzenia centralnego portalu informacyjnego. Wystarczy wziąć pod uwagę, że odpowiednie przygotowanie projektu

„ Przygotowywanie CPI musi się opierać na ścisłej współpracy zespołów techników, analityków i praktyków. Bez tej kooperacji portal nie spełni swego zadania ”

informatycznego w dużej mierze pozwoli wyeliminować większość zagrożeń. Oczywiście, musimy pamiętać, że wraz z rozwojem technologii informacyjnych pojawiają się kolejne niebezpieczeństwa, jednak podobnie jak radzą sobie z nimi kolejne generacje systemów bankowych, tak systemy służby zdrowia powinny ewoluować ku bezpieczeństwu, a przede wszystkim wydajności. ■