

Ochrona lekarskiego laptopa

Coraz więcej danych medycznych przechowywanych jest na urządzeniach mobilnych: laptopach, tabletach czy nawet smartfonach. Od 1 sierpnia 2014 r. lekarze będą już używali wyłącznie komputerów, również przenośnych. Jak medycy mają chronić dane pacjentów zapisane na laptopach?

Każdy lekarz powinien wykazać się podstawową znajomością zasad kryptografii. – *Szyfrowanie danych na twardych dyskach czy pendrive'ach jest absolutnie konieczne. Przy dzisiejszych metodach kryptograficznych, często darmowych, możliwe jest zaszyfrowanie dysku w komputerze lub innym urządzeniu mobilnym w taki sposób, że osoba, która przejmie nad dyskiem kontrolę, bo na przykład ukradnie nam sprzęt, nie będzie w stanie dotrzeć do zapisanych tam danych. W przeciwnym przypadku możemy być współodpowiedzial-*



Jednak ich uszczegółowienie znajduje się w przepisach branżowych. W każdym przypadku, gdy przetwarzanie danych (np. ich pozyskiwanie czy udostępnianie) jest normowane przepisami szczególnymi, mają one pierwszeństwo przed regulacjami ustawy o ochronie danych osobowych. Jakie obowiązki ma więc lekarz prowadzący indywidualną praktykę, będący jednocześnie wytwarzającym dane, a także administratorem danych osobowych?

W obecnych czasach każdy lekarz powinien wykazać się podstawową znajomością zasad kryptografii. Szyfrowanie danych na twardych dyskach czy pendrive'ach jest absolutnie konieczne.

ni za utratę danych osobowych – mówi **dr Wojciech Rafał Wiewiórowski**, Generalny Inspektor Ochrony Danych Osobowych. Do ochrony wystarczy pobrać z Internetu lub zakupić program do szyfrowania pendrive'ów i zabezpieczenia ich hasłem. Ale to tylko wierzchołek góry lodowej, jaką jest ochrona danych medycznych pacjentów.

Ogólne zasady przetwarzania informacji osobowych określa ustawa o ochronie danych osobowych (z 29 sierpnia 1997 r.).

Lekarz tworzy i chroni

Lekarz, zgodnie z przepisami, ma obowiązek prowadzić indywidualną dokumentację medyczną pacjenta. Wynika to z art. 41, ust. 1 ustawy z 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty. Sposób prowadzenia i udostępniania dokumentacji medycznej przez lekarza określają przepisy ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Dlatego to przede wszystkim w kontekście tej ustawy i wydanego na jej podstawie rozporządzenia

Polityka bezpieczeństwa danych

ministra zdrowia z 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania należy rozpatrywać kwestię zabezpieczenia danych osobowych przetwarzanych przez lekarza. Dodatkowo

w ochronie zdrowia. To one określają m.in. zasady pozyskiwania, wykorzystywania i przechowywania danych medycznych, w tym tworzenia, archiwizowania i zabezpieczania dokumentacji medycznej.

Wymogi dotyczące zabezpieczenia danych odnoszą się zarówno do danych przetwarzanych na kartach papierowych, jak w systemach informatycznych.

w odniesieniu do zabezpieczenia dokumentacji medycznej w formie elektronicznej należy jeszcze wziąć pod uwagę przepisy ustawy z 28 kwietnia 2011 r. o systemie informacji

Trzy poziomy przetwarzania danych

Poziom co najmniej **podstawowy** stosuje się, gdy administrator w systemie informatycznym przetwarza tylko dane tzw. zwykłe (bez szczególnie chronionych), jak np. imię i nazwisko, adres zamieszkania czy numer PESEL i żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych nie jest połączone z siecią publiczną.

Poziom co najmniej **podwyższony** stosuje się, gdy w systemie informatycznym przetwarzane są dane szczególnie chronione, czyli przykładowo dane o stanie zdrowia, kodzie genetycznym czy nalogach, ale żadne z urządzeń systemu informatycznego nie jest połączone z siecią publiczną.

Natomiast poziom **wysoki** stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

Szczegółowy opis środków bezpieczeństwa stosowany na poszczególnych poziomach określa załącznik do rozporządzenia (§ 6 ust. 5) z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Na podmiocie tworzącym dokumentację – lekarzu – ciąży obowiązek jej odpowiedniego zabezpieczenia. Wynika to z § 73 powołanego rozporządzenia ministra zdrowia z 21 grudnia 2010 r., który brzmi: *Podmiot udzielający świadczeń zdrowotnych zapewnia odpowiednie warunki zabezpieczające dokumentację przed zniszczeniem, uszkodzeniem lub utratą i dostępem osób nieupoważnionych, a także umożliwiające jej wykorzystanie bez zbędnej zwłoki. W przepisach jest mowa o podmiocie udzielającym świadczeń. W praktyce lekarz prowadzący indywidualną praktykę lekarską jest takim podmiotem. Również miejsce przechowywania bieżącej dokumentacji wewnętrznej określa podmiot udzielający świadczeń zdrowotnych (§ 74 powołanego rozporządzenia). Lekarz-właściciel placówki tworzy dokumentację oraz określa miejsce jej przechowywania zarówno w formie papierowej, jak i elektronicznej (o wymogach dotyczących przechowywania dokumentacji elektronicznej czytaj w ramce: **Przechowywanie dokumentacji**).*

Warto zauważyć, że wiele rozwiązań technicznych związanych z zabezpieczeniem dokumentacji medycznej prowadzonej w formie elektronicznej zawartych w rozdziale 8 rozporządzenia ministra zdrowia (z 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania) jest wzorowanych na przepisach rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, jako aktu wykonawczego do ustawy o ochronie danych osobowych, do przestrzegania których lekarz również jest zobowiązany. Przesądzają one o tym, że administrator danych (właściciel placówki) jest zobowiązany do właściwego zabezpieczenia danych osobowych. W tym celu musi

Polityka bezpieczeństwa danych



dr. Wojciech Rafał Wiewiórowski
Generalny Inspektor Ochrony
Danych Osobowych

GIODO uprawniony jest do:

- kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wydawania decyzji administracyjnych i rozpatrywania skarg w sprawach wykonania przepisów o ochronie danych osobowych,
- prowadzenia rejestru zbiorów danych oraz udzielania informacji o zarejestrowanych zbiorach,
- opiniowania projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych,
- inicjowania i podejmowania przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
- uczestniczenia w pracach międzynarodowych organizacji i instytucji zajmujących się problematyką ochrony danych osobowych.

zastosować środki zabezpieczające zbiór danych, o których mowa w art. 36–39a ustawy o ochronie danych osobowych. Ma zatem obowiązek zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych

Wybór odpowiednich środków gwarantujących przetwarzanym danym optymalny stopień zabezpieczenia pozostawiają do uznania konkretnemu administratorowi danych osobowych (lekarzowi-właścicielowi). To on najlepiej zna środowisko, w jakim przetwarza dane osobowe, dlatego sam decyduje o użyciu środków danego rodzaju. Natomiast skuteczność zastosowanych rozwiązań podlega ocenie w czasie kontroli przeprowadzanej przez upoważnionych pracowników Generalnego Inspektora Ochrony Danych Osobowych. Podsumowując: lekarz-właściciel wytwarza i chroni dane wytworzone, odpowiada za wybór sposobu ochrony, a GIODO tylko kontroluje jej skuteczność.

Jakie rodzaje zabezpieczeń wybrać

Wybór rodzajów zabezpieczeń jest zależny przede wszystkim od wielkości placówki. W szczególności od ilości pomieszczeń w których przetwarzane są dane, liczby baz danych oraz pracowników mających dostęp do danych. Zastosowane rodzaje zabezpieczeń składają się na tzw. politykę bezpieczeństwa, która powinna zostać udokumentowana (opisana) przez administratora danych (właściciela, dyrektora). W przypadku indywidualnej praktyki lekarskiej – samodzielnie przez lekarza. Natomiast zastosowane zabezpieczenia w systemie informatycznym, służącym do przetwarzania danych osobowych, administrator danych powinien opisać w specjalnej dokumentacji zwanej instrukcją zarządzania systemem informatycznym. Wymogi dotyczące zabezpieczenia danych odnoszą się zarówno do danych przetwarzanych w sposób tradycyjny, jak i do danych przetwarzanych w sys-

Wybór środków gwarantujących bezpieczeństwo danych pozostaje w gestii administratora danych osobowych (właściciela placówki). To on najlepiej zna środowisko. Natomiast skuteczność zastosowanych rozwiązań podlega ocenie GIODO w trakcie kontroli.

osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36 ust. 1).

temach informatycznych (o tym, co powinna zawierać polityka bezpieczeństwa informacji, czytaj w ramce: **Polityka bezpieczeństwa informacji**).

Ponadto każdy administrator danych ma obowiązek wskazania w instrukcji zarządzania systemem informatycznym

Polityka bezpieczeństwa danych

(dokumencie zatwierdzonym przez administratora danych – właściciela placówki) zastosowanego przez niego poziomu bezpieczeństwa przetwarzania danych osobowych. Uwzględniając kategorie przetwarzanych danych oraz zagrożenia, rozporządzenie wprowadziło poziomy bezpieczeństwa przetwarzania informacji: podstawowy, podwyższony, wysoki (o poziomach bezpieczeństwa przetwarzanych danych, czytaj w ramce: **Trzy poziomy przetwarzania danych**).

Obowiązki dużych podmiotów

W przypadku większych placówek, zatrudniających kilku, kilkunastu czy większą liczbę pracowników, w instrukcji zarządzania systemem informatycznym administrator danych (właściciel, reprezentujący go menedżer) powinien opisać także szereg procedur związanych z bezpieczeństwem przetwarzanych danych osobowych, o których mowa w § 5 rozporządzenia (z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych). Ma on m.in. obowiązek wskazać procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazać osobę odpowiedzialną za te czynności. Powinien także wymienić procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników syste-

Polityka bezpieczeństwa informacji

Polityka bezpieczeństwa powinna zawierać w szczególności:

- 1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe,
- 2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
- 3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
- 4) sposób przepływu danych pomiędzy poszczególnymi systemami,
- 5) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

(Na podstawie § 4 rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych).

Każda placówka, nawet jednoosobowa, powinna mieć politykę bezpieczeństwa informacji oraz instrukcję zarządzania systemem teleinformatycznym.



Ochronie podlegają zarówno dane papierowe, jak i elektroniczne

mu oraz opisać stosowane metody i środki uwierzytelnienia związane z zarządzaniem i użytkowaniem (np. procedury tworzenia i przyznawania haseł użytkownikom). Ważne jest także opisanie, jak tworzone są kopie zapasowe zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, a także miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

Instrukcja zarządzania systemem informatycznym powinna obejmować również informację, w jaki sposób zabezpieczono system informatyczny przed działalnością oprogramo-

Polityka bezpieczeństwa danych

wania szkodliwego, a także wskazywać procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. W instrukcji zarządzania systemem informatycznym powinny być także

określone procedury wykonywania kopii zapasowych oraz sposób zabezpieczenia oprogramowania przed ingerencją osób trzecich, atakiem hakerskim, złośliwymi wirusami (np. poprzez firewall).

Zastosowane zabezpieczenia w systemie informatycznym służącym do przetwarzania danych osobowych administrator danych powinien opisać w specjalnej dokumentacji zwanej instrukcją zarządzania systemem informatycznym.

Przechowywanie e-dokumentacji

Wymagania dotyczące przechowywania dokumentacji prowadzonej w postaci elektronicznej określone zostały w rozdziale 8 rozporządzenia ministra zdrowia z 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania (§ 80–86). Przykładowo, zgodnie z § 80 tego rozporządzenia, dokumentacja może być prowadzona w postaci elektronicznej, pod warunkiem sporządzania jej w systemie teleinformatycznym zapewniającym:

- 1) zabezpieczenie dokumentacji przed uszkodzeniem lub utratą,
- 2) zachowanie integralności i wiarygodności dokumentacji,
- 3) stały dostęp do dokumentacji dla osób uprawnionych oraz zabezpieczenie przed dostępem osób nieuprawnionych,
- 4) identyfikację osoby dokonującej wpisu oraz osoby udzielającej świadczeń zdrowotnych i dokonywanych przez te osoby zmian,
- 5) udostępnienie, w tym przez eksport w postaci elektronicznej dokumentacji albo części dokumentacji będącej formą dokumentacji określonej w rozporządzeniu, w formacie XML i PDF,
- 6) eksport całości danych w formacie XML, w sposób zapewniający możliwość odtworzenia tej dokumentacji w innym systemie teleinformatycznym,
- 7) wydrukowanie dokumentacji w formach określonych w rozporządzeniu.

Jeśli dane przetwarzane w zbiorze udostępnia się innym podmiotom za pomocą systemu informatycznego (teletransmisja danych), to w instrukcji powinien być opisany sposób takiego przepływu danych. Podstawowym wymogiem jest wówczas zabezpieczenie informacji przesyłanych drogą teletransmisji przed udostępnieniem ich osobom nieuprawnionym oraz przed utratą, uszkodzeniem lub zniszczeniem. W przypadku gdy przetwarzający dane wykorzystuje przenośne urządzenia zawierające dane osobowe (np. laptop, pendrive), to jest zobowiązany do szyfrowania tych danych. Wracamy więc do zagadnienia szyfrowania danych, które będzie głównym zadaniem każdego lekarza. Najprostszym sposobem jest zaś użycie loginu i odpowiednio skomplikowanego hasła dostępu.



Urządzenia mobilne zawierające dane muszą być szyfrowane

**Biuro Generalnego Inspektora Ochrony
Danych Osobowych**