NOWOTWORY Journal of Oncology • 2006 • volume 56
Number 4 • 483–495

Medyczne systemy informatyczne – Bezpieczeństwo sieci komputerowych (aspekty organizacyjne i prawne) – cz. I

Piotr Kasztelowicz

Medical computer systems – Safety of computer networks (legal and organizational aspects) – part I

Co powinno być zrobione, lecz nie zostało

Wykorzystanie systemów informatycznych w medycynie ma szczególny charakter, ponieważ obejmuje ono ważną dziedzinę, jaką jest przekazywanie informacji dotyczącej stanu zdrowia, przebiegu choroby i sposobu leczenia. Dane te przechowywane są przez długi okres czasu zgodnie z wymogami prowadzenia dokumentacji medycznej. Dane te również powinny być przekazywane w momencie zmiany przez pacjenta placówki leczniczej. Jeśli zadajemy sobie pytanie, jakie są przyczyny złego funkcjonowania polskiego systemu zdrowotnego, to niewątpliwie jedną z nich jest brak wymiany informacji o pacjencie pomiędzy leczącymi go lekarzami. Wyobraźmy sobie pacjenta onkologicznego, który jest stopniowo diagnozowany przez lekarza rodzinnego, następnie trafia do placówki onkologicznej, gdzie jest poddawany różnym metodom leczenia. W międzyczasie – np. pomiędzy kolejnymi kursami chemioterapii jest leczony przez lekarza rodzinnego. Sprawa komplikuje się jeszcze bardziej, jeśli oprócz choroby onkologicznej pacjent jest leczony z powodu serca, cukrzycy czy innych schorzeń. W jaki sposób wówczas uzyskać informacje o stanie ogólnym pacjenta i stopniu zaawansowania np. choroby niedokrwiennej serca, co może istotnie wpłynąć na rokowanie i wybór leczenia onkologicznego? Odpowiedzią powinno być dążenie do poprawy wymiany informacji o pacjencie pomiędzy różnymi lekarzami. W dzisiejszych czasach taką możliwość daje jedynie komputerowa baza danych z możliwością przekazywania informacji za pośrednictwem sieci komputerowej. Dotykamy tutaj kluczowego problemu – konieczności stworzenia jednolitego formatu danych – czyli komputerowego rekordu pacjenta.

Nakreślmy więc zadania

Jeśli rozważamy zagadnienia bezpieczeństwa danych medycznych w systemach komputerowych to jednym z ważnych elementów może być właściwa organizacja tego przedsięwzięcia. Przy całościowym traktowaniu komputeryzacji jednostek opieki zdrowotnej zdrowia wyznaczenie strategicznych zadań na poszczególnych szczeblach nie jest trudne. Kluczowym zadaniem jest staranne przygotowanie i rozdzielenie zadań w projekcie komputeryzacji placówki leczniczej.

Ministerstwo Zdrowia i instytucje szczebla centralnego:
- stworzenie standardu elektronicznego rekordu pacjenta i elektronicznej historii choroby,
- ustalenie standardów i zakresu przesyłania danych do określonych placówek zajmujących się leczeniem oraz funduszy zdrowia lub kas chorych,
- wdrożenie elektronicznego podpisu i zasad bezpiecznego transferu,
- nadzór, aby systemy informatyczne wdrażane w poszczególnych placówkach ochrony zdrowia i funduszach zdrowotnych spełniały w/w standardy i pozwalały na wzajemną komunikację opartą o bezpieczne protokoły wymiany danych.

Samorząd wojewódzki:
- opracowanie i finansowanie regionalnych programów tworzenia infrastruktury informatycznej, najlepiej w formie konkursów projektów nadsyłanych przez określone publiczne i niepubliczne placówki służby zdrowia; projekty powinny uwzględniać przede wszystkim dwie grupy korzyści: pierwszą – korzyści, jakie mo-

W aktualnym zeszycie *Nowotworów* publikujemy pierwszą część artykułu dotyczącego bezpieczeństwa danych medycznych w sieciach komputerowych. Autor, dr Piotr Kasztelowicz, od kilkunastu lat zajmuje się tym zagadnieniem. Należy do grupy polskich lekarzy najbardziej zaangażowanych w tworzenie rodzimego Internetu medycznego.
Artykuł podzielono na dwie części: w pierwszej autor omawia aktualne wymogi prawne (wynikające z polskiego oraz europejskiego prawodawstwa) oraz elementarne zasady bezpiecznego użytkowania elektronicznej dokumentacji medycznej. W drugiej części, która ukaże się w kolejnym zeszycie *Nowotworów*, autor przedyskutuje mechanizmy zabezpieczające dane medyczne (tj. identyfikatory i hasła, podpis elektroniczny, ściany ogniowe), a także zagrożenia wynikające z istnienia wirusów komputerowych i sposoby ustrzeżenia się przed ich działaniem.

że odnieść pacjent z możliwości szybkiego przekazywania jego danych, tj. elektronicznej historii choroby wraz z cyfrowym zapisem jego badań i wyników pomiędzy leczącymi go na terenie danego województwa placówkami ochrony zdrowia; drugą – korzyści związane z usprawnieniem zarządzania, liczeniem kosztów i nadzorem przez kasę chorych lub fundusz ubezpieczeniowy, tj. korzyści wynikające z elektronicznego rozliczania się świadczeniodawcy z funduszem zdrowotnym.

Instytucje miejskie i gminne:
– integracja systemów placówek podstawowej opieki zdrowotnej z placówkami opieki stacjonarnej.

Przychodnia, szpital, praktyka lekarska:
– indywidualny, dostosowany do potrzeb i specyfiki danej placówki projekt uwzględniający wykonanie sieci, kupno sprzętu, oprogramowania, wybór sposobu zarządzania (zatrudnienie własnych informatyków lub zlecenie usług firmie zewnętrznej), szkolenie pracowników (projekt powinien oczywiście uwzględniać założenia i standardy określone dla globalnej infrastruktury zdrowia).

Chciałbym dodać, że na każdym z tych etapów podejmowane decyzje mogą w istotny sposób wpływać na bezpieczeństwo danych komputerowych.

Dokumentacja elektroniczna

Medyczna dokumentacja elektroniczna polega na zastąpieniu tradycyjnego sposobu gromadzenia wymaganych prawnie [Rozporządzenie Ministra Zdrowia z dnia 10 sierpnia 2001 r. w sprawie rodzajów dokumentacji medycznej w zakładach opieki zdrowotnej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania (Dz. U. Nr 88 poz. 966) oraz rozporządzenie Ministra Zdrowia z dnia 30 lipca 2001 r. w sprawie indywidualnej dokumentacji medycznej, sposobu jej prowadzenia oraz szczegółowych warunków jej udostępniania (Dz. U. Nr 83 poz. 903)] informacji o pacjencie specjalistycznymi bazami danych nazywanych elektronicznym rekordem pacjenta. Wymogi prowadzenia takiej dokumentacji obok wspomnianego Rozporządzenia Ministra Zdrowia określa Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne z 17 lutego 2005 (Dz.U. Nr 64 poz. 565). Pokrótce przepisy te wymagają utworzenie w danej placówce decydującej się na prowadzenie dokumentacji elektronicznej stworzenie planu informatyzacji, wyodrębnienia w danej instytucji zespołu osób odpowiedzialnych za administrowanie i nadzorowanie danych poufnych oraz określa, w jaki sposób będą tworzone minimalne normy bezpieczeństwa danych cyfrowych. Z tym zagadnieniem związana jest także Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883) nakładająca zgodnie z dyrektywą Unii Europejskiej obowiązek powołania administratora danych osobowych (http://pl.wikipedia.org/wiki/Administrator_danych_osobowych) oraz administratora bezpieczeństwa informacji, których obowiązkiem jest pełen nadzór nad zbieranymi w danej jednostce danymi osobowymi. W zakresie służbowym administrator danych osobowych podlega Generalnemu Inspektorowi Danych Osobowych. Jeśli rozpatrujemy tworzenie elektronicznego rekordu pacjenta w warunkach placówki medycznej istotnymi elementami wynikającymi z tych uregulowań prawnych są:
– stworzenie spójnego projektu komputeryzacji placówki medycznej opartego na sprawdzonym oprogramowaniu i bezpiecznie wykonanej sieci komputerowej (zarówno w aspekcie elementów fizycznych sieci jak i używanego oprogramowania – systemu operacyjnego, zabezpieczeń);
– zadbanie o zainstalowanie i właściwe zarządzanie oprogramowaniem służącym do oddzielenia danych wewnętrznych objętych tajemnicą lekarską od sieci zewnętrznej (tj. Internetu); zadaniem tym powinien zajmować się zespół informatyków pod nadzorem administratora bezpieczeństwa informacji;
– stworzenie regulaminu dla użytkowników sieci komputerowej, który w sposób precyzyjny określać będzie obowiązki i uprawnienia poszczególnych osób oraz procedury postępowania w przypadkach włamań, awarii czy innych problemów;
– powołanie zespołu informatyków odpowiedzialnych za zarządzanie systemami komputerowymi; zespół informatyków musi być przeszkolony i zobowiązany do zachowania tajemnicy służbowej a także lekarskiej z racji posiadanego pełnego dostępu do danych pacjentów w szpitalu;
– zadbanie o ustalenie funkcjonalnego standardu oprogramowania systemowego (na serwerach) oraz użytkowego (dla poszczególnych użytkowników), w których oprócz oprogramowania podstawowego (systemu szpitalnego) mieściłby się pakiet biurowy, oprogramowanie multimedialne używane dla celów telemedycznych, dostęp do Internetu z zabezpieczeniami (*firewall*) oraz programem antywirusowym;
– codzienny nadzór nad prawidłowością działania sieci oraz poszczególnych ich stanowisk (w tym analiza zapisów dzienników serwerów) przez zespół informatyków, tworzenie kopii zapasowych danych i właściwe przechowywanie ich.

Za stworzenie spójnego projektu odpowiada dyrektor (właściciel placówki). Bardzo ważna jest świadomość, że komputeryzacja placówki medycznej nie jest jednorazowym działaniem, lecz stałym przedsięwzięciem zmierzającym do usprawnienia obiegu informacji w placówce medycznej poprzez wykorzystywanie systemów informatycznych. W projekcie trzeba uwzględniać między innymi także konieczność uzupełniania sprzętu komputerowego, dostosowywania go do potrzeb użytkownika, aktualizację oprogramowania i zabezpieczeń oraz dostosowywanie sprzętu do nowych działań. Dyrektor (właściciel) placówki powinien nie tylko jednorazowo wyasygnować środki (lub pozyskać je z odpowiednich programów Unii Europejskiej), lecz przeznaczać odpowiednie środki w bieżącym budżecie kierowanej przez siebie placówki. Właści-

wa komputeryzacja powinna przynosić danej placówce oszczędności wynikające z poprawy i przyspieszenia zarządzania danymi medycznymi i finansowymi. Ponadto w placówkach naukowych komputeryzacja jest nieodzowna dla prowadzenia badań.

Instalacja i właściwe zarządzanie oprogramowaniem służącym do oddzielenia danych wewnętrznych objętych tajemnicą lekarską od sieci zewnętrznej

Współcześnie wszystkie instytucje posiadają dostęp do Internetu, który jest niezbędnym w codziennej pracy źródłem informacji. Niezwykle ważną rzeczą jest świadomość, że w przypadku informatyzacji placówki medycznej będziemy mieli do czynienia z dwoma sieciami działającymi obok siebie; dane wewnętrzne muszą być oddzielone. Istotą takiego podziału musi być to, że użytkownik stacji komputerowej w przychodni czy szpitalu winien posiadać autoryzowany dostęp do danych wewnętrznych oraz do Internetu, natomiast dla osób z zewnątrz nie powinno być dostępu do wewnętrznej bazy informacyjnej. Dla celów bezpieczeństwa właściwe stworzenie takich mechanizmów i codzienny nadzór nad poprawnym działaniem systemów zabezpieczających jest kluczowy.

Regulamin dla użytkowników sieci komputerowej

Podstawą zabezpieczenia sieci przed niepowołanymi działaniami z zewnątrz i od wewnątrz sieci jest dobrze zaprojektowany regulamin. W projekcie takiego regulaminu należy uwzględnić między innymi:

- zasady użytkowania komputerów PC przyłączonych do sieci,
- sposoby nadawania, przechowywania i chronienia haseł dostępu do danych, serwerów i jego usług,
- zasady zgłaszania oraz usuwania awarii w tym rolę administratora w ich raportowaniu,
- uprawnienia osób funkcyjnych (w tym administratorów całej sieci, wybranych serwerów i usług, a także moderatorów i osób nadzorujących dane medyczne od strony merytorycznej – kierownicy klinik, ordynatorzy, kierownicy i członkowie zespołów badawczych),
- zasady zabezpieczeń sieci i postępowania w przypadku prób ich omijania lub łamania, w tym ustalenie definicji próby włamania do sieci, nieuprawnionego dostępu, uszkadzania sieci (w tym rozprzestrzeniania wirusów),
- zasady dostępu do pomieszczeń, w których znajdują się poszczególne urządzenia sieciowe,
- schemat działań poszczególnych osób w przypadku awarii lub uszkodzenia komputera lub sieci.

Regulamin pełni funkcje „kodeksu drogowego” dla osób poruszających się w cyberprzestrzeni. Jednakże zbyt restrykcyjny regulamin powoduje najczęściej, że w ogóle przestaje się go stosować, jest bowiem traktowany jako nieżyciowy i paraliżujący możliwość korzystania z Internetu i komputerów w ogóle.

Troska o ustalenie funkcjonalnego standardu oprogramowania

Medyczna baza danych nie jest zazwyczaj wystarczającym oprogramowaniem spełniającym wszystkie oczekiwania użytkownika. Wielokrotnie potrzebny jest także edytor tekstu, podręczna baza danych, arkusz kalkulacyjny i wiele innych programów (m.in. przeglądarki internetowe, programy do poczty elektronicznej). Warto, aby od samego początku przyjąć w danej placówce jednolity, zgodny z powszechnym standard oprogramowania i udostępnić go użytkownikowi. Działanie takie jest niezwykle ważne z punktu widzenia bezpieczeństwa sieci, gdyż unika się w ten sposób używania programów niesprawdzonych (często samodzielnie instalowanych przez użytkowników). Pozwala to na lepszą kontrolę bezpieczeństwa systemu i sieci.

Dr Piotr Kasztelowicz
Oddział Chorób Płuc
Wojewódzki Szpital Zespolony im. Ludwika Rydygiera w Toruniu
e-mail: Piotr.Kasztelowicz@am.torun.pl