Jak zabezpieczyć dokumentację medyczną w placówce – 6 wskazówek

WSKAZÓWKA 1. Stosuj 6 reguł bezpieczeństwa dokumentacji medycznej

1. Systematyczne szacowanie ryzyka zagrożeń i zarządzanie nimi.
2. Opracowanie i stosowanie udokumentowanych procedur zabezpieczania i przetwarzania dokumentacji, w tym procedur dostępu oraz przechowywania.
3. Stosowanie środków bezpieczeństwa adekwatnych do zagrożeń, uwzględniających najnowszy stan wiedzy.
4. Dbałość o aktualizację oprogramowania.
5. Bieżące kontrolowanie funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowa ocena ich skuteczności.
6. Przygotowanie i realizacja planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenie na informatyczne nośniki danych i do nowych formatów danych, jeżeli wymaga tego zapewnienie ciągłości dostępu do dokumentacji.

WSKAZÓWKA 2. Zagwarantuj odpowiedni poziom zabezpieczeń w systemie IT

Zapewnij, aby system IT stosowany do przechowywania elektronicznej dokumentacji medycznej spełniał następujące warunki:

- **integralność treści dokumentacji i metadanych** polegająca na zabezpieczeniu przed wprowadzaniem zmian (z wyjątkiem modyfikacji wprowadzanych w ramach udokumentowanych procedur);
- **stały dostęp do dokumentacji** dla osób uprawnionych;
- **zabezpieczenie przed dostępem osób nieuprawnionych;**
- **identyfikacja osoby sporządzającej dokumentację** oraz wprowadzającej wpis lub inną zmianę i zakresu zmian w dokumentacji lub metadanych;
- **informacja o czasie sporządzenia dokumentacji** i wprowadzenia wpisu lub innej zmiany;
- **przyporządkowanie cech informacyjnych** do odpowiednich rodzajów dokumentacji;
- **możliwość prowadzenia i udostępniania dokumentacji** w określonych formatach i standardach HL7 oraz DICOM lub innych;
- **możliwość wydruku** dokumentacji;
- **możliwość eksportu** całości danych w wymienionych standardach i formatach, w sposób umożliwiający odtworzenie ich w innym systemie IT.

WSKAZÓWKA 3. Zabezpiecz serwery i serwerownię

Serwery czy pomieszczenia, gdzie przechowujesz dokumentację w postaci papierowej, zabezpiecz w taki sposób, aby ochronić ją przed zniszczeniem, utratą, dostępem osób nieuprawnionych, w tym przed kradzieżą.

Koniecznie określ pomieszczenia o podwyższonym standardzie bezpieczeństwa danych, to znaczy takie, w których wprowadza się lub tworzy dane.

Należą do nich: rejestracja, recepcja, izba przyjęć, gabinet lekarski, pracownia diagnostyczna, laboratorium itd.

W tych pomieszczeniach osoby nieuprawnione, np. pacjenci i osoby im towarzyszące, **nie mogą przebywać bez pracownika placówki** lub innej osoby uprawnionej.

W placówce medycznej samodzielnie przetwarzającej i archiwizującej dane pacjentów wyznacz pomieszczenia o znaczeniu krytycznym, w których znajduje się infrastruktura sieciowa, serwerowa oraz pomieszczenie administratora systemu informatycznego.

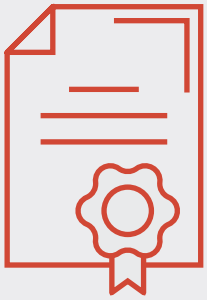
Pomieszczenia te muszą spełnić wysokie **wymogi w zakresie bezpieczeństwa**, tzn.:

- mieć system kontroli dostępu uniemożliwiający osobom nieuprawnionym dostęp (solidnej konstrukcji drzwi, bramki, ochrona),
- mieć wydajną klimatyzację,
- mieć instalację przeciwpożarową w postaci wewnętrznego systemu gaszenia wraz z systemem alarmowym,
- mieć zabezpieczenie przed utratą zasilania,

- nie mieć otworów okiennych,
- mieć pomiar parametrów takich jak: wilgotność, temperatura, które mogą w negatywny sposób wpłynąć na działanie urządzeń,
- mieć monitoring wizyjny.

Przebywanie osób w pomieszczeniach o znaczeniu krytycznym ma liczne ograniczenia, m.in.:

- musi podlegać autoryzacji,
- jest dozwolone wyłącznie dla osób upoważnionych lub mających zezwolenia wydane przez kierownika jednostki,
- jest możliwe wyłącznie w celu wykonywania obowiązków służbowych.



WSKAZÓWKA 4. Szyfruj dane medyczne

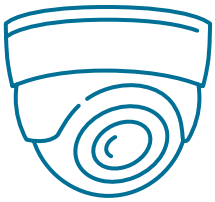
Dostęp do danych medycznych przechowywanych i przetwarzanych w systemie EDM – w celu zagwarantowania odpowiedniego poziomu bezpieczeństwa – powinny mieć tylko uprawnione osoby, a dodatkowo **dane powinny być szyfrowane**.

Dostęp ten odbywa się na podstawie zdefiniowanej w systemie metody logowania (hasło, certyfikat elektroniczny), która określi liczbę prób bezskutecznego logowania się do aplikacji – zaleca się 3 takie próby. Po wyczerpaniu prób logowania uruchamia się mechanizm blokowania konta użytkownika.

Komputery powinny być wyposażone w mechanizm blokowania ekranu lub zamykania sesji użytkownika w przypadku okresowego braku aktywności w aplikacji.

Wszystkie czynności wykonywane w aplikacji przez użytkowników powinny być rejestrowane w systemie. Rejestry te muszą być **zabezpieczone przed usunięciem lub modyfikacją**. Wszystkie problemy z dostępem i działaniem aplikacji powinny być zgłaszane zgodnie z obowiązującą w organizacji procedurą.

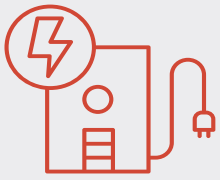
System EDM musi mieć mechanizm zapewniający **rozliczalność tworzonej dokumentacji**, przede wszystkim powinien oznaczać czasem początkowy wpis, modyfikację, wymianę danych oraz identyfikować osobę wprowadzającą zmianę.



WSKAZÓWKA 5. Zapewnij fizyczne zabezpieczenia gabinetów

Obszary o podwyższonym poziomie bezpieczeństwa typu: gabinet lekarski, laboratorium, powinny mieć:

- bezpieczne drzwi;
- kontrole dostępu w postaci przynajmniej jednego z zabezpieczeń: karta dostępowa z czytnikiem elektronicznym, przepustka;
- instalację przeciwpożarową;
- monitoring wizyjny drzwi wejściowych;
- monitoring zdarzeń, systemu wykrywania włamań;
- inne zabezpieczenia, np. kraty w oknach.



WSKAZÓWKA 6. Stosuj alternatywne źródła zasilania

Zapewnij więcej niż jedno źródło zasilania. Możesz to zrobić przez dodatkowe niezależne przyłącze energetyczne lub przez zakup generatora prądotwórczego.

Ponadto w celu zachowania ciągłości działania elementów krytycznych (serwery, urządzenia sieciowe) możesz zapewnić zasilanie gwarantowane: urządzenie UPS, agregaty prądotwórcze.

Regularnie testuj też sprawność działania UPS-ów i generatorów prądotwórczych.

Wiedza i Praktyka sp. z o.o., ul. Łotewska 9a, 03-918 Warszawa, nr rejestrowy BDO: 000008579,
Centrum Obsługi Klienta: tel. 22 518 29 29, faks: 22 617 60 10, www. formularze.wip.pl

ISBN 978-83-269-9996-3

HMD 20