

Zapewnienie bezpieczeństwa danych medycznych w szpitalnym systemie informatycznym

Medical data security assurance in hospital computer-based system

MARZENA PAWIŃSKA, ANDRZEJ SZPAK, MAGDALENA ZALEWSKA

Zakład Zdrowia Publicznego Akademii Medycznej w Białymstoku, ul. I Armii Wojska Polskiego 2/2, 15-104 Białystok

Modern medicine achievements impose many challenges on people working in healthcare facilities. These challenges include legal, scientific and practical issues. One of these challenges is the need for accumulation, storing and protection of growing amount of medical data of different kind. The compromise meaning that, at the same time, patients' autonomy is protected and the access to data (within limitations) is free for people involved in the treatment is inevitable.

Traditional, paper-based records are not enough for daily efficient work of healthcare system. The use of computer-based data makes the flow of information in a hospital easier, and also the communication between hospital and its surroundings is much more simple. The development of computer-based networks in hospitals requires however the fulfillment of rigorous security norms according to transformed data, especially the data about patients' health status.

The article describes basic security policy rules and the factors enabling development of a model security system in a hospital.

Many factors inhibit the construction of model security system, which include: availability of the main computer system administrator (wages, especially in underfinanced public healthsector, and lower prestige of workplace in contrast to other high technology posts in industry); level of access to data description for each group of personnel, development of threats emerging from malware and computer delinquency, hardware and software costs, archivization and storage of electronic records. Problems are also observed with implementation of new technology and administration system (resistance to changes), especially when they require change of work organization (old organizational habits).

In conclusion, complete model of hospital computer-based system security is possible, but it requires strategic expenses. First – the motivation and participation of all system users and creativity of the system administrator. Second – money to implement changes. Financial means are usually very limited, and they have to be efficiently spent.

Key words: medical data, security, system, administrator

Osiągnięcia współczesnej medycyny stawiają przed osobami pracującymi w zakładach opieki zdrowotnej wyzwania, zarówno od strony prawnej, naukowej, jak i praktycznej. Jednym z nich jest konieczność gromadzenia, przechowywania i ochrony coraz większych ilości, różnorodnych danych medycznych. Konieczne jest dojście do kompromisu, w którym jednocześnie jest chroniona sfera autonomii pacjenta oraz możliwy jest swobodny (w określonych granicach) obieg informacji związany z procesem leczenia.

Sama dokumentacja papierowa przestaje wystarczać do codziennego, sprawnego działania jednostek opieki zdrowotnej. Wykorzystanie danych w postaci elektronicznej umożliwi łatwiejszy przepływ informacji wewnątrz szpitala oraz pomiędzy nim, a otoczeniem zewnętrznym. Rozwijająca się komputeryzacja szpitalnictwa wymaga jednak spełnienia rygorystycznych norm bezpieczeństwa w kwestii ochrony przetwarzanych danych szczególnie, jeżeli chodzi o informacje o stanie zdrowia pacjentów. Artykuł opisuje podstawowe założenia polityki bezpieczeństwa oraz czynniki sprzyjające budowie modelowego systemu zabezpieczeń.

Istnieją również czynniki utrudniające budowę modelowego systemu zabezpieczeń, spośród których za istotne uważa się: pozyskanie dobrego głównego administratora systemu informatycznego (warunki płacowe, szczególnie w publicznym sektorze ochrony zdrowia oraz niższy prestiż stanowiska względem pracowników działalności podstawowej); określenie poziomu dostępu do danych poszczególnych grup pracowników; rozwój zagrożeń związanych z malware i przestępczością komputerową, wysoki koszt sprzętu oraz oprogramowania, archiwizacja oraz przechowywanie dokumentów elektronicznych. Trudności spotykane są również przy wdrażaniu nowych rozwiązań technologicznych i administracyjnych (opór wobec zmian), szczególnie jeżeli wymagają one zmiany organizacji pracy (stare nawyki organizacyjne).

Podsumowując, kompletny model zabezpieczeń szpitalnego systemu informatycznego, jest możliwy do realizacji, jednakże wymaga dwóch strategicznych nakładów. Po pierwsze – chęci do pracy i zaangażowania wszystkich użytkowników systemu oraz silnej motywacji i kreatywności administratora systemu. Po drugie – środków finansowych na realizację zamierzeń. Te są zazwyczaj bardzo ograniczone, więc muszą być rozdysponowane w sposób jak najbardziej efektywny.

Słowa kluczowe: dane medyczne, bezpieczeństwo, system, administrator

Ochrona danych osobowych w zakładzie opieki zdrowotnej – teoria i praktyka

Personal data protection in a hospital – theory and practice

PAWEŁ DZIERZYŃSKI, JACEK ŁUKOMSKI, ERWIN STRZESAK

Szpital Wojewódzki w Poznaniu, ul. Juraszów 7/19, 60-479 Poznań

The introduction of IT systems into hospitals made the data access and processing much easier. The special character of the data stored in those systems may have potentially serious consequences in case of unauthorized usage. The authors present legal regulations as well as methods utilized in hospital IT systems which serve the purpose of protecting personal data.

Key words: personal data, medical documentation

Informatyzacja zakładów opieki zdrowotnej stała się powodem łatwiejszego dostępu do przetwarzanych danych. Specyfika informacji gromadzonych w tych systemach wiąże się w większymi konsekwencjami w przypadku ich nieautoryzowanego wykorzystania. Autorzy przedstawiają uregulowania prawne oraz metody stosowane w szpitalnych systemach informacyjnych dla zapewnienia właściwej ochrony danych osobowych.

Słowa kluczowe: dane osobowe, dokumentacja medyczna