Dokumentacja medyczna i jednostkowe dane medyczne

miniprzewodnik dla lekarzy po wybranych regulacjach prawnych

Warszawa 2023

wersja 1.0

SPIS TREŚCI

Wykaz używanych skrótów 2

Wprowadzenie 3

1. Czym jest dokumentacja medyczna i jednostkowe dane medyczne? 4
2. Komu mogę udostępniać dokumentację medyczną i jednostkowe dane medyczne? 5
3. Komu mogę udostępniać dokumentację medyczną i jednostkowe dane medyczne po śmierci pacjenta? 8
4. Czym jest tzw. dawstwo danych? 8
5. W jaki sposób mogę udostępniać dokumentację medyczną i jednostkowe dane medyczne? 10
6. W jakim czasie należy udostępnić dokumentację medyczną i jednostkowe dane medyczne? 11
7. Przez jaki czas należy przechowywać dokumentację medyczną i jednostkowe dane medyczne? 12
8. Jak należy zabezpieczyć dokumentację medyczną i jednostkowe dane medyczne? 13
9. Czy dokumentacja medyczna i jednostkowe dane medyczne mogą być wykorzystywane przez sztuczną inteligencję? 15
10. Czym jest anonimizacja i pseudonimizacja danych? 16

WYKAZ UŻYWANYCH SKRÓTÓW

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L 2016 Nr 119, str. 1), dalej jako: „RODO”;
2) Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2009 Nr 52, poz. 417 z późn. zm.), dalej jako: „ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta”;
3) Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 Nr 113, poz. 657 z późn. zm.), dalej jako: „ustawa o systemie informacji w ochronie zdrowia”;
4) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2018 r. poz. 1560 ze zm.), dalej jako: „ustawa o krajowym systemie cyberbezpieczeństwa”;
5) Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. z 2020 r. poz. 666 z późn. zm.), dalej jako: „rozporządzenie Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania”;

Niniejszy miniprzewodnik ma charakter informacyjny. Zawarte w nim zagadnienia zostały przedstawione w podstawowym zarysie w celach edukacyjnych. Przedstawia stan prawny na 12 grudnia 2023 r.

Opracowanie: dr Paweł Kaźmierczyk

Materiał powstał we współpracy z kancelarią Domański Zakrzewski Palinka sp. k.

WPROWADZENIE

Praca lekarza nieodzownie wiąże się z prowadzeniem dokumentacji medycznej. Jak dotąd podstawową formą dokumentowania stanu zdrowia pacjenta i opisu udzielanych mu świadczeń zdrowotnych była forma papierowa. Za sprawą postępującego od lat procesu informatyzacji sektora ochrony zdrowia tradycyjne teczki pacjentów wypierane są przez dokumenty elektroniczne. Coraz więcej danych medycznych przetwarzanych jest w postaci cyfrowej, co rodzi nowe szanse i wyzwania.

Jednym z takich wyzwań jest prowadzenie i udostępnianie dokumentacji medycznej i danych o stanie zdrowia pacjentów zgodnie z przepisami obowiązującego prawa, które nie zawsze są w pełni jasne i czytelne, nawet dla prawników. Tym trudniej odnaleźć się w nich lekarzom, którzy powinni mieć jasność, jak należy postępować z określonymi dokumentami lub zbiorami danych.

Celem tego miniprzewodnika jest przybliżenie lekarzom w możliwie przystępny sposób kluczowych przepisów związanych z obszarem dokumentacji medycznej oraz jednostkowych danych medycznych. Zwracamy w nim także uwagę na wybrane, szczegółowe zagadnienia związane m.in. z anonimizacją i pseudonimizacją danych, wykorzystywaniem danych na potrzeby stosowania sztucznej inteligencji czy możliwości związane z tzw. dawstwem danych. Dokument może być tym bardziej przydatny, że przed nami unijny plan stworzenia wspólnej przestrzeni danych dotyczących zdrowia (European Health Data Space).

Publikacja ma charakter informacyjny, nie stanowi porady prawnej i jej nie zastępuje. Nie wyczerpuje też głównego tematu. Ma stanowić „pierwszą pomoc" dla lekarek i lekarzy w razie wątpliwości związanych z właściwym postępowaniem z danymi medycznymi lub dokumentacją medyczną[1].

Materiał powstał w ramach inicjatywy „NIL IN – Sieć Lekarzy Innowatorów" działającej przy Naczelnej Izbie Lekarskiej.

Partnerem publikacji jest **Sano - Centrum Zindywidualizowanej Medycyny Obliczeniowej - Międzynarodowa Fundacja Badawcza**

sano

Projekt otrzymał dofinansowanie w ramach programu Horyzont 2020 - ramowego programu Komisji Europejskiej w zakresie badań naukowych i innowacji – umowa grantowa nr 857533 oraz z Programu Międzynarodowe Agendy Badawcze Fundacji na rzecz Nauki Polskiej.

Fundusze Europejskie Inteligentny Rozwój | Rzeczpospolita Polska | FNP Fundacja na rzecz Nauki Polskiej | Unia Europejska Europejski Fundusz Rozwoju Regionalnego

[1] W celu uzupełnienia wiedzy zalecamy w pierwszej kolejności objaśnienia prawne z dnia 3 października 2019 r. wydane przez Rzecznika Praw Pacjenta w oparciu o art. 33 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców „Udostępnianie, prowadzenie i przechowywanie dokumentacji medycznej – zagadnienia praktyczne".

1. CZYM JEST DOKUMENTACJA MEDYCZNA I JEDNOSTKOWE DANE MEDYCZNE?

Choć dokumentacja medyczna stanowi nieodzowny element pracy lekarza, a szereg obowiązków zawodowych dotyczy zasad jej prowadzenia, obowiązujące przepisy prawa **nie zawierają definicji dokumentacji medycznej**.

Dla wyznaczenia dokładnego zakresu dokumentów, które stanowią dokumentację medyczną kluczowy jest art. 25 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, który w ust. 1 wskazuje, że **dokumentacja medyczna** zawiera co najmniej:

1) oznaczenie pacjenta, pozwalające na ustalenie jego tożsamości, tj. nazwisko i imię (imiona), datę urodzenia, oznaczenie płci, adres miejsca zamieszkania, numer PESEL (w przypadku noworodka - numer PESEL matki, a w przypadku osób, które nie mają nadanego numeru PESEL - rodzaj i numer dokumentu potwierdzającego tożsamość)[2];

2) oznaczenie podmiotu udzielającego świadczeń zdrowotnych ze wskazaniem komórki organizacyjnej, w której udzielono świadczeń zdrowotnych;

3) opis stanu zdrowia pacjenta lub udzielonych mu świadczeń zdrowotnych;

4) datę sporządzenia.

Dokumenty, które zawierają powyższe elementy, stanowić będą dokumentację medyczną. Tym samym nie wszystkie dokumenty, z którymi spotyka się lekarz w swojej pracy, stanowić będą dokumentację medyczną, np. dokumenty rozliczeniowe z płatnikiem publicznym, skargi i wnioski pacjentów, itp.

Co więcej, szczegółowe rodzaje dokumentów oraz wymogi co do ich zawartości zostały precyzyjnie określone w rozporządzeniu Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania[3]. Co ważne, zgodnie z § 1 ust. 1 przywołanego aktu prawnego, dokumentacja medyczna powinna być prowadzona w postaci elektronicznej[4]. Tym samym to postać elektroniczna jest podstawową postacią prowadzenia dokumentacji medycznej – papierowe dokumenty występują na zasadzie wyjątku od tej reguły, m.in. w sytuacji, gdy warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej.

Szczególnym rodzajem dokumentacji medycznej jest **elektroniczna dokumentacja medyczna**, która została zdefiniowana w art. 2 pkt 6 ustawy o systemie informacji w ochronie zdrowia. Stanowią ją tylko recepty, określone przez Ministra Zdrowia typy dokumentów (np. karta informacyjna z leczenia szpitalnego)[5], określone przez Ministra Zdrowia skierowania[6], zlecenia na zaopatrzenie i zlecenia naprawy wyrobów medycznych, karty szczepień oraz wyniki badania histopatologicznego -

[2] W przypadku gdy pacjentem jest osoba małoletnia, całkowicie ubezwłasnowolniona lub niezdolna do świadomego wyrażenia zgody - nazwisko i imię (imiona) przedstawiciela ustawowego oraz adres jego miejsca zamieszkania.

[3] Nieco odmienne zasady obowiązują w podmiotach leczniczych dla osób pozbawionych wolności oraz utworzonych przez Ministra Obrony Narodowej lub ministra właściwego do spraw wewnętrznych.

[4] Dokumentacja może być prowadzona w postaci papierowej tylko jeżeli przepis przywołanego rozporządzenia tak stanowi lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej.

[5] Pełny katalog określa rozporządzenie Ministra Zdrowia w sprawie rodzajów elektronicznej dokumentacji medycznej.

[6] Pełny katalog określa rozporządzenie Ministra Zdrowia w sprawie skierowań wystawianych w postaci elektronicznej w Systemie Informacji Medycznej.

wytwarzane obowiązkowo w postaci elektronicznej - oraz opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych.

Przepisy prawa posługują się też pojęciem **jednostkowych danych medycznych**, które zostały zdefiniowane w art. 2 pkt 7 ustawy o systemie informacji w ochronie zdrowia jako dane osoby fizycznej o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej oraz dotyczące jej stanu zdrowia, w tym profilaktyki zdrowotnej i realizacji programów zdrowotnych (np. przepisane leki, wyniki badań laboratoryjnych). Tym samym pojęcie danych zostało odróżnione od pojęcia dokumentu, tj. dokumentacja medyczna może zawierać jednostkowe dane medyczne. Podstawowym repozytorium jednostkowych danych medycznych są właśnie dokumenty elektroniczne oraz cyfrowe bazy danych zawierające dane odnoszące się do kolejnych etapów procesu opieki nad pacjentem od momentu rejestracji pacjenta do lekarza. Dzięki temu rozróżnieniu można uzyskać dostęp i wykorzystywać tylko część danych pacjenta bez konieczności uzyskiwania pełnej dokumentacji. Przykładowo, wybrane jednostkowe dane medyczne są raportowane do systemu centralnego w ramach danych zdarzenia medycznego, dzięki temu na ich podstawie inny lekarz ma możliwość zlokalizowania i uzyskania dostępu do innych danych lub pełnej dokumentacji potrzebnej mu do opieki nad pacjentem.

Tym samym lekarz w swojej codziennej pracy będzie miał styczność z dokumentami, których znaczna część stanowić będzie dokumentację medyczną prowadzoną w postaci elektronicznej lub papierowej. Część dokumentacji medycznej prowadzonej w postaci elektronicznej stanowić będzie elektroniczną dokumentację medyczną, np. e-recepty czy e-skierowania. W dokumentach i systemach IT placówek medycznych znajdować się będą jednostkowe dane medyczne (które mogą stanowić zarazem dane osobowe).

2. KOMU MOGĘ UDOSTĘPNIAĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE?

Dokumentacja medyczna i jednostkowe dane medyczne podlegają szczególnej ochronie prawnej. Dostęp do nich pod pewnymi warunkami mogą uzyskać tylko osoby i podmioty określone w przepisach prawa. Za udostępnianie danych i dokumentów odpowiada podmiot wykonujący działalność leczniczą, którym może być osoba prawna, np. szpital lub przychodnia, która zazwyczaj przyjmuje wewnętrzne procedury w tym zakresie i wyznacza osoby odpowiedzialne za udostępnianie. Jeżeli lekarz prowadzi samodzielnie własną praktykę, sam musi jednak pamiętać o poniższych zasadach.

Podstawowy katalog osób i podmiotów, którym należy udostępnić dokumentację medyczną, określa art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Dokumentację udostępnia się samemu pacjentowi lub jego przedstawicielowi ustawowemu, a także osobie upoważnionej przez pacjenta.

Ponadto, dokumentację należy udostępnić innym podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do zapewnienia ciągłości świadczeń zdrowotnych (np. sytuacja, w której pacjent zostaje przeniesiony do innego szpitala).

Przykład: o udostępnienie dokumentacji medycznej prosi daleki kuzyn pacjenta przedstawiając odpis upoważnienia udzielonego mu przez pacjenta, którego oryginał znajduje się jednak

w dokumentacji medycznej w położonym w innym województwie szpitalu, w którym to kilka miesięcy temu leczył się pacjent. Czy lekarz powinien udostępnić dokumentację?

Tak. Jak wskazał m.in. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 15 grudnia 2016 r. (sygn. VII SAB/Wa 19/16), oświadczenie pacjenta o możliwości udostępnienia dokumentacji medycznej osobie najbliższej, złożone również w innej placówce medycznej i nie odwołane w żaden sposób (wyraźny lub dorozumiany) powoduje, że oświadczenie to zachowuje swoją moc również w innych placówkach ochrony zdrowia skoro jest dołączane do karty choroby w ramach indywidualnej dokumentacji pacjenta. Przyjęcie innego rozumowania prowadziłoby do nieakceptowalnych z punktu widzenia wykładni prawa, ale i zasad logicznego rozumowania sytuacji.

Dokumentację medyczną udostępnia się także innym uprawnionym na podstawie przepisów prawa podmiotom – na ich wniosek - w związku z wykonywanymi przez nie zadaniami niezwiązanymi bezpośrednio z procesem opieki zdrowotnej nad pacjentem:

- organom władzy publicznej, w tym Rzecznikowi Praw Pacjenta, Narodowemu Funduszowi Zdrowia, organom samorządu zawodów medycznych oraz konsultantom w ochronie zdrowia, a także Rzecznikowi Praw Pacjenta Szpitala Psychiatrycznego, w zakresie niezbędnym do wykonywania przez te podmioty ich zadań, w szczególności nadzoru i kontroli;
- podmiotom prowadzącym kontrolę podmiotów leczniczych na zlecenie ministra właściwego do spraw zdrowia w zakresie niezbędnym do przeprowadzenia kontroli;
- w przypadku SPZOZ - upoważnionym przez podmiot tworzący osobom wykonującym zawód medyczny, w zakresie niezbędnym do sprawowania nadzoru nad podmiotem leczniczym niebędącym przedsiębiorcą;
- Agencji Oceny Technologii Medycznych i Taryfikacji, w zakresie niezbędnym do wykonywania przez nią jej ustawowych zadań;
- Agencji Badań Medycznych w zakresie określonym ustawą o Agencji Badań Medycznych;
- ministrowi właściwemu do spraw zdrowia, sądom, w tym sądom dyscyplinarnym, prokuraturom, lekarzom sądowym i rzecznikom odpowiedzialności zawodowej, w związku z prowadzonym postępowaniem;
- uprawnionym na mocy ustaw organom i instytucjom, jeżeli badanie zostało przeprowadzone na ich wniosek;
- organom rentowym oraz zespołom do spraw orzekania o niepełnosprawności, w związku z prowadzonym przez nie postępowaniem;
- podmiotom prowadzącym rejestry usług medycznych, w zakresie niezbędnym do prowadzenia rejestrów;
- zakładom ubezpieczeń, ale tylko za zgodą pacjenta;
- komisjom lekarskim podległym ministrowi właściwemu do spraw wewnętrznych, wojskowym komisjom lekarskim oraz komisjom lekarskim Agencji Bezpieczeństwa Wewnętrznego lub Agencji Wywiadu, podległym Szefom właściwych Agencji;

- osobom wykonującym zawód medyczny, w związku z prowadzeniem procedury oceniającej podmiot udzielający świadczeń zdrowotnych na podstawie przepisów o akredytacji w ochronie zdrowia albo procedury uzyskiwania innych certyfikatów jakości, w zakresie niezbędnym do ich przeprowadzenia;
- osobom wykonującym czynności kontrolne względem podmiotów prowadzących bazy danych w zakresie ochrony zdrowia, w zakresie niezbędnym do ich przeprowadzenia;
- członkom zespołów kontroli zakażeń szpitalnych w zakresie niezbędnym do wykonywania ich zadań.

Dokumentacja medyczna może być udostępniona także szkole wyższej lub instytutowi badawczemu do wykorzystania w celach naukowych, bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy (art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta). W związku z tym, zasadniczemu ograniczeniu podlega krąg potencjalnych osób, które mogą uzyskać dokumentację medyczną bez zgody pacjenta na potrzeby prac naukowych. W ten sposób dokumentacji nie uzyska np. prywatny przedsiębiorca, który chce wykorzystać dostępne dane na potrzeby prowadzonego badania klinicznego lub budowania rozwiązania opartego o sztuczną inteligencję. W dalszym ciągu ma on jednak możliwość uzyskania dostępu do dokumentacji na podstawie zgody pacjenta. To rozwiązanie z perspektywy osoby potrzebującej danych w celu naukowym może okazać się trudne ze względów organizacyjnych, np. próba uzyskania zgód od kilkuset pacjentów z terenu całego kraju, lub wręcz niemożliwe w przypadku śmierci pacjenta.

Dodatkowo, na gruncie RODO może nie być jasne, jak rozumieć wymóg przekazania dokumentacji „bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy” w świetle zasad anonimizacji i pseudonimizacji (por. punkt 10). Przedstawić można dwie podstawowe interpretacje:

- możliwości przekazania dotyczy wyłącznie dokumentacji medycznej, która uniemożliwia ustalenie tożsamości pacjenta zarówno odbiorcy, jak również placówce medycznej udostępniającej dane (anonimizacja) – takie rozwiązanie wydaje się jednak niezasadne, jako że podmiot leczniczy nie może utracić danych przetwarzanych w ramach dokumentacji medycznej;
- możliwość przekazania dokumentacji medycznej w formie, która uniemożliwia odbiorcy danych ustalenie tożsamości pacjenta, przy czym tożsamość pacjenta może być potencjalnie ustalona przez placówkę medyczną, która ma dostęp do danych wyjściowych („surowych”). W świetle przepisów RODO będą to więc dane spseudonimizowane, a więc dalej dane osobowe.

Przepis art. 35 ustawy o systemie informacji w ochronie zdrowia przewiduje odmienne zasady udostępniania samych danych osobowych lub jednostkowych danych medycznych pacjentów, które są przetwarzane w systemie teleinformatycznym podmiotu wykonującego działalność leczniczą. W praktyce najczęściej będą to dane zawarte w dokumentach stanowiących elektroniczną dokumentację medyczną (pojęcie to zostało wyjaśnione w poprzednim punkcie). Dostęp do tych danych mają:

- pracownik medyczny, który wytworzył elektroniczną dokumentację medyczną;
- pracownik medyczny wykonujący zawód w placówce, u której została wytworzona elektroniczna dokumentacja medyczna zawierająca dane osobowe lub jednostkowe dane medyczne pacjenta,

w związku z wykonywaniem przez niego zawodu w tej placówce, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia;

- lekarz, pielęgniarka lub położna udzielający usługobiorcy świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej;
- każdy pracownik medyczny w sytuacji zagrożenia życia usługobiorcy.

W innych przypadkach udostępnienie danych osobowych lub jednostkowych danych medycznych następuje wyłącznie za zgodą pacjenta lub jego przedstawiciela ustawowego. Wyrażając zgodę, wskazuje się zakres czasowy i przedmiotowy dostępu do tych danych.

3. KOMU MOGĘ UDOSTĘPNIAĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE PO ŚMIERCI PACJENTA?

Po śmierci pacjenta dokumentacja medyczna powinna zostać udostępniona wyłącznie osobie upoważnionej przez pacjenta jeszcze za życia lub osobie, która w chwili zgonu pacjenta była jego przedstawicielem ustawowym. Dokumentacja medyczna jest udostępniana także osobie bliskiej[7], chyba że udostępnieniu sprzeciwi się inna osoba bliska lub sprzeciwił się temu pacjent za życia.

W przypadku sporu między osobami bliskimi o udostępnienie dokumentacji medycznej, zgodę na udostępnienie wyraża sąd na wniosek osoby bliskiej lub osoby wykonującej zawód medyczny. Osoba wykonująca zawód medyczny może wystąpić z wnioskiem do sądu także w przypadku uzasadnionych wątpliwości, czy osoba występująca o udostępnienie dokumentacji lub sprzeciwiająca się jej udostępnieniu jest osobą bliską.

W przypadku gdy pacjent za życia sprzeciwił się udostępnieniu dokumentacji medycznej, sąd na wniosek osoby bliskiej może wyrazić zgodę na udostępnienie dokumentacji medycznej i określić zakres jej udostępnienia, jeżeli jest to niezbędne w celu dochodzenia odszkodowania lub zadośćuczynienia, z tytułu śmierci pacjenta lub dla ochrony życia lub zdrowia osoby bliskiej.

Przepisy nie regulują zasad udostępniania jednostkowych danych medycznych po śmierci pacjenta. W zakresie, w jakim zawarte są w dokumentacji medycznej, należy stosować do nich powyższe zasady. W zakresie pozostałych danych właściwe jest postępowanie na analogicznych zasadach.

4. CZYM JEST TZW. DAWSTWO DANYCH?

Pojęcie dawstwa danych może kojarzyć się z dawstwem krwi lub narządów. I słusznie, przyświeca mu bowiem podobna idea, tylko pacjent zamiast dzielić się materiałem biologicznym, dzieli się swoimi danymi o stanie zdrowia, które mogą być dalej wykorzystane w różnych dopuszczalnie prawnie celach, w szczególności w celach naukowych. Tym samym udostępniając indywidualne dane (dane osobowe lub anonimowe) można działać na rzecz rozwoju medycyny.

Z pojęciem dawstwa danych lekarze będą mogli spotkać się coraz częściej za sprawą rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (tzw. akt w sprawie

[7] Osoba bliska w rozumieniu ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oznacza małżonka, krewnego do drugiego stopnia lub powinowatego do drugiego stopnia w linii prostej, przedstawiciela ustawowego, osobę pozostającą we wspólnym pożyciu lub osobę wskazaną przez pacjenta.

zarządzania danymi), który reguluje m.in. zasady funkcjonowania dostawców usług udostępniania danych, czyli profesjonalnych podmiotów zajmujących się gromadzeniem danych z wielu źródeł w celu tworzenia dużych baz danych do ponownego wykorzystania (z ang. *secondary use of data*). Należy przez to rozumieć możliwość wykorzystywania przez osoby fizyczne, firmy, organizacje pozarządowe lub instytucje publiczne danych będących w posiadaniu określonych podmiotów do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie, dla którego to celu dane te zostały zebrane lub wytworzone. Dane przeznaczone do celów ponownego wykorzystywania powinny być przy tym zanonimizowane lub zmodyfikowane, zagregowane lub przekształcone za pomocą innej metody zapobiegającej ujawnieniu tożsamości, tak by nie naruszać prywatności osób, których dotyczą. Dzięki mechanizmom ponownego wykorzystywania danych możliwe staje się skorzystanie z potencjału ogromnych baz danych – dane mogą być dalej wykorzystywane np. w celach naukowych lub kształtowania polityki publicznej w ochronie zdrowia.

Lekarze powinni pamiętać, że przepisy prawa medycznego nie zawierają obecnie żadnych szczególnych regulacji odnoszących się do dawstwa danych. Oznacza to, że jest ono dopuszczalne, o ile odbywa się na zasadach udostępniania dokumentacji medycznej i jednostkowych danych medycznych opisanych w tym przewodniku. Najczęstszą podstawą umożliwiającą dawstwo danych medycznych będzie zatem zgoda pacjenta. Przed wyrażeniem takiej zgody pacjent powinien otrzymać zrozumiałe informacje na temat celów i sposobu wykorzystania jego danych. Zgoda pacjenta na dawstwo danych, podobnie jak zgoda na udzielenie świadczenia zdrowotnego, powinna być świadoma.

Przywołane rozporządzenie posługuje się też pojęciem „altruistycznego podejścia do danych", które oznacza możliwość dzielenia się z innymi podmiotami przez osoby, których dane dotyczą[8], na podstawie ich dobrowolnie wyrażonej, świadomej zgody, danymi osobowymi do celów realizowanych w interesie ogólnym, takich jak cele badań naukowych lub poprawa jakości usług publicznych. Dane mogą być bezpłatnie udostępniane w tych celach tzw. organizacjom altruizmu danych, czyli wyspecjalizowanym podmiotom, które muszą spełniać dodatkowe wymogi (w szczególności prowadzić działalność o charakterze niekomercyjnym i być prawnie niezależnym od jakiegokolwiek podmiotu nastawionego na zysk) oraz uzyskać wpis do specjalnego rejestru[9]. Organizacja altruizmu danych nie może wykorzystywać danych do celów innych niż cele leżące w interesie ogólnym, w odniesieniu do których osoba, której dane dotyczą, zezwoliła na przetwarzanie. Organizacja altruizmu danych ma także zakaz stosowania wprowadzających w błąd praktyk marketingowych, by nakłaniać do przekazywania danych.

Co ważne z perspektywy lekarza, o ile organizacja altruizmu danych powinna zapewniać narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą (np. dostarczać formularze zgody), zasady związane z dostępem do dokumentacji medycznej i jednostkowych danych medycznych pozostają takie same jak przedstawione w poprzednich punktach – w tym zakresie akt w sprawie zarządzania danymi nie przewiduje żadnych wyjątków. Udostępniając dane lub dokumenty pacjentów organizacjom altruizmu danych należy więc postępować analogicznie jak przy udostępnianiu ich innym podmiotom, w szczególności upewnić się, że pacjent wyraził zgodę na takie udostępnienie oraz jaki jest zakres objętych nią danych.

[8] A także na analogicznych zasadach posiadaczy danych, czyli osób lub podmiotów mających prawo do udzielania dostępu do niektórych danych osobowych lub danych nieosobowych lub do dzielenia się nimi.

[9] W świetle krajowego projektu ustawy o zarządzaniu danymi, taki rejestr prowadzić ma Urząd Ochrony Konkurencji i Konsumentów.

5. W JAKI SPOSÓB MOGĘ UDOSTĘPNIAĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE?

Przepisy prawa regulują nie tylko kwestię tego, komu lekarz może udostępnić dokumentację, ale także sposób, w jaki powinno to nastąpić. W świetle art. 27 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, dokumentację medyczną udostępnia się w następujący sposób:

- do wglądu, w tym także do baz danych w zakresie ochrony zdrowia, w miejscu udzielania świadczeń zdrowotnych, z wyłączeniem medycznych czynności ratunkowych, albo w siedzibie podmiotu udzielającego świadczeń zdrowotnych, z zapewnieniem pacjentowi lub innym uprawnionym organom lub podmiotom możliwości sporządzenia notatek lub zdjęć;
- przez sporządzenie jej wyciągu, odpisu, kopii lub wydruku;
- przez wydanie oryginału za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu, na żądanie organów władzy publicznej albo sądów powszechnych, a także w przypadku gdy zwłoka w wydaniu dokumentacji mogłaby spowodować zagrożenie życia lub zdrowia pacjenta;
- za pośrednictwem środków komunikacji elektronicznej;
- na informatycznym nośniku danych.

Udostępniając dokumentację medyczną za pośrednictwem środków komunikacji elektronicznej lub na informatycznych nośnikach danych należy koniecznie pamiętać o cyberbezpieczeństwie. Przepisy prawa nie narzucają konkretnych środków bezpieczeństwa – to udostępniający powinien móc wykazać, że stosuje rozwiązania adekwatne do zagrożeń, uwzględniających najnowszy stan wiedzy technicznej. W przypadku stosunkowo częstego udostępniania dokumentacji mailem minimalnym standardem powinno być wysyłanie jej tylko na adres wskazany wyraźnie przez pacjenta po uprzednim poinformowaniu go o zagrożeniach związanych z proponowanym kanałem komunikacji. Wysyłka powinna obejmować zaszyfrowany plik z danymi, do którego hasło powinno zostać przesłany do odbiorcy innym, bezpiecznym kanałem komunikacji (np. wiadomością sms).

Zdjęcia rentgenowskie wykonane na kliszy, przechowywane przez podmiot udzielający świadczeń zdrowotnych, są udostępniane za potwierdzeniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu.

Dokumentacja medyczna prowadzona w postaci papierowej może być udostępniona przez sporządzenie kopii w formie odwzorowania cyfrowego (skanu) i przekazanie za pośrednictwem środków komunikacji elektronicznej lub na informatycznym nośniku danych, na żądanie pacjenta lub innych uprawnionych organów lub podmiotów, jeżeli przewiduje to regulamin organizacyjny podmiotu udzielającego świadczeń zdrowotnych.

Przykład: pacjent wnioskuje o wydanie mu oryginału jego dokumentacji medycznej. Lekarz chciałby wykorzystać dane z tej dokumentacji w badaniu naukowym, więc wolałby nie przekazywać oryginału. Czy może tak postąpić?

Nie. Jak wskazał Naczelny Sąd Administracyjny w wyroku z dnia 19 kwietnia 2016 r. (sygn. II OSK 2361/15), stosowana przez podmiot leczniczy praktyka, polegająca na nieudostępnianiu oryginałów dokumentacji medycznej pacjentom, jest praktyką bezprawną. Dostęp do dokumentacji medycznej jest prawem pacjenta, które może być zrealizowane poprzez wydanie oryginału za pokwitowaniem odbioru i z zastrzeżeniem zwrotu po wykorzystaniu. Warto przy tym zauważyć, że zgodnie z § 70 ust.

3 rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania w przypadku udostępnienia dokumentacji w postaci papierowej w taki sposób pozostawia się kopię lub pełny odpis wydanej dokumentacji. Tym samym lekarz będzie mógł dalej wykorzystać dane w celu naukowym.

Należy też pamiętać, że każdy podmiot udzielający świadczeń zdrowotnych (czyli np. indywidualna praktyka lekarska) powinien prowadzić przy tym wykaz zawierający następujące informacje dotyczące udostępnianej dokumentacji medycznej:

1) imię (imiona) i nazwisko pacjenta, którego dotyczy dokumentacja medyczna;

2) sposób udostępnienia dokumentacji medycznej;

3) zakres udostępnionej dokumentacji medycznej;

4) imię (imiona) i nazwisko osoby innej niż pacjent, której została udostępniona dokumentacja medyczna, a w odpowiednich przypadkach, także nazwę uprawnionego organu lub podmiotu;

5) imię (imiona) i nazwisko oraz podpis osoby, która udostępniła dokumentację medyczną;

6) datę udostępnienia dokumentacji medycznej.

6. W JAKIM CZASIE NALEŻY UDOSTĘPNIĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE?

Przepisy prawa nie wyznaczają konkretnego terminu, w którym powinność dojść do udostępnienia dokumentacji medycznej lub jednostkowych danych medycznych.

Rozporządzenie Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania wskazuje w § 70 ust. 1, że dokumentację udostępnia się „bez zbędnej zwłoki”. Oznacza to, że dokumentacja medyczna powinna zostać udostępniona najszybciej jak to tylko możliwe, oczywiście z uwzględnieniem wszystkich okoliczności i możliwości organizacyjnych. Tym samym lekarz nie powinien zanadto zwlekać i odkładać w czasie czynności związanych z udostępnieniem na później. Jeżeli może bez szkody dla innych obowiązków zająć się udostępnieniem, powinien to zrobić.

Pewnych dalszych wytycznych dotyczących terminowości udostępniania dokumentacji medycznej dostarcza orzecznictwo sądów. Jak wskazał Naczelny Sąd Administracyjny w wyroku z dnia 6 września 2016 r. (sygn. II OSK 1247/16): „nałożenie obowiązku udostępnienia dokumentacji medycznej "bez zbędnej zwłoki" dopuszcza zwłokę w działaniu. Dopuszczenie zwłoki z przyczyn braku dostatecznej organizacji podmiotu leczniczego wykonania obowiązku wobec pacjentów, którym udzielane są świadczenia jest nie do przyjęcia. Przesłankę "bez zbędnej zwłoki" należy odnieść tylko do potrzeby podjęcia czynności przygotowania dokumentacji medycznej, której przygotowanie nie jest związane z podjęciem złożonych czynności, jako że podmiot udzielający świadczeń ma obowiązek przechowywania dokumentacji. W zasadzie bez zbędnej zwłoki związane jest z obowiązkiem udostępniania tej dokumentacji niezwłocznie, zważywszy na sposób jej udostępnienia”.

Przykład: regulamin na stronie internetowej praktyki lekarskiej wskazuje, że dokumentacja medyczna udostępniana jest w terminie nie późniejszym niż 14 dni. Czy taka praktyka jest dopuszczalna?

Nie. Jak wskazał Naczelny Sąd Administracyjny w wyroku z dnia 12 grudnia 2017 r. (sygn. II OSK 2188/17), wyznaczenie terminu do realizacji wniosku o udostępnienie dokumentacji medycznej stanowi praktykę naruszającą zbiorowe prawa pacjentów. Wyznaczenie terminu nie później niż w ciągu siedmiu dni pozwala na stosowanie tego terminu jako reguły, naruszając prawo do udostępnienia dokumentacji bez zbędnej zwłoki. Indywidualne przypadki koniecznego wydłużenia terminu udostępnienia dokumentacji medycznej nie dają podstaw do wyprowadzenia odstępstwa od regulacji powszechnie obowiązującej przyznającej prawo do udostępnienia bez zbędnej zwłoki.

7. PRZEZ JAKI CZAS NALEŻY PRZECHOWYWAĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE?

Podobnie jak we wcześniejszych przypadkach, za przechowywanie dokumentacji medycznej odpowiadać będzie najczęściej osoba prawna, np. szpital i przychodnia. Jeżeli jednak lekarz prowadzi własną działalność i działa poza strukturami takich placówek, poniższe obowiązki dotyczą także jego.

Zgodnie z art. 29 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, dokumentację medyczną przechowuje się przez okres 20 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu, z wyjątkiem:

1) dokumentacji medycznej w przypadku zgonu pacjenta na skutek uszkodzenia ciała lub zatrucia, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym nastąpił zgon;
2) dokumentacji medycznej zawierającej dane niezbędne do monitorowania losów krwi i jej składników, która jest przechowywana przez okres 30 lat, licząc od końca roku kalendarzowego, w którym dokonano ostatniego wpisu;
3) zdjęć rentgenowskich przechowywanych poza dokumentacją medyczną pacjenta, które są przechowywane przez okres 10 lat, licząc od końca roku kalendarzowego, w którym wykonano zdjęcie;
4) skierowań na badania lub zleceń lekarza, które są przechowywane przez okres:

   a) 5 lat, licząc od końca roku kalendarzowego, w którym udzielono świadczenia zdrowotnego będącego przedmiotem skierowania lub zlecenia lekarza,

   b) 2 lat, licząc od końca roku kalendarzowego, w którym wystawiono skierowanie - w przypadku gdy świadczenie zdrowotne nie zostało udzielone z powodu niezgłoszenia się pacjenta w ustalonym terminie, chyba że pacjent odebrał skierowanie;
5) dokumentacji medycznej dotyczącej dzieci do ukończenia 2. roku życia, która jest przechowywana przez okres 22 lat.

Po upływie powyższych okresów niszczy się dokumentację medyczną w sposób uniemożliwiający identyfikację pacjenta, którego dotyczyła. Dokumentacja medyczna przeznaczona do zniszczenia może być wydana pacjentowi, jego przedstawicielowi ustawowemu lub osobie upoważnionej przez pacjenta.

8. JAK NALEŻY ZABEZPIECZYĆ DOKUMENTACJĘ MEDYCZNĄ I JEDNOSTKOWE DANE MEDYCZNE?

Prowadzenie dokumentacji medycznej w postaci cyfrowej wiąże się z koniecznością zapewnienia jej cyberbezpieczeństwa. Jednym z podstawowych obowiązków jest więc zapewnienie ochrony danych zawartych w tej dokumentacji (art. 24 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta). Szczegółowe wymogi w tym zakresie wynikają m.in. z przepisów RODO, ustawy o systemie informacji w ochronie zdrowia, ustawy o krajowym systemie cyberbezpieczeństwa, rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania. Z perspektywy lekarza ważne jest to, że za spełnienie większości obowiązków związanych z zabezpieczeniem dokumentacji medycznej odpowiada podmiot wykonujący działalność leczniczą, czyli np. szpital lub przychodnia.

W przypadku prowadzenia własnej praktyki, obowiązki z tym związana ciążą już jednak bezpośrednio na lekarzu. W takiej sytuacji pomocne może być działanie zgodne z jednym z dwóch zatwierdzonych przez Prezesa Urzędu Ochrony Danych Osobowych kodeksów postępowania dedykowanych dla ochrony zdrowia[10].

Niezależnie od sytuacji, warto by każdy lekarz orientował się w poniższych, podstawowych zasadach, których niedochowanie może prowadzić do naruszenia ochrony danych osobowych, co może rodzić wątpliwości co do działania lekarza z należytą starannością.

1. **Dbaj o dane osobowe** - przy wykonywaniu codziennych obowiązków zawodowych zwracaj szczególną uwagę na kwestie związane z ochroną danych osobowych i zachowuj szczególną staranność z tym związaną. Często chodzi o drobne działania - nieodłożony na miejsce dokument, plik zgrany z niezweryfikowanego pendriva czy opuszczenie na chwilę komputera bez wylogowania się z konta może prowadzić do naruszenia ochrony danych.
2. **Znaj i przestrzegaj procedur wewnętrznych** – w szpitalach i przychodniach powinny obowiązywać wewnętrzne polityki bezpieczeństwa, których przestrzeganie stanowi jeden z podstawowych obowiązków każdego pracownika i współpracownika. Opisują one pożądane zasady postępowania dostosowane do specyfiki określonej placówki zdrowotnej. Zapoznaj się z nimi i zapamiętaj co najmniej kluczowe zasady.
3. **Reaguj na naruszenia ochrony danych** – naucz się rozpoznawać sytuacje, które mogą stanowić naruszenie ochrony danych osobowych i zgodnie z przyjętymi procedurami wewnętrznymi informuj o nich niezwłocznie inspektora ochrony danych, przedstawiciela działu systemów IT lub inne osoby zgodnie z przyjętymi zasadami. Nie zwlekaj – administrator danych ma tylko 72 godziny by zgłosić ewentualne naruszenie do UODO.
4. **Naucz się odpowiadać na prośby i pytania pacjentów –** RODO przyznaje pewne prawa osobom, których dane przetwarzasz, takie jak np. prawo do sprostowania danych czy żądania ich usunięcia. Pacjent może poprosić o informacje na temat zasad przetwarzania jego danych osobowych. Warto więc wiedzieć, gdzie pacjent może zapoznać się z klauzulą informacyjną oraz jak postępować w przypadku innych próśb. W razie wątpliwości należy co najmniej potrafić skierować pacjenta do inspektora ochrony danych.
5. **Kontaktuj się z Inspektorem Ochrony Danych** – w razie jakichkolwiek pytań lub wątpliwości związanych z ochroną danych kontaktuj się z Inspektorem Ochrony Danych wyznaczonym przez

[10] https://uodo.gov.pl/pl/426/1110

szpital lub przychodnię. Nie bój się zadawać prostych pytań – lepiej zgłosić się nawet z błahym problemem, niż ryzykować naruszeniem ochrony danych.

6. **Chroń hasła i nie udostępniaj danych do logowania** – pamiętaj o przyjętej wewnętrznie polityce zmiany haseł do systemów teleinformatycznych. Nie udostępniaj danych do logowania do swojego konta koleżankom i kolegom z pracy – nieautoryzowany dostęp do danych i ich ewentualna zmiana może stanowić naruszenie ochrony danych.
7. **Nie przesyłaj danych medycznych poza szpital lub przychodnię** – dostęp do danych pacjentów jest regulowany przez przepisy prawa. Nie rób zdjęć dokumentacji medycznej prywatnym telefonem lub aparatem i nie udostępniaj zdjęć, nawet ich fragmentów, innym osobom, w szczególności w mediach społecznościowych. Nie wynoś służbowego laptopa poza pracę, chyba że postępujesz zgodnie z wewnętrznymi zasadami. Podobnie w przypadku zgrywania danych służbowych na prywatny sprzęt.
8. **Zwracaj uwagę na co i do kogo mówisz** – prowadzenie rozmowy z pacjentem na temat szczegółów jego stanu zdrowia na środku korytarza stanowi zagrożenie dla poufności przekazywanych informacji, podobnie jak przekazywanie ich w prywatnych rozmowach nieuprawnionym do tego pracownikom.
9. **Zwracaj uwagę na nieprawidłowości i reaguj** – jeżeli dostrzegasz sytuacje lub zachowania, które mogą stanowić zagrożenie dla ochrony danych, nie wahaj się poinformować o nich inspektora ochrony danych. Wykorzystywanie systemów operacyjnych, dla których producent zakończył wsparcie techniczne, przechowywania dokumentacji w niezabezpieczonych pomieszczeniach – to tylko przykłady, na które należy zwracać uwagę.
10. **Pamiętaj o odpowiedzialności** – zaniedbania w powyższym zakresie oznaczają zagrożenie wysoką karą finansową dla placówki medycznej, w której wykonujesz zawód. Za naruszenia ochrony danych osobowych także osobiście możesz ponosić odpowiedzialność, w szczególności cywilną i zawodową.

Powyższe dziesięć wskazówek to tylko podstawowe zasady. Jeżeli chciałbyś dowiedzieć się więcej o ochronie danych, w pierwszej kolejności warto porozmawiać z inspektorem ochrony danych.

Doświadczenia ostatnich lat wskazują na rosnące ryzyko związane z zagrożeniami dla bezpieczeństwa danych medycznych. ENISA opublikowała raport na temat zagrożeń cybernetycznych dla europejskiego sektora ochrony zdrowia. Badanie wykazało, że w 2021 roku odnotowano 91 incydentów, w 2022 roku 84 incydenty, a od stycznia do końca marca 2023 roku, czyli tylko przez pierwsze trzy miesiące roku, już 40 incydentów[11]. Jak wynika z dostępnych danych, w Polsce liczba zgłoszonych cyberataków na placówki ochrony zdrowia wzrosła trzykrotnie w ciągu jednego roku – z 13 w 2021 do 43 w 2022 i nadal rośnie[12]. Atak na prywatną sieć laboratoriów medycznych z listopada 2023 r. potwierdza, jak ważne i aktualne są kwestie związane z cyberbezpieczeństwem.

[11] ENISA threat landscape: health sector (January 2021 to March 2023), s. 8. https://www.enisa.europa.eu/publications/health-threat-landscape

[12] https://forsal.pl/lifestyle/technologie/artykuly/9223343,check-point-liczba-cyberatakow-na-sluzbe-zdrowia-w-polsce-wzrosla-trz.html

9. CZY DOKUMENTACJA MEDYCZNA I JEDNOSTKOWE DANE MEDYCZNE MOGĄ BYĆ WYKORZYSTYWANE PRZEZ SZTUCZNĄ INTELIGENCJĘ?

Sztuczna inteligencja[13] jest już z powodzeniem wykorzystywana w polskim systemie ochrony zdrowia. Jak można się spodziewać, w kolejnych latach zjawisko to będzie przybierać na sile, bowiem jest to technologia, z którą wiąże się wielkie nadzieje w kontekście rozwoju medycyny. Coraz więcej lekarzy może mieć więc wątpliwości, jak wykorzystywać ją przy wykonywaniu zawodu zgodnie z prawem, w tym w szczególności w zakresie dostępu i przetwarzania przez nią danych medycznych.

W pierwszej kolejności należy więc wyjaśnić, że nie ma obecnie przepisów prawa, które regulowałyby w szczególny, dedykowany sposób to zagadnienie. Przetwarzanie danych o stanie zdrowia przez sztuczną inteligencję powinno więc odbywać się przy poszanowaniu przywołanych w tym przewodniku zasad przetwarzania dokumentacji medycznej i jednostkowych danych medycznych, a także z poszanowaniem szeregu obowiązków wynikających z RODO. Na poziomie Unii Europejskiej dopiero toczą się prace legislacyjne związane z projektem rozporządzenia Parlamentu Europejskiego i Rady ustanawiającym zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającym niektóre akty ustawodawcze Unii.

W kontekście RODO lekarz powinien pamiętać, że każdy proces przetwarzania danych osobowych wymaga odpowiedniej podstawy prawnej. W zakresie codziennej pracy w placówkach medycznych podstawę taką zapewnia art. 9 ust. 2 lit. h RODO, który umożliwia przetwarzanie danych o stanie zdrowia w zakresie, w jakim jest to niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia przy zachowaniu tajemnicy zawodowej. Ponadto, w praktyce dane o stanie zdrowia są też przetwarzane w ramach badań klinicznych w oparciu o art. 9 ust. 2 lit i lub j RODO, czyli niezbędność ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego lub do celów badań naukowych. W zakresie, w jakim systemy AI realizują te cele, mogą być wykorzystywane także do przetwarzania danych pacjentów, o ile spełnione są także inne warunki związane m.in. z poufnością danych (np. dostawca systemu AI nie wykorzystuje dostępu do danych także w innych celach). Należy też pamiętać, że automatyczne podejmowanie decyzji i profilowanie może być oparte na przetwarzaniu szczególnych kategorii danych osobowych wyłącznie wtedy, gdy taka możliwość wynika z przepisów prawa albo gdy takie działanie odbywa się za wyraźną zgodą osoby, której dane dotyczą. Należy zaznaczyć, że odpowiedzialność za opiekę nad pacjentem ponosi co do zasady lekarz – może on posiłkować się podobnymi rozwiązaniami, ale ostateczne decyzje terapeutyczne powinny należeć do niego.

W zakresie, w jakim lekarz prowadzi własną działalność w ramach indywidualnej praktyki, stosując rozwiązania oparte o AI, podobnie jak w przypadku innych rozwiązań związanych z dostępem do danych, będzie musiał zadbać o spełnienie obowiązków wynikających z RODO, w tym m.in. ocenić, czy w danej sytuacji należy zawrzeć umowę powierzenia danych osobowych.

[13] Na potrzeby tej publikacji nie będziemy wchodzić w rozważania, czym jest sztuczna inteligencja. Pod kątem omawianej tematyki wystarczające jest przyjęcie jej bardzo uproszczonego rozumienia jako szeregu rozwiązań IT bazujących na dostępie i analizie danych, które generują na ich podstawie nowe wyniki.

Jeżeli lekarz stosuje rozwiązania oparte na AI pracując w szpitalu lub przychodni, powinien postępować zgodnie z przyjętymi w danej placówce zasadami postępowania lub wewnętrznymi politykami i procedurami. Warto mieć przy tym świadomość, że zobowiązanie lekarza do postępowania z należytą starannością przy wykonywaniu zawodu oznacza m.in. troskę o dobór narzędzi zgodnych z obowiązującym prawem. Samo nawet podejrzenie, że dane mogą być przetwarzane z naruszeniem powyższych zasad, np. nie są odpowiednio zabezpieczone przed nieuprawnionym dostępem, należy niezwłocznie zgłosić do inspektora ochrony danych lub innej osoby zgodnie z wewnętrznymi zasadami.

10. CZYM JEST ANONIMIZACJA I PSEUDONIMIZACJA DANYCH?

Zgodnie z definicją legalną z art. art. 4 pkt 5. RODO, pseudonimizacja danych oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Jak zatem wynika z powyższej definicji, pseudonimizacja jest pewną operacją dokonywaną na danych osobowych, jest procesem ich przetwarzania. Pseudonimizacja jest przy tym procesem w pełni odwracalnym. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje możliwe do zidentyfikowania. Dane spseudonimizowane są wciąż danymi osobowymi.

Typowym przykładem pseudonimizacji danych osobowych będzie np. zatem posługiwanie się numerem identyfikacyjnym i ograniczonym zestawem danych osobowych zamiast pełnego zestawu danych. Taki numer identyfikacyjny powinien być przechowywany oddzielnie, wraz z informacjami umożliwiającymi identyfikację osoby, i dodatkowo być odpowiednio zabezpieczony.

RODO nie zawiera definicji legalnej procesu anonimizacji danych anonimowych. Uznaje się, że anonimizacja jest procesem, w którym informacje umożliwiające identyfikację osoby są nieodwracalnie usunięte lub zmienione w taki sposób, aby nie istniała już możliwość bezpośredniego lub pośredniego zidentyfikowania podmiotu danych, nawet przez administratora danych działającego samodzielnie lub we współpracy z jakąkolwiek inną stroną. W procesie anonimizacji usuwa się lub modyfikuje informacje, które mogą stanowić dane osobowe w rozumieniu RODO, pozostawiając inne, które nie pozwalają już na identyfikację osoby, której te dane dotyczą. Proces anonimizacji musi być trwały i nieodwracalny. Dane zanonimizowane nie stanowią już danych osobowych.

RODO nie odwołuje się do żadnej konkretnej techniki anonimizacji, zatem to od poszczególnych administratorów danych zależy, czy wybrany przez nich proces „anonimizacji" jest wystarczająco solidny. Istnieją różne praktyki i techniki anonimizacji o różnych stopniach dokładności, np. podejście oparte na randomizacji czy podejście oparte na uogólnianiu.

Występujące wątpliwości interpretacyjne dotyczą przede wszystkim tego, jak należy oceniać nieodwracalność skutku anonimizacji. Wyróżnia się dwa zasadnicze podejścia w tym zakresie:

- **podejście obiektywne** – w tej perspektywie dane są uznawane za zanonimizowane jedynie wtedy, gdy nikt (w tym administrator danych wejściowych) nie jest w stanie zidentyfikować podmiotu, którego dane dotyczą;

- **podejście subiektywne** – w tej perspektywie wystarczającym dla uznania, że dane są danymi zanonimizowanymi jest stwierdzenie, że strona posiadająca dane dotyczące podmiotu danych nie może, postępując zgodnie z przepisami prawa, zidentyfikować tego podmiotu danych.

W świetle dotychczasowej praktyki stosowania prawa trudno przesądzić, które podejście okaże się dominujące. Wydawane dotąd orzeczenia sądowe przemawiają na rzecz podejścia subiektywnego, które jest rozwiązaniem zapewniającym większe możliwości pod kątem wykorzystywania danych np. w celach naukowych. Warto śledzić, czy nie ukazały się wytyczne lub standardy opisujące dokładniej wymogi związane z procesem anonimizacji i pseudonimizacji.