NUMER SPECJALNY
PAŹDZIERNIK 2021 | **NR 13/2021**
ISSN 2719-3799

Masz pytania związane z COVID-19? Zostaw wiadomość e-mailową **ekspertowi** – *szczegóły str. 2*

GABINET STOMATOLOGICZNY

PRAWO I PRAKTYKA

Bezpieczeństwo cyfrowych danych medycznych – porady, instrukcje, listy kontrolne

Regularna ocena zabezpieczeń

Bezpieczeństwo serwerów

Szyfrowanie wiadomości – fakty i mity

Oprogramowanie potrzebne do teleporady

Twój prezent:
JAK ZABEZPIECZYĆ DOKUMENTACJĘ MEDYCZNĄ – 6 WSKAZÓWEK

Wydanie online i wzory dokumentów do pobrania znajdziesz na: **stomatologiawpraktyce**.pl

SERWIS ZOZ.PL

ZARZĄDZANIE W OCHRONIE ZDROWIA

NOWOŚĆ! BEZPIECZEŃSTWO EPIDEMIOLOGICZNE I PROCEDURY

Zarządzaj placówką efektywnie i skutecznie

BEZPŁATNE KONTO TESTOWE

na SerwisZOZ.pl 24h/7 do pełnych zasobów portalu!

Możesz z niego korzystać na swoim laptopie, tablecie czy telefonie

- **wideo porady naszych ekspertów**
- **nielimitowany dostęp do 3000 porad ekspertów**
- **aktualne informacje o zmianach w przepisach i alert prawny**
- **400 wzorów dokumentów**

- **3 pytania do eksperta na e-mail w każdym miesiącu**
- **co miesiąc nowy top temat i e-booki do pobrania**
- **bezpłatny udział w cyklicznych Spotkaniach Menedżerów Ochrony Zdrowia**

Jesteś zainteresowany płatną subskrypcją? Zadzwoń do nas lub napisz e-mail.

Nasi konsultanci dopasują najlepszą ofertę dla Ciebie.

SerwisZOZ.pl dostępny jest 24h/7 dni w tygodniu na laptopie, telefonie i tablecie.

Korzystaj wygodnie z wiedzy gdziekolwiek jesteś!

Zamówienia przyjmuje Centrum Obsługi Klienta: 22 518 29 29, e-mail: cok@wip.pl.

BEZPIECZEŃSTWO CYFROWYCH DANYCH MEDYCZNYCH

W tym numerze:

Dokumenty

Plan całodobowego zabezpieczenia dokumentacji medycznej

Lista kontrolna: 5 elementów do sprawdzenia w elektronicznej dokumentacji medycznej

Lista kontrolna: Jakie zabezpieczenia stosujesz dla elektronicznych nośników informacji

Lista kontrolna: Jak zabezpieczyć dane przekazywane za pośrednictwem poczty elektronicznej

Arkusz ewidencji sprzętu komputerowego i oprogramowania

OCHRONA DANYCH OSOBOWYCH

Dodatkowe materiały na stomatologiawpraktyce.pl

GABINET STOMATOLOGICZNY PRAWO I PRAKTYKA

Wiedza i Praktyka sp. z o.o., ul. Łotewska 9A, 03-918 Warszawa, NIP. 526-19-92-256
Kierownik grupy tematycznej: Alina Sulgostowska
Menedżer produktu: Aleksandra Świder
Redaktor: Renata Kajewska
Koordynacja produkcji: Mariusz Jezierski, Magdalena Huta
Korekta: Anna Marecka
Skład i łamanie: Triograf, Dariusz Kołacz
Drukarnia: KRM Druk Sp. z o.o., Sp. k.
Nakład: 350 egz. **ISSN: 2719-3799**
BDO: 000008579
E-mail do redakcji: stomatologia@wip.pl

Informacje o prenumeracie:
tel.: 22 518 29 29, faks: 22 617 60 10, e-mail: cok@wip.pl
Czynne pon.–pt.: w godz. 8.00–16.00
Poza godzinami pracy można pozostawić wiadomość na skrzynce głosowej

Szanowny Czytelniku!

Niewłaściwe sprawdzanie wdrożonych rozwiązań może skutkować administracyjną karą pieniężną nałożoną przez Urząd Ochrony Danych Osobowych. Z tego względu należy pamiętać, iż regularne testowanie i ocena zabezpieczeń funkcjonujących w gabinecie są niezwykle istotne. Szczególnie ma to znaczenie dla przetwarzania danych osobowych cyfrowo, np. na potrzeby elektronicznej dokumentacji medycznej.

Dlatego w najnowszym wydaniu magazynu „Gabinet stomatologiczny – Prawo i praktyka" eksperci opisują zagadnienia dotyczące m.in. bezpieczeństwa cyfrowych danych medycznych oraz weryfikacji zabezpieczeń. Nasi eksperci wskażą m.in.:

- na co w szczególności musisz uważać w zakresie bezpieczeństwa cyfrowych danych medycznych,
- jakie czynności musi wykonywać administrator danych osobowych w ramach regularnego testowania zabezpieczeń,
- jakie przesłanki zastosował UODO, nakładając karę za brak regularnego testowania,
- jaka jest odpowiedzialność za wygaśnięcie zdalnej ochrony oprogramowania.

Ponadto proponuję zapoznać się z wzorami dokumentów opublikowanymi w tym numerze specjalnym czasopisma, takimi jak:

- Plan całodobowego zabezpieczenia dokumentacji medycznej,
- Lista kontrolna: 5 elementów do sprawdzenia w elektronicznej dokumentacji medycznej,
- Lista kontrolna: Jakie zabezpieczenia stosujesz dla elektronicznych nośników informacji,
- Lista kontrolna: Jak zabezpieczyć dane przekazywane za pośrednictwem poczty elektronicznej.

Anna Śmigulska-Wojciechowska
redaktor prowadząca
stomatologia@wip.pl

PS Jeśli masz problem prawny związany np. z wprowadzeniem e-dokumentacji lub funkcjonowaniem w czasie epidemii, skonsultuj go z naszym ekspertem. Wyślij pytania na adres redakcji: stomatologia@wip.pl. Każdemu Czytelnikowi przekażemy gotowe rozwiązanie.

Regularna ocena zabezpieczeń jako permanentny obowiązek gabinetu

MACIEJ LIPKA
specjalista w zakresie prawa medycznego

Wszystkie podmioty wykonały ciężką pracę polegającą na dostosowaniu przetwarzania danych osobowych do przepisów ogólnego rozporządzenia o ochronie danych (RODO). Niemniej jednak faktu dostosowania do RODO nie można po prostu „odhaczyć", gdyż jego przepisy wymagają naszej stałej czujności. Pierwsze interpretacje wskazują, że można naruszyć przepisy wskutek niewłaściwego doglądania wdrożonych rozwiązań.

W artykule 32 RODO wspomniano o „regularnym testowaniu, mierzeniu i ocenianiu skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania". Jak często zatem należy przeprowadzać owe „regularne" przeglądy i czy jest to obowiązkowe, ponieważ RODO wymieniło ww. „regularne testowanie" jedynie jako przykład?

Przepisy nie wskazują bezpośrednio na określone terminy sprawdzania skuteczności zabezpieczeń. Stosownych przeglądów musimy dokonywać zarówno w wyznaczonych przez siebie, regularnych i rozsądnych (dopasowanych do naszej specyfiki) odstępach czasu, jak i zawsze, gdy zajdzie podejrzenie, że dane osobowe są zagrożone. Jednocześnie regularne sprawdzanie zabezpieczeń powinniśmy traktować jako nasz obowiązek.

Regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych to jeden ze środków mający na celu zabezpieczenie danych osobowych. Niemniej jedna, nie możemy tego środka traktować swobodnie, ponieważ jego niezastosowanie naraża nas na zarzut naruszenia przepisów.

Dlaczego regularne testowanie to obowiązek

Jeżeli chodzi o zabezpieczenie danych osobowych, to zgodnie z art. 32 ust. 1 RODO administrator danych osobowych (ADO) i podmiot przetwarzający (procesor) muszą wdrażać odpowiednie środki techniczne i organizacyjne przy uwzględnieniu:

- stanu wiedzy technicznej;
- kosztów wdrażania;
- charakteru, zakresu, kontekstu i celów przetwarzania oraz
- ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

ADO i procesor muszą tego dokonać/dokonywać, aby zapewnić stopień bezpieczeństwa odpowiadający wspomnianemu ryzyku naruszenia praw lub wolności.

RODO nie wyjaśnia, jak dokładnie temu sprostać, a jego zapisy ograniczają się do wskazania, że „w stosownym przypadku" należy zapewnić m.in. „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania".

Wspomniane regularne testowanie wymienia art. 32 ust. 1 lit. d RODO. Jeżeli spojrzymy na ogólne zasady dotyczące przetwarzania danych osobowych, ujrzymy powyższy środek zabezpieczający w innym świetle. Otóż:

- zgodnie z art. 5 ust. 1 lit. f RODO dane osobowe należy przetwarzać w sposób zapewniający odpowiednie ich bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypad-

kową utratą, zniszczeniem lub uszkodzeniem, za pomocą „odpowiednich" środków technicznych lub organizacyjnych;
- zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO) ADO odpowiada za przestrzeganie m.in. powyższej zasady i musi być w stanie wykazać, że jej przestrzega.

WAŻNE

Bez faktycznego wdrożenia procedur testowania, mierzenia i oceny zabezpieczeń nie odpowiemy na pytanie, czy dane osobowe zabezpieczamy w sposób ciągły. Nie możemy wówczas również udowodnić, że to sprawdziliśmy.

Dlatego też regularne testowanie, mierzenie i ocenianie skuteczności zabezpieczeń należy traktować jako obowiązek placówki medycznej. Co więcej, fakt regularnej weryfikacji zabezpieczeń musimy móc udowodnić, np. sporządzając odpowiednie raporty.

Co oznacza termin „regularne"?

Nie można wskazać bezpiecznych odstępów czasu pomiędzy dokonywaniem regularnego testowania wdrożonych środków bezpieczeństwa. Wszystko bowiem zależy od sytuacji indywidualnej placówki, od rodzaju i ilości przetwarzanych danych, a także od infrastruktury, w której się poruszamy. Dlatego też najrozsądniej wyznaczyć sobie arbitralnie regularne terminy, w których będziemy dokonywać sprawdzeń.

Punktem wyjścia powinna być procedura (lub jej fragment), w której wskażemy, co i jak często sprawdzać.

PRZYKŁAD

Gabinet ustala, że stan techniczny pomieszczenia serwerowni będzie sprawdzać co rok, natomiast zabezpieczenia związane z oprogramowaniem do przechowywania dokumentacji medycznej będą podlegać regularnym, comiesięcznym przeglądom.

Niemniej jednak każda procedura powinna przewidywać:

- niezwłoczne dokonanie przeglądu zabezpieczeń na wypadek zdarzeń nagłych (np. powzięciu informacji o rezygnacji dostawcy oprogramowania z czuwania nad jego bezpieczeństwem);
- sposób informowania o podejrzeniu nieprawidłowości (np. postępowanie personelu w przypadku podejrzenia nieprawidłowości i związane z tym zgłaszanie ich przełożonym lub określonej komórce ADO).

PRZYKŁAD

Zapis procedury:
„Przegląd zabezpieczeń dokumentacji medycznej jest również dokonywany niezwłocznie po powzięciu informacji, z których wynika, że zabezpieczenia mogą być nieskuteczne. Źródłem takich informacji mogą być np. doniesienia:
a) z mediów lub z innych źródeł o atakach hakerskich na używane w placówce oprogramowanie;
b) z mediów lub z innych źródeł o tym, że dane osobowe przetwarzane w placówce znalazły się w posiadaniu osób nieuprawnionych;
c) o katastrofach naturalnych, takich jak pożar czy zalanie;
d) (…)

Powyższy obowiązek rodzi zatem konieczność przeprowadzenia szkoleń wśród personelu i udokumentowania faktu, że personel zapoznał się z procedurami bezpieczeństwa.

Czynności w ramach regularnego testowania zabezpieczeń

Powstaje też pytanie, na jakich czynnościach ma właściwie polegać „regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania". Oczywiście dokładne definiowanie wszystkich pojęć występujących w RODO mija się z celem, zwłaszcza że ten akt prawny ma z założenia dawać autonomię przy doborze zabezpieczeń.

Warto zatem przytoczyć zakres czynności, jakie placówka medyczna najczęściej powinna podejmować przy regularnym sprawdzaniu istniejących zabezpieczeń danych osobowych. Będą to zatem zwłaszcza: