ZnanyLekarz

60 PYTAŃ I ODPOWIEDZI EKSPERTA DOT.

RODO

Eksperckich odpowiedzi na pytania o RODO udzielił adwokat Łukasz Łyczkowski. Zapraszamy do lektury!

Odpowiedzi padły podczas webinaru z RODO. Udzielone odpowiedzi mają charakter ogólny i oparte zostały o przepisy RODO i innych aktów prawnych. Przed udzieleniem odpowiedzi nie weryfikowano stanu faktycznego, który może mieć wpływ na sposób stosowania poszczególnych przepisów oraz na treść udzielonej odpowiedzi. Odpowiedzi nie mogą być rozumiane jako wyczerpujące dany problem lub zagadnienie oraz nie mogą stanowić jedynej podstawy do stosowania przepisów RODO czy innych przepisów o ochronie danych osobowych. Odpowiedzi nie stanowią również porady prawnej, a jakakolwiek odpowiedzialność ZnanyLekarz lub adwokata udzielającego odpowiedzi jest wyłączona. Stan prawny aktualny na dzie 31 maja 2018 r. (chyba, że zaznaczono inaczej).

1. Jak informować pacjenta o przetwarzaniu danych osobowych? Przy każdej rejestracji do gabinetu? Można to zrobić przy pierwszej wizycie lub podczas zapisu do lekarza? Generalnie: czy za każdym razem trzeba informować danego pacjenta o przetwarzaniu jego danych?

Nie, nie trzeba przy każdej wizycie informować pacjenta o przetwarzaniu danych osobowych, natomiast trzeba poinformować nowych pacjentów i upewnić się, że dotychczasowi pacjenci zostaną poinformowani przy pierwszej wizycie po wejściu w życie RODO. Oczywiście można odznaczyć w systemie, że pacjent został poinformowany o przetwarzaniu danych osobowych i jeżeli już raz został poinformowany i nic się w zakresie państwa działalności, na przykład państwa danych rejestrowych, nie zmieniło, to kolejny raz tego pacjenta nie trzeba informować. Problematyczna jest tylko sytuacja, gdy pacjent podaje swoje dane przez telefon i trzeba je zapisać. Wtedy należy spełnić obowiązek informacyjny przez telefon. W tym aspekcie pomoże nasze rozwiązanie - ZnanyLekarz Phone, które pomaga zarządzać recepcją i połączeniami przychodzącymi w placówkach medycznych. Pewnym rozwiązaniem jest również proponowane przez ZnanyLekarz.pl umawianie pacjentów przez TeleRejestrację - tam obowiązek informacyjny będzie spełniony odpowiednio, a przetwarzanie danych osobowych w tym zakresie będzie legalne. To samo dotyczy kwestii danych osobowych w systemach dla lekarzy oraz placówek medycznych, które oferuje ZnanyLekarz - są zabezpieczone na wysokim poziomie.

2. Jak prosić pacjentów z poczekalni? Wyczytywanie nazwisk odpada, a więc...?

Ta kwestia nie jest uregulowana wprost. Wydaje się, że najlepszym rozwiązaniem jest zaproszenie pacjenta do gabinetu z użyciem jego imienia.

3. Czy należy zbierać od pacjentów potwierdzenie dopełnienia obowiązku informacyjnego? Jakie mogą być konsekwencje niedopełnienia tego obowiązku?

Tak, należy zbierać od pacjentów potwierdzenia dopełnienia obowiązku informacyjnego. Prowadząc wywiad medyczny o przeciwwskazaniach do przeprowadzenia zabiegu zbieracie państwo takie informacje. Na tym samym dokumencie można spełnić obowiązek informacyjny, a jednocześnie pacjent wypełniając formularz o przeciwwskazaniach będzie mógł pokwitować otrzymanie obowiązku informacyjnego. Na wszelkiego rodzaju innych kartach czy potwierdzeniach zarejestrowania na zabieg również można ten obowiązek informacyjny przekazywać i prosić o potwierdzenie. Jakie są konsekwencje niedopełnienia tego obowiązku? Dwojakiego rodzaju. W przypadku ewentualnej kontroli, która może się pojawić w gabinecie z PUODO, czyli od Prezesa Urzędu Danych Osobowych, niestety mogą być wymierzone kary pieniężne. Druga kwestia to możliwość złożenia skargi przez samego pacjenta, że obowiązek informacyjny nie został dopełniony.

4. Czy pracownik gabinetu może być inspektorem ochrony danych, jeżeli nie ma wykształcenia prawniczego? Czy RODO wymaga osadzenia w tej roli osoby zajmującej się działalnością prawną na co dzień?

Może, jak najbardziej. Brak wykształcenia prawniczego nie musi być przeszkodą. Prawnik nie sprawdzi raczej, jak zabezpieczane są dane w systemach informatycznych, może zabraknąć mu kompetencji. Posiadają je raczej osoby, które się zajmują szeroko rozumianym bezpieczeństwem informacji lub mają doświadczenie związane z sieciami informatycznymi. To jest chyba nawet lepszy profil, niż profil prawniczy. Ważne, żeby mieć wiedzę, w jaki sposób te dane osobowe są wykorzystywane i jak je najlepiej zabezpieczać. Inspektor musi mieć wiedzę o stosowaniu RODO, czyli tak naprawdę tego konkretnego aktu prawnego. Gdyby miał pojęcie o obowiązkach lekarza wynikających z ustaw sektorowych, czyli działalności leczniczej, prawach pacjenta czy samym zawodzie lekarza - to oczywiście byłoby bardzo dobre. Natomiast na pewno nie ma wymogu posiadania wykształcenia prawniczego.

5. Czy są jakieś ograniczenia co do tego, kto może być inspektorem ochrony danych osobowych?

Nie ma ograniczeń. Wystarczy, że ta osoba ma wiedzę i praktykę w zakresie ochrony danych osobowych. Czy ma wykształcenie prawnicze, czy informatyczne - nie ma znaczenia, byłoby jednak rekomendowane, żeby miała szeroko rozumiane wykształcenie albo wiedzę na temat ochrony informacji.

6. Jak informować pacjenta o przetwarzaniu danych osobowych, jeżeli rejestracja odbywa się za pomocą portalu ZnanyLekarz.pl?

Tutaj to ZnanyLekarz.pl, jako portal, który zbiera dane pacjentów i przekazuje je państwu, będzie samodzielnie informował o tym, że dane osobowe są wykorzystywane i przekazywane państwu. Więc obowiązek informacyjny zostanie dopełniany przez sam portal. Natomiast po otrzymaniu danych osobowych od portalu ZnanyLekarz.pl, już podczas wizyty pacjenta w gabinecie, też powinniście państwo ten obowiązek informacyjny spełnić. Można się jednak zastanowić, czy informację, którą my przekazujemy odnośnie przetwarzania danych osobowych i ich udostępnienia Państwu nie będzie wystarczająca w świetle art. 14 ust. 5 RODO.

7. Jak wygląda sprawa z dietetykami? Czy muszą zbierać zgody na przetwarzanie danych osobowych, w tym wrażliwych i biometrycznych? Czy wystarczy, że jest to konieczne do spełnienia umowy z pacjentem?

W zakresie świadczenia usług dietetycznych podstawą prawną do przetwarzania danych osobowych jest rzeczywiście umowa zawierana z pacjentem. Natomiast w zakresie danych wrażliwych czy biometrycznych najlepiej uzyskać dodatkowo zgodę na przetwarzanie danych o stanie zdrowia.

8. Jaki zakres obowiązków jest wymagany w przypadku praktyki prywatnej obejmującej tylko kilku pacjentów w miesiącu? Czy wtedy też wyznaczany jest administrator i inspektor danych osobowych?

Wszystkie obowiązki wynikające z RODO, w szczególności obowiązki informacyjne, są w 100% stosowane dla takiego podmiotu. Nie ma znaczenia, czy państwo macie jednego pacjenta, czy dwóch, czy tysiące. Skala działalności może mieć znaczenie dla obowiązku wyznaczenia inspektora danych osobowych. Jeżeli państwo prowadzicie działalność na dużą skalę, pojawia się obowiązek wyznaczenia inspektora danych osobowych. Natomiast nie trzeba wyznaczać administratora. Z uwagi na fakt, że państwo przetwarzacie te dane osobowe w ramach swojej działalności zawodowej, sami jesteście administratorem danych osobowych. Nie trzeba określać się mianem administratora - realizując działania związane z przetwarzaniem danych osobowych po prostu spełnia się automatycznie tę definicję.

9. Czy obowiązki informacyjne można spełniać ustnie?

Można, natomiast problem ze spełnianiem obowiązków informacyjnych ustnie jest taki, że potem trudno je udowodnić. RODO wprowadza tak zwaną zasadę rozliczalności, czyli nic innego, jak konieczność udowodnienia, że obowiązki zostały spełnione. Jeżeli nie jest to zrobione w sposób pisemny czy elektroniczny poprzez stronę internetową, fakt wykazania, że obowiązek informacyjny został spełniony, może być problematyczny. Dlatego ustne przekazanie informacji nie zawsze jest właściwe.

10. Czy i w jaki sposób pacjent potwierdza, że został poinformowany o ochronie jego danych osobowych?

Najlepiej na piśmie bądź w formie elektronicznej, kwitując swoim podpisem.

11. Co w przypadku serwerów hostowanych przez firmy zewnętrzne, zwłaszcza działające poza Unią Europejską? Czy wówczas komunikacja z pacjentem jest w świetle prawa legalna?

Trzeba sprawdzić czy serwer, który jest poza Unią Europejską, albo dostawca, który państwu ten serwer zapewnia, zobowiązał się do stosowania przepisów RODO. Gorzej jest, jeżeli dostawca serwera, poczty bądź systemu informatycznego nie jest z Unii Europejskiej, a na przykład z Chin bądź z innego państwa, powiedzmy, wątpliwego pod względem ochrony. Czy będzie to legalne? Pewnie przetwarzanie danych medycznych na takich serwerach nie będzie legalne.

12. Jak rozumieć skalę działalności? 1000 pacjentów rocznie, około 5000 w bazie - czy to jest duża, czy mała skala działalności?

Niestety, to jest określane płynnie i decydujące słowo w tym zakresie będzie miał urzędnik, który przyjdzie na kontrolę. W związku z tym trzeba być ostrożnym w tym zakresie i mieć tak naprawdę z tyłu głowy, że nawet mniejszy gabinet może w świetle prawa przetwarzać dane osobowe na “dużą skalę”. Za przetwarzanie danych rozumie się także przechowywanie danych osobowych pacjentów z minionych lat. Proszę też zauważyć, że przepisy dotyczące inspektora ochrony danych pozwalają pewnym zrzeszeniom podmiotów powołać wspólnego inspektora. Być może inicjatywa w tym zakresie izb lekarskich byłaby właściwa.

13. Wystawiamy pacjentowi fakturę, jego dane osobowe trafiają więc do biura rachunkowego, w domyśle: zewnętrznego. Mogą też być dostępne dla pracowników urzędu skarbowego. Czy pacjent powinien być o tym informowany?

W obowiązku informacyjnym wynikającym z artykułu 13. mamy zapis o kategoriach odbiorców danych osobowych. Istnieją podmioty, które mogą mieć dostęp do państwa danych osobowych. Biuro rachunkowe, które państwa obsługuje księgowo, jak najbardziej jest odbiorcą danych osobowych. W tym zakresie z biurem rachunkowym powinna zostać zawarta umowa dotycząca danych osobowych, która znajduje uzasadnienie czy podstawę prawną w artykule 28. RODO, czyli tak zwana umowa powierzenia danych osobowych. Czy informować o tym, że dane mogą być udostępniane urzędowi skarbowemu? Zgodnie z definicją, urząd skarbowy jako podmiot publiczny nie jest odbiorcą danych osobowych.

14. Co zrobić, jeżeli mam dane, a pacjent nie wyrazi zgody na ich przetwarzanie?

W państwa działalności, jeżeli jesteście państwo lekarzami bądź lekarzami dentystami, zgoda na przetwarzanie danych osobowych nie jest wymagana, bo nie stanowi podstawy prawnej do przetwarzania w zakresie prowadzenia działalności leczniczej. Zgoda w państwa działalności najczęściej może mieć podstawę do wykorzystywania danych w szeroko rozumianym marketingu. Natomiast państwa podstawą do przetwarzania danych osobowych najczęściej jest obowiązek, wynikający z przepisów prawa, który mówi, że państwo macie przetwarzać dane osobowe w postaci dokumentacji medycznej, która musi zawierać pewne określone elementy. W związku z tym na państwa jest nałożony obowiązek przetwarzania danych osobowych i w tym zakresie nie musicie państwo uzyskiwać dodatkowej zgody. W artykule 24. ustawy o prawach pacjenta jest wprost napisane: istnieje obowiązek o przetwarzaniu danych osobowych, czyli obowiązek prowadzenia dokumentacji medycznej, w której dane osobowe są w tym zakresie przetwarzane.

15. A jeżeli pacjent zażyczył sobie, by został zapomniany?

To nie jest tak, że pacjent zawsze sobie może zażyczyć, żeby został zapomnianym. Państwo macie obowiązek prowadzenia dokumentacji medycznej i przetwarzania w związku z tym danych osobowych przez określony czas. Wynika to z ustawy o prawach pacjenta i rzeczniku praw pacjenta. Obowiązek nie ustaje nawet po śmierci pacjenta. W związku z tym

pacjent nie może skutecznie wnieść o bycie zapomnianym, jeżeli po Państwa stronie istnieje obowiązek prawny przetwarzania danych.

16. Czy chcąc zrobić pacjentowi zdjęcie przed i po zabiegu musimy również uzyskać na to zgodę?

Pytanie, w jaki sposób i w jakim celu będziecie państwo to zdjęcie wykorzystywać. Jeżeli do promocji swojego gabinetu i swojej działalności, a twarz fotografowanego będzie widoczna i rozpoznawalna, to jak najbardziej zgoda powinna być pozyskana. Ale jeżeli jest to na przykład zdjęcie tylko nogi bądź pleców, bądź innej części ciała, na podstawie których się nie da zidentyfikować tej osoby, to zgoda nie jest wymagana.

17. Czy umowa z zewnętrznym dostawcą usług przechowywania danych zwalnia z odpowiedzialności przed PUODO?

Niestety za wszelkiego rodzaju zaniechania takiego podmiotu, z którym państwo macie zawartą umowę, również ponosicie odpowiedzialność.

18. Jak przechowywać dane posiadane w formie papierowej?

Do tej pory w zakresie kontroli z urzędu, którym było GIODO, zwracano uwagę na to, kto ma dostęp do tych danych i w jaki sposób one są przechowywane: czy leżą w otwartych w szafach, czy te szafy są zamykane, czy są metalowe, ognioodporne, zabezpieczone przed zalaniem i tak dalej. Tutaj sytuacja się nie zmieni, ale tak naprawdę nie ma jednoznacznych wytycznych, w jaki sposób zabezpieczać dane. To państwo musicie ustalić samodzielnie, jak je przechowywać. Czy przechowywanie danych pacjentów w otwartych szafach, czy w segregatorach albo pudłach, do których będzie miało łatwy dostęp wielu pracowników, będzie uznane za prawidłowe? Domyślam się, że nie. W związku z tym kwestia jest do uregulowania po państwa stronie, wewnętrznymi procedurami.

19. Co w przypadku telefonicznej rejestracji? Jeżeli pacjent podaje imię, nazwisko i numer telefonu, to czy pracownik rejestracji powinien odczytywać informacje dotyczące pozyskania danych osobowych czy przetwarzania danych osobowych?

Nie ma w tym zakresie żadnego wyłączenia, chyba że pacjent był wcześniej już poinformowany. Jeżeli pierwszy raz dzwoni i podaje swoje dane osobowe, to niestety należy spełnić obowiązek informacyjny. Praktyką jest jednak odsyłanie do treści obowiązku informacyjnego zamieszczonego na stronie internetowej placówki.

20. Jak wygląda kwestia monitoringu w centrum medycznym, w którym przyjmuję? Czy muszę o tym informować, jeśli tylko wynajmuję lokal?

Kwestia monitoringu przez RODO nie jest uregulowana jednoznacznie. Z pomocą przychodzi Kodeks pracy, który określa zasady stosowania monitoringu (w relacji pracodawca - pracownik). O monitoringu jednak trzeba informować.

21. Jak wygląda kwestia zgody pacjenta na wykonanie zdjęcia twarzy w leczeniu ortodontycznym przed i po leczeniu?

Zależy, do czego zostanie wykorzystane. Jeżeli ma być pokazywane jako dowód skuteczności lekarza i jakości świadczonych usług, to kwestia zgody na przetwarzanie danych osobowych w tym celu od pacjenta jest konieczna - zastosowanie zdjęcia wykracza bowiem poza obowiązki wynikające z prowadzenia dokumentacji czy świadczenia usług medycznych.

22. Co w momencie, gdy pacjent nie potwierdzi przekazania obowiązku informacyjnego? Czy mam go przyjąć, skoro przetwarzanie danych wynika z ustawy? Może mi potem zarzucić, że nie został poinformowany, kto jest administratorem danych i komu dane są przekazywane.

Tutaj zalecałbym naprawdę należytą staranność. Jeżeli państwo informujecie wszystkich swoich pacjentów, że dane są przetwarzane, a ktoś nie chce podpisać potwierdzenia, że uzyskał taką informację, ale jesteście państwo w stanie wykazać, że przekazujecie informację wszystkim pacjentom i tylko jednostkowo ktoś nie chciał podpisać - to nie znaczy, że tej informacji nie mógł uzyskać. To była decyzja pacjenta. Sytuacja wydaje mi się trochę graniczna, natomiast rozumiem, że może to być problematyczne.

23. Jak spełnić obowiązki wynikające z ochrony danych osobowych w sytuacji umieszczenia danych w chmurze, do której dostęp ma kilka osób poprzez bezpośrednie połączenie? Czy dostęp do chmury musi być zabezpieczony hasłem wpisywanym każdorazowo, czy wystarczy zabezpieczenie hasłem komputera?

Lepiej, żeby dostęp do chmury był indywidualnie nadany dla każdego użytkownika tej chmury i żeby każdorazowo osoba, która chce skorzystać z tej chmury się logowała - wtedy przynajmniej pozostanie ślad, kto, co robił. Najczęściej dostawcy rozwiązań chmurowych są na tyle zaawansowani, że nie pozwolą na to, żeby bez logowania dostęp był możliwy.

24. Czy można przy rejestracji telefonicznej nagrywać rozmowy? Prawo na to pozwala?

Nagrywanie jest dozwolone zawsze wtedy, gdy osoba nagrywana wyrazi zgodę na rejestrowanie rozmowy. Aby potwierdzić spełnienie obowiązku informacyjnego przez telefon,

możecie państwo nagrywać rozmowy, tylko musicie o tym poinformować. Gdy ktoś nie wyraża zgody na nagrywanie, to powinien się tak naprawdę rozłączyć.

25. Pojawia się kwestia psychologa. Psycholog nie jest podmiotem medycznym, czy w związku z tym nie ma obowiązku prowadzenia dokumentacji?

Istnieje ustawa o zawodzie psychologa. Nakłada ona obowiązek zachowania w tajemnicy uzyskanych danych pacjentów.

26. Czy na przypomnienie o wizycie kontrolnej w gabinecie lekarskim jest wymagana wcześniejsza zgoda pacjenta?

W mojej ocenie nie jest wymagana zgoda pacjenta na taką komunikację. W interesie pacjenta leży, żeby mu przypomnieć o wizycie, zwłaszcza jeżeli ma to duży wpływ na jego stan zdrowia albo może mieć wpływ na stan zdrowia - bo na przykład kończą mu się leki i trzeba wypisać nową receptę. Komunikacja w tym zakresie, czy to przez SMSa, czy przez maila, czy nawet telefonicznie, jest uzasadniona państwa interesem, żeby jak najlepiej zapewnić bezpieczeństwo pacjentowi i jak najlepiej świadczyć świadczenia zdrowotne.

27. Sprzęt trafia do serwisu, a zawiera dane pacjentów. Co wtedy?

Wtedy firma serwisująca sprzęt powinna mieć zawartą z państwem umowę dotyczącą danych osobowych, opartą o artykuł 28. RODO, która mówi między innymi o tym, że danych nie powinni wykorzystywać w inny sposób, niż tylko w zakresie serwisowania sprzętu, i że powinni zastosować odpowiednie środki między innymi ochraniające dane.

28. Czy można uznać pacjenta za poinformowanego, jeżeli na drzwiach gabinetu będzie informacja o przetwarzaniu danych osobowych, z podaną podstawą prawną?

Tak, zgodnie z ustawą o prawach konsumenta można w ten sposób spełniać obowiązek informacyjny.

29. Jak wygląda komunikacja z pacjentem przez Messengera na Facebooku, czy jest to dopuszczalne?

To jest kwestia bardzo niejednoznaczna. Korzystanie z Facebooka do korespondencji z pacjentem nie powinno mieć miejsca jeżeli zachodzi ryzyko ujawniania danych medycznych pacjenta.

30. Czy informowanie pacjenta o byciu zapomnianym ma w ogóle sens, skoro prawo zobowiązuje lekarza do przechowywania dokumentacji medycznej przez 30 lat?

Niestety, wszystkie te informacje, których RODO wymaga, musicie państwo przekazywać. Nawet w sytuacji, gdy pacjent tak naprawdę nie będzie w stanie takiego prawa wykonać.

31. Czy nie powinniśmy w takim razie informować pacjenta, że nie będzie mógł skutecznie wykonać prawa do bycia zapomnianym?

Niestety, RODO jest regulacją pełną absurdów. Ująłbym to: lepiej powiedzieć, że pacjent ma prawo do bycia zapomnianym, bo przepis tego wymaga, ale jeżeli on rzeczywiście przyjdzie i powie, że chce być zapomnianym, to wówczas poinformować, że macie państwo obowiązek wynikający z przepisów prawa do przetwarzania danych osobowych, w związku z którym nie będzie mógł skutecznie być zapomnianym. Wiem, że to nie brzmi logicznie, ale niestety... w tym zakresie przepisy RODO nie są logiczne.

32. Co w przypadku utraty danych osobowych, na przykład na skutek nieodwracalnego uszkodzenia nośnika pamięci komputera? Kogo informować i o czym?

Jeżeli na tym nośniku danych znajdowała się cała baza i nie było kopii zapasowej, to utraciliście państwo nieodwracalnie dane medyczne. Trzeba wówczas niestety poinformować urząd nadzoru, bo taki jest obowiązek. Trzeba się zgłosić do PUODO, czyli Prezesa Urzędu Ochrony Danych Osobowych z informacją, że taki incydent miał miejsce, w terminie 72 godzin od momentu stwierdzenia utraty danych. Natomiast jeżeli to jest tylko jeden z nośników, na którym są te dane osobowe przechowywane i można je odzyskać, to nie będzie potrzeby informowania PUODO.

33. Czy poinformowanie o incydencie utraty danych wiąże się automatycznie z karą?

Nie umiem odpowiedzieć, nie jestem urzędnikiem Prezesa Urzędu Ochrony Danych Osobowych. Domyślam się, że może to być podstawa do wszczęcia kontroli w tym zakresie, ale czy to się automatycznie wiąże z karą? Niekoniecznie, ale nie potrafię całkowicie wykluczyć takiego ryzyka.

34. Czy dobrym rozwiązaniem jest nagranie komunikatu z oświadczeniem o przetwarzaniu danych w sytuacji, gdy pacjent dzwoni pierwszy raz zarejestrować się na wizytę?

Uważam, że to dobre rozwiązanie.

35. Jak w dokumentacji elektronicznej uzyskać podpis pacjenta o obowiązku informacyjnym?

Jeżeli jest prowadzona dokumentacja elektroniczna, wystarczający będzie nawet checkbox przy oświadczeniu: “Oświadczam, że zostałem poinformowany o przetwarzaniu moich danych osobowych”.

36. Czy trzeba mieć zgodę na korespondencję mailową z pacjentami?

Jeżeli państwo prowadzicie komunikację w zakresie jakiegoś rodzaju marketingu, to tak. Ale jeżeli chodzi o korespondencję związaną z szeroko rozumianą działalnością leczniczą, na przykład informujecie państwo o zarejestrowaniu się na wizytę, to zgoda na korespondencję nie jest konieczna. Trzeba jednak zapewnić, że nikt niepowołany nie uzyska dostępu do tych danych i korespondencji.

37. Czy informacje o przetwarzaniu danych osobowych można umieścić na na stronie internetowej gabinetu?

Na pewno warto mieć taką zakładkę „dane osobowe”. Dzięki temu będziecie państwo mogli wykazać należytą staranność: pacjent, który odwiedza stronę internetową gabinetu, może zawsze się zapoznać z informacją o danych osobowych.

38. Czy można zeskanować podpisane przez pacjenta oświadczenie o byciu poinformowanym i dołączyć je do elektronicznej dokumentacji, a oryginał zniszczyć?

Nie ma obowiązku pisemności w zakresie poinformowania o danych osobowych, o przetwarzaniu danych osobowych. W związku z tym możecie państwo oczywiście zebrać tradycyjne podpisy pacjentów, a potem je zdigitalizować i dołączyć do dokumentacji, zaś oryginał zniszczyć.

39. Jak brak obowiązku pisemności ma się do rozliczalności?

No właśnie kluczowa jest rozliczalność. Potwierdzenia od pacjentów, że zostali poinformowani, mogą mieć formę nagrania rozmowy czy innego zapisu elektronicznego. Mogą być pisemne oczywiście też, ale jeżeli jesteście państwo w stanie inaczej wykazać, że dany pacjent został poinformowany o przetwarzaniu danych, musi to być respektowane.

40. Czy możemy oddzwonić na nieodebrany numer telefonu?

W tym zakresie nic się nie zmienia, czyli możecie państwo oddzwonić na nieodebrany numer telefonu. Proszę zauważyć, że pierwotnie zainteresowanym w komunikacji jest ten dzwoniący.

41. A podpis rejestratorek, że poinformowały danego pacjenta?

Jest to na pewno sposób na udowodnienie, że obowiązek został spełniony - notatka służbowa, że pacjent XYZ został poinformowany o danych osobowych przez danego pracownika w danym dniu. Ułatwi to sytuację, gdy pacjent nie chce się podpisać.

42. Czy nie można poinformować ogólnie społeczeństwa, że lekarze muszą przetwarzać dane pacjentów?

Byłoby to bardzo dobre rozwiązanie, niestety ustawodawca unijny nie jest tak szczodry i nie wyłączył lekarzy z obowiązków informacyjnych. Oczywiście dla każdego rozsądnego człowieka jest jasne, że idąc do lekarza musi podać swoje dane, ale niestety nie zwalnia to z obowiązku informacyjnego.

43. Czy informowanie pacjenta przez telefon lub email o leczeniu jest dopuszczalne?

Problem jest taki, czy jesteście państwo w stanie w stu procentach zidentyfikować, kto do państwa dzwoni i komu te dane przez telefon przekazujecie, żeby nie przekazać danych osobie nieuprawnionej. W kwestii komunikacji przez email też byłbym ostrożny, zwłaszcza, że adres email niekoniecznie musi pokrywać się z tym, którym państwo dysponujecie w swoich bazach. Osoba nieupoważniona nie może mieć dostępu do danych pacjenta.

44. Czy w RODO nie ma już obowiązku zgłaszania zbiorów danych?

Nie ma obowiązku zgłaszania zbioru danych, natomiast być może część z państwa będzie musiała prowadzić tak zwany rejestr czynności przetwarzania, uregulowany w artykule 30. RODO - czyli informacje, co robicie państwo z odpowiednimi danymi osobowymi.

45. Jak wysokie kary przewiduje RODO?

W RODO niestety kary są bardzo wysokie. Maksymalna wysokość kary w przypadku osób prowadzących działalność gospodarczą może wynosić nawet 20 000 000 €. Oczywiście ma to być przeliczane na podstawie średniego kursu NBP na złotówki, a więc obecnie maksymalna kara to powyżej 80 000 000 zł.

46. Gabinet stomatologiczny mieści się w pomieszczeniach szkoły. Dyrektor szkoły dysponuje kluczami do wszystkich pomieszczeń. Czy w związku z tym konieczne jest wprowadzenie do umowy najmu dodatkowych postanowień regulujących ochronę wrażliwych danych przetwarzanych przez gabinet?

Jest to rozwiązanie rekomendowane. Gabinet powinien zadbać, aby pracownicy szkoły nie mieli wglądu do dokumentacji, np. umieszczając dokumentację w zamykanej szafie, do której klucze mają wyłącznie pracownicy gabinetu.

47. Czy jeśli pacjent chce uzyskać fakturę, to w obowiązku informacyjnym powinien być punkt, że jego dane będą przetwarzane przez biuro rachunkowe? Jeśli tak, czy trzeba wpisywać dokładną nazwę i adres biura rachunkowego?

Zgodnie z art. 13 ust. 1 lit e RODO w obowiązku informacyjnym kierowanym do osoby, której dane dotyczą należy wskazać tzw. odbiorców danych osobowych lub kategorie odbiorców. Odbiorcami zgodnie z definicją z art. 4 pkt 9 RODO są wszystkie podmioty, którym ujawnia się dane osobowe, z wyłączeniem podmiotów publicznych prowadzących przewidziane prawem postępowania. W związku z powyższym, firma księgowa jest uznawana za odbiorcę danych osobowych. Fakt przekazywania danych osobowych temu podmiotowi powinien być uwzględniony w obowiązku informacyjnym. Proszę zwrócić uwagę, że przywołany art. 13 ust. 1 lit. E mówi o "kategoriach odbiorców", więc nie ma konieczności przekazywania pełnej nazwy biura księgowego. Można poprzestać na stwierdzeniu, że dane osobowe mogą być ujawniane firmom księgowym. Z firmą księgową należy zawrzeć umowę powierzenia przetwarzania danych osobowych zgodną z art. 28 RODO.

48. Jeśli na stronie internetowej jest kalendarz kontaktowy, czy wymagana jest umowa z firmą udostępniającą serwer na przetwarzanie danych osobowych?

Tak. Umowa powinna odpowiadać warunkom formalnym z art. 28 RODO.

49. Czy należy zawierać umowę z księgową o przetwarzaniu danych osobowych?

Tak. Umowa powinna odpowiadać warunkom formalnym z art. 28 RODO.

50. Czy dopuszczalna jest sytuacja, w której na wizytę jedziemy do domu pacjenta, tam tworzymy papierowe notatki i później wieziemy je ze sobą?

RODO nie wprowadza zmian w tej kwestii. Jeżeli dane będą odpowiednio zabezpieczone, to nie powinno to stanowić ryzyka dla lekarza.

51. Czy powinniśmy mieć np. jakąś teczkę, w której będą się znajdować oświadczenia o zgodzie na przetwarzanie danych, umowy o przetwarzaniu danych, sposobach zabezpieczenia danych papierowych i elektronicznych. Czy coś jeszcze powinno się znaleźć w takiej teczce?

W takiej dokumentacji powinny być upoważnienia do przetwarzania danych wydane na podstawie art. 29 RODO i podpisane przez pracowników. RODO nie przewiduje wzorów konkretnych dokumentów jakie mają się znaleźć w takiej przykładowej teczce.

52. Program, który posiadam do opracowania jadłospisu działa online. Czy w związku z tym mam np. zaszyfrować pacjenta, czy uzyskać od firmy informację, że dane są bezpieczne?

Jeżeli program te przetwarza dane pacjentów, to powinna zostać zawarta umowa dot. danych osobowych zgodna z art. 28 RODO.

53. Jeżeli przyjmuje pacjenta na wizycie domowej, to wystarczy poinformować, że dane będą przechowywane w określonym miejscu?

Nie. Informuje się o tym kto dane wykorzystuje i w jakim celu. Nie trzeba informować o miejscu przetwarzania danych - podstawa art. 13 RODO.

54. Jak RODO ma się do pracy psychoterapeuty? Psychoterapeuta uzależnień i psycholog formalnie nie są psychoterapeutami – ten zawód nie ma regulacji, jest wyszczególniony jedynie w NFZ, a więc regulacje te nie dotyczą osób niewspółpracujących z NFZ.

W przypadku psychoterapeutów, którzy są również psychologami: w ustawie o zawodzie psychologa nie ma wymogu prowadzenia dokumentacji, jej przechowywania i udostępniania, a kwestie zapisy dotyczące danych osobowych dotyczy dobrowolności i szczególnych okoliczności udostępniania danych wrażliwych np. wyników badań. Wychodzi więc na to, że jesteśmy zwykłymi podmiotami usługowymi, z tym że przetwarzamy dane wrażliwe.

55. Ile trwa okres przechowywania danych? Czy za podstawę należy przyjąć Kodeks cywilny?

Tam termin przedawnienia wynosi lat dziesięć, a dla roszczeń o świadczenia okresowe oraz roszczeń związanych z prowadzeniem działalności gospodarczej – trzy lata. W przypadku konieczności przechowywania dokumentacji medycznej pacjenta okres obowiązkowy jej przechowywania wynika z ustawy o prawach pacjenta i Rzeczniku praw pacjenta. Istnieją wyjątki dotyczące głównie zdjęć rentgenowskich i skierowań.

56. W gabinetach terapeutycznych nie ma zwyczaju podpisywania umów na usługę psychoterapii. Czy powinniśmy mieć takie umowy? Czy wystarczy zgoda na przetwarzanie danych?

Fakt, że umowa nie zostaje spisana na papierze, nie powoduje, że w obrocie prawnym jej nie ma. Innymi słowy, nie trzeba zawsze zawierać papierowej umowy, żeby z prawnego punktu widzenia do umowy doszło. Zgoda na przetwarzanie danych nie będzie potrzebna, bo wystarczająca jest ustna umowa z pacjentem. W obowiązku informacyjnym z art. 13 RODO należy wskazać, że podstawą prawną jest właśnie taka umowa ustna z pacjentem.

57. Czy żona, będąca lekarzem, może w jednoosobowym gabinecie upoważnić męża jako osobę do kontaktu w zakresie telefonicznej rejestracji, udzielania telefonicznej informacji o cenniku i zakresie usług oraz spełnienia obowiązku informacyjnego przez ADO przy telefonicznej rejestracji nowych pacjentek?

Nie ma ku temu przeciwskazań prawnych. Ważne, żeby upoważniony, czyli w tym wypadku mąż, miał nadane upoważnienie do przetwarzania danych osobowych (podstawa prawna: art. 29 RODO).

58. Jak rozumieć zapis, że zanim przekażę dane osobowe firmie zewnętrznej powinienem jako ADO ją sprawdzić? Jak postąpić z umowami już zawartymi?

Dotychczasowe umowy z podmiotami zewnętrznymi powinny być aneksowane i dostosowane do art. 28 RODO, który faktycznie przewiduje możliwość sprawdzenia takiego podmiotu.

59. Czy po 25.05.2018 będzie można samodzielnie wpisać nazwisko pacjenta w internetowym kalendarzu w ZnanyLekarz.pl? Starszy pacjent dzwoni do mnie i prosi o zapisanie go na wizytę, sam nie korzysta z Internetu.

Tak. Zarówno obecnie obowiązujące umowy ze ZnanyLekarz,.pl jak i zmiany do tych umów, które państwu proponujemy, uzasadniają i legalizują takie działanie. Umowy regulujące dopisywanie pacjentów do Kalendarza Wizyt, które proponujemy są zgodne z art. 28 RODO. Dzięki temu możecie państwo bez problemu zapisywać pacjentów do Kalendarza Wizyt. W tym zakresie ZnanyLekarz.pl działa na państwa rzecz jako tzw. podmiot przetwarzający.

60. Wymagane jest wskazanie przez pacjenta osoby uprawnionej do otrzymywania informacji. Tej osoby fizycznie nie ma w gabinecie. Co wówczas z RODO?

W takim przypadku dochodzi do tzw. uzyskania danych pośredniego. Innymi słowy, uzyskuje się dane osoby nie od niej samej, ale od innej osoby, np. członka rodziny. Obowiązek informacyjny w stosunku do tej osoby normuje art. 14 RODO. Powinniście więc państwo teoretycznie informować tę osobę o przetwarzaniu jej danych. Jednak art. 14 ust. 5 lit. C wprowadza wyjątek od informowania. W skrócie, wyjątek ten stanowi, że obowiązku informacyjnego nie trzeba w stosunku do tej osoby wykonywać, ponieważ macie państwo obowiązek prawny przetwarzania jej danych.