Studia Medyczne Akademii Świętokrzyskiej tom 2
Kielce 2004

Grażyna Kowalik
Zakład Pielęgniarstwa Społecznego
Instytutu Kształcenia Medycznego Akademii Świętokrzyskiej w Kielcach
Kierownik: prof. dr hab. n. med. S. Zabielski
Dyrektor: prof. dr hab. W. Dutkiewicz

OCHRONA INFORMACJI ZDROWOTNYCH W STANACH ZJEDNOCZONYCH*

STRESZCZENIE

Lekarze powinni znać prawne obowiązki ochrony możliwych do zidentyfikowania informacji zdrowotnych pacjenta. Mimo że dane zapisywane na papierze mają takie same standardy prywatności, jednak te, które są gromadzone lub przesyłane elektronicznie, mogą być podatne na przedostanie się w niepowołane ręce. Ta uwaga potwierdza potrzebę prywatności i poufności danych medycznych pacjentów, sugeruje zabezpieczenie ich przed dostępem niepowołanych osób oraz niewłaściwym ich użyciem. Zabezpieczenia powinny być właściwe dla techniki gromadzenia, uaktualniania oraz przesyłania danych. Nie mogą nadmiernie obciążać lub utrudniać dostępu do opieki medycznej.
Amerykańska Akademia Pediatrii zaleca, aby zabezpieczenia były dostosowane do potrzeb pacjentów. Obecnie w Stanach Zjednoczonych prowadzi się dyskusje na temat ograniczenia odpowiedzialności lekarzy do przekazywania danych. Sądzi się, że nowe standardy prywatności i poufności pacjentów muszą równoważyć potrzeby zdrowotne społeczeństwa oraz prawa pacjentów, bez zmniejszania możliwości lekarzy do udzielenia wysokiej jakości opieki medycznej. Lekarze oraz stowarzyszone z nimi instytucje są odpowiedzialne za bezpieczeństwo oraz poufność danych medycznych. Aktualnie, w ponad czterdziestu stanach, ujawnienie medycznych informacji jest zabronione.
Akt ubezpieczenia zdrowotnego z 1996 r. (HIPAA) upoważnia rząd Stanów Zjednoczonych do uchwalenia narodowych standardów prywatności danych medycznych poprzez czynności legislacyjne lub regulacyjne.

Słowa kluczowe: ochrona, informacje zdrowotne, Stany Zjednoczone.

SUMMARY

Doctors should know their legal responsibilities to protect the privacy of identifiable patient health information. Although paper and electronic medical records have the same privacy standards, health data that are stored or transmitted electronically are vulnerable to unique security breaches. This statement describes the privacy and confidentiality needs and rights of pediatric patients and suggests appropriate security strategies to deter unauthorized access and inappropriate use of patient data. These requirements should be reasonable and appropriate for the technology used to store update, and transmit data. Most importantly, the security provisions should not unduly burden physicians or impede the provision of health care.

* Opracowano na podstawie Pediatric Practice Action Group and Task Force on Medical Informatics. Pediatrics 1999; 104(4). Privacy Protection of Health Information Patient Rights and Pediatrician Responsibilities.

The American Academy of Pediatrics recommends that legislated or regulated provisions accommodate the unique needs of pediatric patients newborns, infants, children, adolescent, and young adults. Any new standards for patient privacy and confidentiality must balance the health needs of the community and the rights of the patient without compromising the ability of pediatricians to provide quality care. Pediatricians or their affiliated institutions are responsible for the security and confidentiality of medical records in their possession. Currently more than 40 states have statutes imposing civil or criminal penalties for impermissible disclosure of medical information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) authorizes the federal government to establish a national standard for medical record privacy either by legislative or regulatory action.

Key words: protection, health information, The United States.

UŻYTKOWNICY INFORMACJI ZDROWOTNYCH W STANACH ZJEDNOCZONYCH

Decyzja o monitorowaniu, ograniczaniu lub kontrolowaniu dostępu do danych medycznych jest uzależniona od pierwotnego lub kolejnego ich użycia. Pierwotni użytkownicy to pracownicy klinik (lekarze, pielęgniarki, terapeuci oraz inne pokrewne instytucje), którzy korzystają z informacji zdrowotnych w celu zapewnienia pacjentowi odpowiedniej opieki medycznej.

Innymi użytkownikami informacji zdrowotnych są pracownicy naukowi, nauczyciele, płatnicy ubezpieczenia od odpowiedzialności cywilnej, administratorzy, przedstawiciele prawa, księgowi, pracodawcy oraz pracownicy firm ubezpieczeniowych; ich dostęp do danych zdrowotnych nie musi być związany z leczeniem pacjenta.

Pacjenci mają prawo być powiadomieni o osobach korzystających z ich danych medycznych. Ubezpieczyciele lub płatnicy zdrowotni, którzy żądają dostępu do danych zdrowotnych w celu ich wykorzystania, powinni powiadomić o tym pacjentów oraz udzielić informacji, w jakim celu wykorzystują dane; ich obowiązkiem jest ochrona poufności pacjenta.

DOSTĘP DO DANYCH MEDYCZNYCH

Dane medyczne są własnością instytucji, w której zostały zapisane; pacjenci mają prawo wglądu do nich. Lekarze i ich pacjenci oraz opiekunowie decydują, kto może mieć ograniczony lub pełny dostęp do tych danych. Opiekunowie mają prawo przeglądać dane medyczne dzieci, kiedy chcą. Wyjątek stanowią nieletni, mający prawo do poufności. Zasadniczą rolą lekarzy jest mediacja między rodzicami i nastolatkami, w celu zmniejszenia konfliktu dotyczącego dostępu do informacji medycznych. Ogranicza się dostęp do danych medycznych stosownie do wieku, postawionej diagnozy lub innych czynników określonych przez stanowe lub federalne prawo. Decyzja pacjentów musi być respektowana i nie powinna być negowana.

Rodzice i opiekunowie powinni mieć świadomość ryzyka związanego z udostępnianiem informacji zdrowotnych w celach nie związanych z leczeniem. Zaleca się im, aby rozważyli:
– precyzyjność informacji,
– czy z danych korzysta pierwotny czy kolejny użytkownik?,
– urzędowe użycie danych,
– czy zastrzeżono ograniczenie lub pełny dostęp do danych?,
– czy dane identyfikują pacjenta?,
– czy dane są analizowane i publikowane jako niezależne, czy są powiązane z innymi danymi i przedstawione jako wnioski z analizy?

Instytut Medycyny w Stanach Zjednoczonych określił trzy poziomy zabezpieczeń danych medycznych pacjenta: nieuprzywilejowane (najmniej precyzyjne dane), uprzywilejowane (precyzyjne i poufne dane) oraz bardzo precyzyjne i poufne. Zabezpieczenia elektroniczne dotyczą elektronicznego podpisu, hasła, identyfikacji pacjenta i poświadczenia kliniki, gwarantując wysoki poziom tajności najbardziej precyzyjnych informacji. Jednak mogą pojawić się trudności z zabezpieczeniem takich informacji, jak: choroba przekazana drogą seksualną, adopcja, nadużywanie przemocy fizycznej, nadużywanie substancji, płciowość, choroby genetyczne, rak lub choroby umysłowe, jeżeli przekazuje się je kolejnym użytkownikom.

Informacje zdrowotne, do których jest ograniczony dostęp, mogą wymagać dodatkowych zabezpieczeń, np. użycia osobnego działu (gdy dane są zapisywane na papierze) lub hasła (gdy dane są zapisywane elektronicznie).

UDOSTĘPNIANIE AKT MEDYCZNYCH

Lekarze oraz stowarzyszone z nimi instytucje powinni egzekwować dyscyplinę w ujawnianiu akt medycznych oraz posiadać oryginalne dokumenty dotyczące zdrowia pacjenta. Anonimowe informacje i dane o pacjentach, używane do badań lub publicznych funkcji zdrowotnych, powinny być udostępniane pod nadzorem właściwych instytucji, np. instytucji przeglądu danych (IRBs). Ujawnianie informacji bez zgody pacjenta jest karane.

PRECYZJA I INTEGRALNOŚCI DANYCH MEDYCZNYCH

Lekarze oraz związane z nimi instytucje są odpowiedzialnie za precyzję i integralność danych medycznych. Informacje powinny być dokładne, obiektywne, czytelne, aktualne i pełne. Żaden zapis stanu zdrowotnego pacjenta nie powinien być kasowany. Jeżeli zapis o zdrowiu pacjenta jest niewłaściwy, może być zmieniony przez klinikę czy szpital. Kliniki używające elektronicznego systemu infor-

macji muszą weryfikować system zabezpieczeń, w celu wyeliminowania dostępu osób nieupoważnionych oraz zmieniania danych.

Rodzice lub opiekunowie mogą dołączać komentarze na piśmie do elektronicznych danych.

ELEKTRONICZNE PRZESYŁANIE DANYCH

Lekarze powinni starać się używać właściwych zabezpieczeń, gdy przesyłają dane pacjenta drogą elektroniczną, np. faksem, pocztą elektroniczną, Internetem. Osoba, która otrzymuje dane, jest za nie odpowiedzialna. Informacje zdrowotne nie powinny być przesyłane do nieznanych odbiorców. Dla zachowania poufności należy przesłać potwierdzenie odbioru po otrzymaniu danych oraz zapewnienie użycia ich do właściwych celów. Producenci oprogramowania mają możliwość poprawić bezpieczeństwo przesyłania danych. Jeżeli pojawia się przekaz medyczny, osoby otrzymujące go są odpowiedzialne za niego i zobligowane używać danych wyłącznie do własnych celów. Dla szerszego użycia informacji medycznych potrzebna jest zgoda pacjenta.

ELEKTRONICZNY BILLING

Przekształcenie dokumentów związanych z rachunkowością w elektroniczne billingi oraz zwrot kosztów mogą przyczynić się do użycia zewnętrznych źródeł elektronicznej wymiany danych (EDI). Izby rozrachunkowe EDI otrzymują dane przesłane elektronicznie od związanych z nimi instytucji (np. gabinetu lekarskiego lub kliniki), przekształcają dane w elektroniczny format, a następnie wysyłają do płatnika. Sprzedawcy EDI powinni zapewnić klientów, że ich system zabezpieczania danych spełnia federalne standardy, zabezpieczając dane pacjenta.

Według obecnych standardów HIPAA, za niedopełnienie wymogów może być nałożona kara od 100$ do 25 000$ na osobę w ciągu roku. W konsekwencji instytucje korzystające z EDI nie powinny być odpowiedzialne za błędy sprzedawców. Federalne standardy elektronicznego przesyłania danych nie spełniają wymogów stanowego prawa, jeżeli nie otrzymają zgody od ministra zdrowia.

REJESTR ZDROWIA

Rejestr zdrowia w Stanach Zjednoczonych to zorganizowany system: gromadzenia, przechowywania, wyszukiwania, analizowania i rozpowszechniania informacji na temat chorób, czynników ryzyka lub ujawnienia okoliczności powodujących niszczenie zdrowia. Rejestr może być kierowany przez agencje federalnego

rządu (np. Narodowy Rejestr Ujawniania Informacji Zdrowotnych), uniwersytety (np. nadzór, epidemiologia i końcowy rezultat, rejestr zachorowań na raka), organizacje niekomercyjne (np. rejestr chorób oczu), prywatne organizacje (np. rejestr transplantacji) lub rządy stanowe (np. elektroniczny rejestr narodzin, system monitorowania noworodków oraz rejestr uodpornień).

Plany wprowadzenia numeru identyfikacji pacjenta (UPI), jako uproszczenie administracyjne HIPAA, zostały wstrzymane, kiedy zauważono, że placówka UPI mogłaby stworzyć narodowy bank danych zdrowotnych. Rodzi to obawy dotyczące prywatności i poufności informacji medycznych pacjenta.

Rząd federalny zdecydował utrzymać rozwój standardów UPI do momentu ustanowienia regulacji chroniących prywatność informacji zdrowotnych pacjenta. Ponad 20 stanów powołało rejestry odporności, natomiast wiele z pozostałych rozważa ich zalegalizowanie.

Publiczne badania zdrowotne mają na celu ochronę społeczeństwa przed wybuchem epidemii chorób, których można uniknąć poprzez szczepionki, a także obliczenia kosztów opieki oraz uproszczenie gromadzenia danych zdrowotnych w stanowych agencjach zdrowia i szkołach. Wydaje się, że bez właściwego zabezpieczenia, dotyczącego udostępniania danych odpornościowych pacjenta oraz rejestru szczepień, może nastąpić ograniczenie prywatności informacji zdrowotnych pacjenta.

W Kalifornii wprowadzono prawo pozwalające lekarzom na dostęp do baz danych dotyczących odporności, bez uprzedniej zgody pacjenta.

Sądzi się, że lekarze powinni zminimalizować ryzyko związane z przekazywanie danych. Przed rozpoczęciem gromadzenia danych odpornościowych należałoby zabezpieczyć prywatność pacjenta, włączając ograniczenia do dostępu danych, uaktualnienie, przegląd lub przekazywanie danych, oraz nakładać surowe kary za nieupoważnione ujawnienie danych. Personel rejestru ma oferować na piśmie standardy zabezpieczeń. Mają być one znane także pracownikom rejestru, pacjentom oraz rodzicom. Cel użycia danych powinien zostać wyjaśniony.

Obowiązkiem lekarzy w Stanach Zjednoczonych jest ochrona medycznych informacji pacjentów. Federalne przepisy wypierają mniej znaczące prawa ochrony oraz zakładają, że nieistniejące prawo pacjenta (szczególnie nieletnich) do prywatności powinno być wycofane lub ograniczone.

REKOMENDACJE AMERYKAŃSKIEJ AKADEMII PEDIATRII

Lekarze w Stanach Zjednoczonych powinni zachęcać polityków do ustanowienia prawa, w celu zniesienia ryzyka związanego z gromadzeniem, ochroną, analizowaniem lub rozpowszechnianiem danych medycznych. Powinni też wspierać prawo powiadamiania pacjentów (przynajmniej co roku) o wglądzie do ich danych medycznych (w zawiadomieniu – nazwa instytucji, której dane są udostępnione

i cel ich użycia). Dobrze jest, jeżeli pacjenci są powiadomieni o ryzyku związanym z podpisaniem zgody na udostępnienie informacji medycznych. Zaleca się, aby pacjenci lub ich opiekunowie mieli nie tylko prawo wglądu do własnych danych medycznych, ale także powinno się zezwalać dołączać komentarze do nich, kopiować je oraz dawać możliwość upoważniania osób do korzystania z danych pacjentów.