OFFICE FOR CIVIL RIGHTS

PRYWATNOŚĆ, BEZPIECZEŃSTWO I ELEKTRONICZNA DOKUMENTACJA MEDYCZNA

Pana(-i) świadczeniodawca opieki zdrowotnej może być w trakcie zmiany papierowej dokumentacji na elektroniczną dokumentację zdrowotną (EHR) lub być może od pewnego czasu stosuje już EHR. EHR umożliwia świadczeniodawcom bardziej efektywne wykorzystanie informacji w celu poprawy jakości i wydajności opieki, nie zmieni jednak zabezpieczeń podejmowanych w celu ochrony danych zdrowotnych.

EHR i dane zdrowotne

EHR to elektroniczna wersja kart w formie papierowej, jakie prowadzone są w gabinetach lekarza lub innych świadczeniodawców opieki zdrowotnej. EHR może zawierać historię medyczną, uwagi oraz inne informacje na temat zdrowia, w tym objawy, rozpoznanie, leki, wyniki badań laboratoryjnych, parametry życiowe, szczepienia i raporty z badań diagnostycznych, na przykład badania RTG.

Świadczeniodawcy współpracują z innymi lekarzami, szpitalami i planami ubezpieczenia zdrowotnego nad znalezieniem sposobów udostępniania tych informacji. Dane zawarte w EHR mogą być ujawniane innym organizacjom zaangażowanym w opiekę nad pacjentem, jeśli systemy komputerowe są ustawione na komunikację. Informacje zawarte w dokumentacji powinny być ujawniane wyłącznie w celach zgodnych z prawem lub w celach, na które pacjent wyraził zgodę.

Pacjentowi przysługują prawa do ochrony danych niezależnie, czy dane te są przechowywane w formie papierowej czy elektronicznej. Przepisy federalne chroniące dane zdrowotne pacjenta mają również zastosowanie do informacji zawartych w EHR.

Korzyści płynące z EHR

Niezależnie od tego czy świadczeniodawca zmienia właśnie dokumentację papierową na EHR, czy już od jakiegoś czasu stosuje w swoim gabinecie EHR, pacjent może na tym skorzystać w następujący sposób:

- **Ulepszona jakość opieki.** W związku z rozpoczęciem stosowania przez lekarzy EHR i określeniem sposobów bezpiecznego udostępniania danych zdrowotnych pacjentów innym świadczeniodawcom, współpraca świadczeniodawców i zapewnienie pacjentowi potrzebnej opieki będzie ułatwione. Na przykład:
    - EHR będzie zawierała informacje o lekach stosowanych przez pacjenta, tak aby świadczeniodawcy nie zalecili pacjentowi leków, które mogą mu szkodzić.
    - Tak jak w przypadku większości systemów komputerowych, systemy EHR są odpowiednio zabezpieczone, tak więc na przykład w przypadku katastrofy, takiej jak huragan, dane zdrowotne można odzyskać.
    - W nagłym przypadku można uzyskać dostęp do EHR. Jeśli pacjent ulegnie wypadkowi lub nie będzie w stanie wyjaśnić swojej historii zdrowotnej, szpital wyposażony w system będzie mógł skontaktować się z systemem lekarza pacjenta. Szpital uzyska informacje o lekach stosowanych przez pacjenta, jego problemach zdrowotnych oraz badaniach, a dzięki temu będzie w stanie podejmować szybsze i bardziej trafne decyzje o opiece.

- **Skuteczniejsza opieka.** Lekarze korzystający z EHR mogą łatwiej i szybciej uzyskać wyniki badań laboratoryjnych pacjenta i poinformować go o postępach leczenia. Jeśli w ramach systemów lekarze mogą udostępniać sobie informacje, mogą oni ujawniać sobie wyniki testów, dzięki czemu powtarzanie pewnych badań nie będzie konieczne. Ma to znaczenie szczególnie w przypadku badań RTG i pewnych testów laboratoryjnych, dzięki czemu pacjent będzie rzadziej narażony na promieniowanie i inne działania uboczne. Brak konieczności powtarzania badań oznacza również niższe koszty opieki zdrowotnej ponoszone przez pacjenta w ramach współpłatności i udziałów własnych.
- **Bardziej dogodna opieka.** EHR może przypominać świadczeniodawcom o skontaktowaniu się z pacjentem w chwili, gdy będzie się zbliżał termin określonych badań przesiewowych. Możliwość wzajemnego udostępniania sobie informacji przez lekarzy, farmaceutów, laboratoria oraz innych członków zespołu ds. opieki oznacza brak konieczności wielokrotnego wypełniania przez pacjenta tych samych formularzy, czekania na przekazanie innemu lekarzowi dokumentacji w formie papierowej lub przenoszenia takiej dokumentacji.

Zabezpieczenie danych zdrowotnych przechowywanych w formie elektronicznej

Większość z nas uważa, że dane zdrowotne są sprawą prywatną i powinny być chronione. Rząd federalny wprowadził Ustawę o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych z roku 1996 (ang. The Health Insurance Portability and Accountability Act of 1996 - HIPAA), aby zapewnić pacjentom prawa do ich danych zdrowotnych, niezależnie od formy ich przechowywania. Rząd ustanowił również Zasadę bezpieczeństwa HIPAA, która wymaga stosowania określonych zabezpieczeń w celu ochrony elektronicznych danych zdrowotnych pacjenta. Poniżej przedstawiono kilka możliwych zabezpieczeń, które mogą być zintegrowane z systemami EHR:

- Narzędzia „kontroli dostępu” takie jak hasła i numery PIN, które ograniczą dostęp do danych pacjenta wyłącznie do osób upoważnionych.
- „Szyfrowanie” przechowywanych informacji. Oznacza to, że danych zdrowotnych nie będą mogły odczytać ani zrozumieć osoby, które nie będą posiadały systemu „odszyfrowującego” dane odpowiednim „kluczem.”
- Funkcja „dziennika inspekcji” rejestrująca osoby uzyskujące dostęp do danych, wprowadzone zmiany oraz ich datę.

Ostatecznie, w świetle przepisów federalnych lekarze, szpitale oraz inni świadczeniodawcy opieki zdrowotnej są zobowiązani do poinformowania pacjenta o naruszeniu prywatności jego danych. Prawo wymaga również, aby świadczeniodawca poinformował o tym Sekretarza ds. zdrowia i usług społecznych. Jeśli naruszenie prywatności będzie dotyczyło ponad 500 mieszkańców danego stanu lub jurysdykcji, świadczeniodawca musi również powiadomić o tym najważniejsze środki masowego przekazu obsługujące dany stan lub jurysdykcję. Wymóg ten umożliwia pacjentom uzyskanie informacji o nieprawidłowej ochronie ich danych, a także rozliczać świadczeniodawców za ochronę EHR.

Więcej informacji można uzyskać na stronie **www.hhs.gov/ocr/privacy/**.