dr Artur Romaszewski
mgr Mariusz Kielar
mgr Szczepan Jakubowski
dr hab. Mariusz Duplaga, prof. UJ
Zakład Promocji Zdrowia, Instytut Zdrowia Publicznego, Wydział Nauk o Zdrowiu, Uniwersytet Jagielloński Collegium Medicum
artur.romaszewski@uj.edu.pl

CZĘŚĆ II – DANE O STANIE ZDROWIA W ŚWIETLE NOWYCH WYZWAŃ TECHNICZNYCH, PRAWNYCH I ORGANIZACYJNYCH – WYBRANE ZAGADNIENIA

Wprowadzenie

W opinii autorów niniejszego opracowania, w polskiej ochronie zdrowia mamy do czynienia ze spektakularnym sukcesem usług elektronicznych tj.: e-recepty i e-skierowania oraz praktycznym wdrożeniu Internetowego Konta Pacjenta. Konsekwencją tego procesu jest szybkie zastępowanie w podmiotach leczniczych dokumentacji papierowej na dokumentację w postaci elektronicznej. Dodatkowo nowe regulacje prawne[1],[2] po wielu latach dyskusji i przesuwania terminów wejścia w życie, wprowadziły dokumentację w postaci elektronicznej jako podstawową formę prowadzenia dokumentacji medycznej. Jest to krok niezbędny w kierunku pełnego uruchomienia wprowadzanego 10 lat temu systemu informacyjnego ochrony zdrowia[3]. Wszystko to napawa optymizmem, jednak wciąż jest wiele kwestii, które powinny być uwzględnione w nowych uregulowaniach. Wynikają one głównie z dostosowania krajowych standardów do regulacji obowiązujących w Unii Europejskiej (UE). Mowa przede wszystkim o jak najlepszym wykorzystaniu usług zaufania m.in: podpisu elektronicznego, pieczęci elektronicznej, instytucji walidacji, konserwacji oraz usługę rejestrowanego doręczenia. Wykorzystanie tych narzędzi w prawie dotyczącym obiegu i przetwarzania dokumentów elektronicznych w ochronie zdrowia, w tym elektronicznej dokumentacji medycznej (EDM) jest niezbędne dla prawidłowego funkcjonowania systemu informacyjnego ochrony zdrowia. Jest to również konieczne do transgranicznego obiegu dokumentów medycznych. System informacyjny ochrony zdrowia to struktura, której głównymi priorytetami

[1] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[2] Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej (Dz.U. 2018 poz. 941).
[3] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 nr 113 poz. 657).

są identyfikacja podmiotów biorących udział w tworzeniu i przetwarzaniu oraz zapewnienie integralności dokumentów.

W tym artykule autorzy spojrzą na poruszane wyżej problemy przez pryzmat rozwiązań prawnych obowiązujących w sektorze zdrowotnym. Dodatkowo dokonają oceny zastosowań nowych regulacji o charakterze ogólnym dla potrzeb ochrony zdrowia. Celem takiego zabiegu jest próba uporządkowania tego co jest obowiązujące i co można wykorzystać oraz zwrócenie uwagi na niedociągnięcia i braki.

1. Wyzwania prawne

Główną regulacją prawną stanowiącą legalną podstawę dla zapewnienia bezpieczeństwa transakcji elektronicznych oraz potwierdzania tożsamości w usługach elektronicznych jest Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (eIDAS)[4]. W Polsce aktem wprowadzającym eIDAS jest ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej – także pewne elementy można znaleźć w ustawie o informatyzacji podmiotów realizujących zadania publiczne[5]. Natomiast regulacja o charakterze ogólnym mogąca być dodatkowo wykorzystana w ochronie zdrowia to ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych[6].

Regulacje dedykowane systemowi opieki zdrowotnej to przede wszystkim rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania[7] (oraz regulacje dotyczące) oraz cała grupa regulacji tymczasowych dotyczących covid-19. Nowym rozwiązaniem jest Krajowy Rejestr Pacjentów z Covid[8] oraz teleporada[9] jako forma świadczenia zdrowotnego.

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
[5] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
[6] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).
[7] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[8] Rozporządzenie Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej (Dz.U. 2020 poz. 1395).
[9] Rozporządzenie Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej (Dz.U. 2020 poz. 1395).

Przyjęte w powyższych aktach prawnych rozwiązania zostały wykorzystane w regulacjach dotyczących ochrony zdrowia tj. ustawy o systemie informacji w ochronie zdrowia (dotyczącej m.in. elektronicznej dokumentacji medycznej) jak także w regulacjach dotyczących dokumentacji medycznej w postaci elektronicznej.

Z punktu widzenia codziennej działalności podmiotów leczniczych niezawodne funkcjonowanie dokumentacji medycznej i zapewnienie jej bezpieczeństwa to jedno z najważniejszych zadań. Dlatego bardzo oczekiwanym aktem prawnym było rozporządzenie regulujące tworzenie, prowadzenie i archiwizowanie dokumentacji medycznej. Wejście regulacji zakończyło wieloletni spór o datę wprowadzenia dokumentacji medycznej w postaci elektronicznej jako podstawowej formy funkcjonowania tej dokumentacji w podmiotach leczniczych. Wejście nowych przepisów zakończyło trudny etap przejściowy, przetwarzania przez podmioty świadczące usługi zdrowotne danych zgromadzonych zarówno w dokumentacji papierowej jak i w postaci elektronicznej. Obecna regulacja nie dopuszcza prowadzenia dokumentacji medycznej w dwóch formach: papierowej i elektronicznej. Zasadą staje się prowadzenie dokumentacji w postaci elektronicznej natomiast forma papierowa jest dopuszczalna w uzasadnionych, wynikających z prawa sytuacjach.

2. Wyzwania organizacyjne i techniczne

Należy zauważyć, że okres pandemii przyniósł z sobą nowy typ usługi tzn. teleporada. Pierwsza regulacja teleporady wprowadzona została przepisami tzw. „specustawy" o COVID-19 z 2 marca 2020 r[10]. Jej celem nie było diagnozowanie i leczenie pacjenta, lecz prowadzenie podziału pacjentów: na tych, których należy przyjąć stacjonarnie i na tych, którym można pomóc w ramach e-wizyty. Teleporada udzielana była tylko pacjentom dzwoniącym na ogólnopolską infolinii obsługiwaną przez NFZ w związku z koronawirusem. Lekarz prowadził karty teleporada i miał obowiązek przechowywać je przez 30 dni od dnia udzielenia porady.

Natomiast e-wizyta zostały uregulowane[11] przed pandemią i podobnie jak wizyty stacjonarne były rejestrowane w dokumentacji medycznej pacjenta.

Wzrost liczby danych przekazywanych w sieciach teleinformatycznych, a przede wszystkim wprowadzenie jako podstawy gromadzenia danych i informacji o pacjencie

[10] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 374).
[11] Rozporządzenie Ministra Zdrowia z dnia 31 października 2019 r. zmieniające rozporządzenie w sprawie świadczeń gwarantowanych z zakresu podstawowej opieki zdrowotnej (Dz.U. 2019 poz. 2120).

dokumentacji w postaci elektronicznej oprócz oczywistych korzyści wymusza też na użytkownikach obowiązek zapewnienia bezpieczeństwa tak przetwarzanym danym.

W rozporządzeniu Ministra Zdrowia z dnia 31 października 2019 (art. 1. 5, 6)[12] ten problem potraktowano bardzo ogólnie wskazując na wybrane wymagania dotyczące zabezpieczenia dokumentacji medycznej oraz systemu teleinformatycznego, w którym jest prowadzona dokumentacja medyczna.

Na zagrożenia cybernetyczne zwraca uwagę w raporcie Naczelna Izby Kontroli (NIK)[13]. W wyniku kontroli wykazano liczne nieprawidłowości w zakresie zabezpieczenia i dostępu do danych wrażliwych w tym do danych gromadzonych w elektronicznej dokumentacji medycznej. Wśród błędów można wskazać m.in.:

- Przyznanie nieodpowiednich uprawnień dostępu do danych pacjentów – dotyczyło to pielęgniarek, którym przyznano w systemie HIS (*ang. Hospital information system*, Szpitalny System Informatyczny) uprawnienia dostępu do danych pacjentów z oddziałów lub poradni szpitala, na których nie świadczyły pracy;
- Brak odpowiednich upoważnień do przetwarzania danych osobowych pacjentów;
- Upoważnienia dla osób, które nie powinny przetwarzać danych osobowych;
- Nieodbieranie byłym pracownikom uprawnień w systemach informatycznych;
- Niewłaściwy proces autoryzacji użytkowników w systemie operacyjnym – nie wydawano indywidualnych loginów i haseł poszczególnym pracownikom, przez co tymi samymi danymi do autoryzacji w systemach operacyjnych posługiwała się grupa osób np. pracownicy danego oddziału szpitala.
- W kilku szpitalach część komputerów nie wymagała uwierzytelniania (można było uruchomić system operacyjny bez podawania loginu i hasła);
- Zastosowanie haseł dostępowych o nieodpowiedniej złożoności;
- Przyznanie pracownikom zaangażowanym w proces przetwarzania danych osobowych uprawnienia administratora systemów operacyjnych wykorzystywanych komputerów, mimo że w ich zakresach obowiązków nie przypisano im zadań związanych z administrowaniem infrastrukturą informatyczną.

[12] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[13] Najwyższa Izba Kontroli, *Wdrożenie Przez Podmioty Lecznicze Regulacji Dotyczących Ochrony Danych Osobowych*, Warszawa, 14 listopad 2019.

Dużo uwag NIK dotyczyło zastosowania rozwiązań technicznych i organizacyjnych zabezpieczenia danych o stanie zdrowia. Niewłaściwe zabezpieczenia danych osobowych w postaci elektronicznej. W zdecydowanej większości szpitali nie zastosowano odpowiednich środków technicznych do zabezpieczenia danych osobowych przechowywanych w postaci elektronicznej. Poszczególne elementy wpływające na bezpieczeństwo zostały niewłaściwie zaplanowane bądź były w nieodpowiedni sposób użytkowane. Inne nieprawidłowości to m.in.:

- Przechowywanie kopii zapasowej danych na nośnikach, których dotyczyła ta kopia;
- Przekazywanie w zgłoszeniach serwisowych dane osobowe pacjentów, a także ich danych medycznych – informacje te nie były niezbędne do rozwiązania usterek, możliwe było wykorzystanie automatycznie nadanego, zanonimizowanego numerów ID pacjenta;
- Brak stosowania odpowiednich środków zabezpieczenia elektronicznej dokumentacji medycznej;
- Brak ochrony oprogramowania antywirusowego lub brak aktualnych baz sygnatur wirusów.

W praktyce funkcjonowania podmiotów leczniczych najczęściej newralgicznym „czynnikiem" jest człowiek. Fakt ten, mimo że znany od lat dalej jest bardzo znaczący w zapewnieniu bezpieczeństwo danych zawartych w bazach danych firm medycznych. Innymi słowy za bezpieczeństwo danych zawartych w dokumentacji odpowiada przede wszystkim odpowiednio przygotowany personel. Często dochodzi bowiem do zachowań, których żadne środki techniczne nie są w stanie zahamować. W tej grupie znajdują się m.in. wysyłanie dokumentacji medycznej jako załącznika wiadomościach e-mailowych, robienie zdjęć dokumentacji przez smartfony, które są wszechobecne w miejscach przetwarzania danych, wynoszeniem dokumentacji poza miejsce udzielania świadczenia, przesyłaniem dokumentacji na prywatne urządzenia mobilne, przenoszenie dokumentacji pacjentów na niezabezpieczonych nośnikach danych, czy przekazywanie swoich haseł współpracownikom.

Ponadto wskazuje się na nieodpowiednie stosowanie przestarzałych aplikacji do sporządzania EDM i aplikacji klinicznych, które nie zostały zaprojektowane do bezpiecznego działania w aktualnym środowisku sieciowym. Kolejną przyczyną okazuje się niejednorodny

charakter systemów i aplikacji sieciowych oraz wykorzystywanie urządzeń z obsługą sieci, w tej samej sieci co infrastruktura krytyczna podmiotu[14].

W związku z powyższymi zagrożeniami, a przede wszystkim ze znaczeniem danych o stanie zdrowia dla prywatności osób, które one dotyczą nie dziwi fakt, że regulacje prawne zawierają przepisy mające za zadanie maksymalne ich zabezpieczenie. Jest to widoczne w regulacjach dotyczących ochrony danych osobowych, dokumentacji medycznej w postaci elektronicznej oraz przetwarzania danych w systemie informacyjnym ochrony zdrowia i systemie NFZ – to znacząca liczba przepisów odwołujących się do technologii. Niestety niesie to ze sobą pewne niebezpieczeństwa, ponieważ pojawiają się pojęcia techniczne oraz instytucje prawne, które są obce większości odbiorców. Przykładami takich pojęć są: profil zaufany, podpis elektroniczny (osobisty, kwalifikowany, zaawansowany), pieczęć elektroniczna, szyfrowanie czy pseudonimizacja. Dodatkowo przywoływane są różnego rodzaju normy i standardy, które w zasadzie nic nie mówią odbiorcom regulacji prawnych, a wywołują sprzeciw wobec tych rozwiązań. Często bowiem trudno jest zrozumieć istotę rozwiązań, a jeszcze trudniej zastosować ją w praktyce. Tym bardziej, że większość podmiotów leczniczych nie może liczyć na instytucjonalną pomoc. To co jest również niepokojące to różne interpretacje uprawnień pacjenta, które można zaobserwować w praktyce codziennej w zastosowaniu rozwiązań zawartych w Internetowym Koncie Pacjenta. Przykładem może być upoważnienie wydane przez pacjenta do dokumentacji medycznej, które nie jest respektowane w rejestracjach podmiotów medycznych i trzeba wypełniać papierowe oświadczenie w podmiocie medycznym ponownie.

Analizując nowe rozwiązania dotyczące dokumentacji medycznej widać wskazania dotyczące obowiązku posługiwania się odpowiednimi rozwiązaniami technologicznymi. Dokumentację podpisuje się 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 (ZUS). Zgodnie z zasadą, że rodzaj podpisu jest wskazywany do danej czynności prawnej przez ustawodawcę należy operować podpisami wymienionymi w przepisach. Większą dowolność rozwiązań pozostawiono do prowadzenia dokumentacji wewnętrznej. W tym przypadku można podpisać dokumentację również przy

[14] J. Makuch, M. Guziak, *Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, Tom 14, nr 2, s. 86-102, https://doi.org/10.34862/rbm.2020.2.6. (data odczytu 16.03.2021).

wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego, a więc decyzję podejmuje kierownik podmiotu leczniczego.

Rozpatrując problematykę dokumentacji w postaci elektronicznej w ochronie zdrowia, należy zauważyć, że w codziennej praktyce funkcjonuje wiele innych dokumentów elektronicznych związanych z bieżącą działalnością np. dokumenty kadrowe, księgowe lub dotyczące akcji prozdrowotnych. Tworząc dokumenty w postaci elektronicznej trzeba mieć na uwadze, że podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych (art. 25 ust. 1)[15].

Część z tych dokumentów (głównie sprawozdań z działalności spółki – m.in. sprawozdania finansowe i z działalności spółki) ma przypisane rodzaje podpisów, część natomiast nie ma. Można więc stosować podpis zwykły, który generalnie jest deklarację tożsamości osoby, która podpisała dokument. Zwykły podpis elektroniczny nie jest szczegółowo uregulowany przepisami, a jego wybór jest wynikiem decyzji podpisującego. Zwykłym podpisem elektronicznym będzie każde dodanie przez usługę służącą do składania podpisu informacji o podpisującym, gdzie podpisujący mógł podjąć decyzje o tym, że podpisuje dokument jednocześnie, jego wiarygodność zależy od tego jak zostanie zaewidencjonowany przez usługę do składania podpisów[16.] Kwalifikowany podpis elektroniczny już na mocy unijnego prawa może zostać zastąpiony podpisem własnoręcznym bez konieczności wprowadzania dodatkowych zapisów w krajowych ustawodawstwach. Odróżnia to znacząco jego moc prawną od pozostałych rodzajów podpisów elektronicznych.

Warto zwrócić uwagę na transgraniczny charakter tego podpisu. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany w Polsce. Przepisy prawne przewidują obligatoryjność kwalifikowanego podpisu elektronicznego dla wybranych dokumentów. Aktualnie podpisywanymi elektronicznie dokumentami w Polsce są kolejno: roczne sprawozdania finansowe, dokumentacja pracownicza, dokumenty finansowe oraz pełnomocnictwa.

Regulacja dotycząca dokumentacji medycznej pomija natomiast instytucje pieczęci elektronicznej. W przeciwieństwie do podpisu elektronicznego związanego z osobą fizyczną

[15] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
[16] *Zwykły, zaawansowany czy kwalifikowany podpis elektroniczny? Sprawdź jakie są różnice! | OSnews.pl.* http://osnews.pl/zwykly-zaawansowany-czy-kwalifikowany-podpis-elektroniczny-sprawdz-jakie-sa-roznice/ (data odczytu 16.03.2021).

pieczęć elektroniczna jest przypisana do osoby prawnej. Skutkiem jej złożenia jest potwierdzenie autentyczności i integralności dokumentu. Dokument oznaczony pieczęcią elektroniczna posiada dowody, że został utworzony przez podmiot identyfikowany tą pieczęcią oraz dowody, że nie zmienił swojej zawartości[17]. Innymi słowy pieczęć elektroniczna złożona na danym dokumencie elektronicznym, jest gwarantem, że dokument elektroniczny pochodzi od konkretnego wskazanego podmiotu (np. podmiotu leczniczego) oraz że zawiera określoną treść, której nie można zmienić (zasada integralności). Jeśli treść e-dokumentu zostanie zmieniona po nałożeniu e-pieczęci, wówczas na etapie weryfikacji otrzymamy komunikat o uznaniu e-pieczęci za wadliwą. Weryfikację pieczęci podobnie jak podpisu umożliwia certyfikat wystawiony przez uprawniony podmiot. Natomiast wykorzystując usługę walidacji można uzyskać informację wskazującą podmiot, który złożył daną pieczęć elektroniczną. Podsumowując, pieczęć elektroniczna działa zasadniczo tak samo jak podpis elektroniczny, przy czym[18]:

- Składającym pieczęć jest podmiot prawny, firma, urząd lub organizacja;
- Pieczęć nie jest podpisem organizacji, czyli nie jest związana z reprezentacją i nie służy do składania oświadczeń woli w imieniu organizacji;
- Potwierdza autentyczność dokumentu — dokument nią opatrzony został wystawiony przez daną organizację.
- ważność kwalifikowanej (certyfikowanej zgodnie z rozporządzeniem eIDAS) e-pieczęci – podobnie jak w przypadku kwalifikowanego podpisu elektronicznego jest domniemana, a po jej wydaniu w jednym państwie członkowskim nie można jej odrzucić w innym państwie członkowskim

Podsumowując, należy zauważyć, że e-pieczęć może się sprawdzić w obszarach, które[19]:

- wymagają zapewnienia integralności i autentyczności dokumentów na wysokim poziomie;
- preferują automatyzację wydawania dokumentów;

[17] M. Kostro, M. Tabor, *Identyfikacja i Uwierzytelnienie w Usługach Elektronicznych*, Związek Banków Polskich, Warszawa 2020, https://www.zbp.pl/getmedia/860b8ebd-4a6a-4fc9-a944-ddb8e9918f2a/ZBP_przewodnik_2020_v6 (data odczytu 16.03.2021).

[18] *Raport: Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce. 2017*. Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf (data odczytu 16.03.2021).

[19] *Raport: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (data odczytu 16.03.2021).

- przenoszą odpowiedzialność za wystawiony dokument na organizację, składającą e-pieczęć (nie ma konieczności poszukiwania osoby odpowiedzialnej indywidualnie za wystawiony e-dokument).

W ochronie zdrowia obszarem, w których nie wymaga się podpisów elektronicznych konkretnych podpisów elektronicznych (kwalifikowanego, osobistego, zaufanego lub wydawanego przez ZUS) jest dokumentacja wewnętrzna. Mimo projektowanej zmiany w przepisach nowa regulacja pozostawiła bez zmiany przepis dopuszczający jej podpisywanie również przy wykorzystaniu wewnętrznych mechanizmów systemu teleinformatycznego. Głównie mowa o rozwiązaniach dostarczanych przez firmy informatyczne wraz z oprogramowaniem do prowadzenia dokumentacji w postaci elektronicznej. Wydaje się, że w takiej sytuacji staje się możliwe wykorzystania właściwości e-pieczęci (opartej o kwalifikowany certyfikat) do dokumentów podpisywanych zwykłym podpisem elektronicznym u opatrzonego pieczęcią elektroniczną. Zwykła pieczęć nie korzysta z domniemania integralności danych i autentyczności pochodzenia danych powiązanych z tą pieczęcią. Z tego domniemania korzysta dopiero kwalifikowana pieczęć elektroniczna[20].

Taką konstrukcję można przyjąć w podmiotach leczniczych w odniesieniu do m.in. dokumentacji udostępnianej policji, sądom, prokuraturze.

W bieżącej pracy podmiotów leczniczych możliwe jest zastosowanie rozwiązania wprowadzonego w 2016 r. formę dokumentową czynności prawnych. Do zachowania tej formy wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie. Dokumentem jest dowolny nośnik informacji, który pozwala zapoznać się z jej treścią. Podstawową różnicą pomiędzy tą formą a formą pisemną (lub formą elektroniczną) jest, wobec tego brak konieczności opatrzenia dokumentu własnoręcznym podpisem (lub kwalifikowanym podpisem elektronicznym). Dochowujemy formy dokumentowej, w przypadku dokumentu w postaci tekstowej z podpisem powielanym mechanicznie (np. ksero, skan), a także wiadomości elektronicznej (mailowej) zakończonej wpisaniem imienia i nazwiska piszącego lub danymi pozwalającymi ustalić jego tożsamość. W pewnych sytuacjach będzie to też kliknięcie przycisku „Akceptuję” na stronie internetowej. Wszystkie te formy mają na celu powiązanie osoby możliwej do zidentyfikowania z informacjami przechowywanymi w formie elektronicznej. Formą dokumentową będzie, wobec

[20] *Grupa robocza ds. rejestrów rozproszonych i blockchain - Cyfryzacja KPRM - Portal Gov.pl*, https://www.gov.pl/web/cyfryzacja/blockchain (data odczytu 12.03.2020).

tego zastosowanie zarówno zwykłego podpisu elektronicznego, jak i zaawansowanego podpisu elektronicznego.

3. Rejestrowane doręczenie elektroniczne – przyjazna i bezpieczna gwarancja wzajemnej uznawalności danych

Zgodnie z art. 3 pkt. 36 eIDAS usługa rejestrowanego doręczenia elektronicznego oznacza usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany[21]. Przedmiotowa usługa świadczona przez stronę trzecią, czyli tym samym nie jest możliwe jej realizowanie przez urząd lub inny podmiot działający na rzecz komunikacji ze swoimi klientami. Wbudowany mechanizm strony trzeciej gwarantuje niezależne źródło dowodu i skutek prawny wysłania i otrzymania danych przekazanych za pomocą usługi rejestrowanego doręczenia elektronicznego. W praktyce usługa taka zapewnia skuteczną ochronę przed utratą integralności i poufności przetwarzanych danych oraz gwarantuje ich bezpieczeństwo.

Aktualnie na terenie Unii Europejskiej kwalifikowane elektroniczne doręczenia funkcjonują jedynie w pięciu państwach członkowskich, wśród których prym wiodą Włochy. Wszystkie powyższe kraje dzięki wdrożeniu usługi elektronicznego doręczenia dysponują nowoczesnymi możliwościami gwarancji wzajemnego uznawania danych, skutecznego zabezpieczania komunikacji w sektorze usług publicznych oraz jeszcze większym postępem cyfryzacji szeroko rozumianych usług administracji publicznej. Dodatkowo przykład Włoch wskazuje na nieoceniony potencjał elektronicznych doręczeń jako narzędzia usprawniającego zdalną komunikację i obsługę administracyjną w najtrudniejszych momentach pandemii[22].

W Polsce uchwalona ustawa o doręczeniach elektronicznych z dnia 18 listopada 2020 r. (Dz.U. 2020 poz. 2320), której przepisy mają wejść w życie 1 lipca 2021 roku, ma na celu określenie zasad wymiany korespondencji z podmiotami publicznymi zarówno w relacji z innymi podmiotami publicznymi oraz z podmiotami niepublicznymi, w tym z osobami

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
[22] *Raport: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (data odczytu 16.03.2021).

fizycznymi (obszar regulacji dotyczyć będzie m.in. relacji pomiędzy obywatelem a organem administracji publicznej czy pomiędzy sądem a stronami postępowania, w tym także między w/w podmiotami a sądem). Tym samym w połowie 2021 r. w naszym kraju zostanie oddana do użytku publiczna usługa rejestrowanego doręczenia elektronicznego zapewniająca cyfrowe potwierdzenie nadania i odbioru korespondencji. Dzięki takiemu rozwiązaniu wprowadzona zostanie zasada pierwszeństwa korespondencji elektronicznej przed dotychczasową przesyłanej w formie papierowej. Uproszczone zostaną obecne wymogi warunkujące możliwość prowadzenia korespondencji elektronicznej takie, jak m.in. zgoda na doręczanie elektroniczne w danej sprawie, zgoda na doręczanie elektroniczne w korespondencji z danym podmiotem, wniesienie podania drogą elektroniczną czy zarejestrowanie się w systemie[23].

Architektura funkcjonalna wprowadzanej usługi wzorowana będzie na modelu wskazanym w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE (Dz.Urz. UE z 2014 r. L 257, s. 73). Dodatkowo uchwalona ustawa przewiduje uruchomienie publicznej usługi hybrydowej adresowanej do osób wykluczonych cyfrowo, dzięki czemu takie osoby będą miały możliwość otrzymywania korespondencji nadal w formie papierowej od podmiotów publicznych wysyłających ją domyślnie w postaci elektronicznej[24].

W praktyce ustawa o doręczeniach elektronicznych nakłada szereg nowych obowiązków na podmioty publiczne oraz niepubliczne podlegające jej regulacji. Najważniejszym z nich jest obowiązek doręczania między podmiotami korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego. Standardowa przesyłka listowa została dopuszczona jedynie w drodze wyjątku i wyłącznie w razie nieskuteczności doręczenia korespondencji domyślną drogą elektroniczną. Kolejna obligację stanowi konieczność przekazania adresu do tzw. bazy adresów elektronicznych, dzięki czemu doręczanie korespondencji każdorazowo odbywać się będzie na podany adres do doręczeń elektronicznych wpisany do bazy. To zaś umożliwi odbieranie i przeglądanie korespondencji w jednym miejscu (tj. jednej skrzynce do doręczeń) i w ujednolicony sposób, a także – co istotne – nie będzie kolizyjne z możliwością dostępu do usług *online* świadczonych przez podmioty publiczne.

[23] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (data odczytu 16.03.2021).
[24] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (data odczytu 16.03.2021).

Podmioty podlegające wpisowi do KRS będą zobligowani do wyznaczenia tzw. administratora skrzynki doręczeń, czyli osobę upoważnioną do zarządzania skrzynką korespondencyjną (takie zarządzanie sprowadza się przede wszystkim do wysyłania i odbierania korespondencji oraz przydzielania osobom fizycznym uprawnień do dokonywania operacji na skrzynce). W przypadku osoby fizycznej, w tym podmiotu zarejestrowanego w CEIDG (tj. w Centralnej Ewidencji i Informacji o Działalności Gospodarczej) powyższa opcja będzie możliwa, ale nie obowiązkowa. Na potrzeby realizacji doręczeń elektronicznych powstanie nowy system teleinformatyczny[25].

Podsumowanie

Wciąż brakuje szczegółowych regulacji dokumentacji medycznej podpisanej elektronicznie m.in. w aspekcie konserwacji pieczęci elektronicznie. Przy tak dużych zmianach w technologiach technikach prowadzenia elektronicznej dokumentacji medycznej, ustawodawca powinien rozważyć zorganizowanie instytucjonalnego wsparcia dla podmiotów wdrażających nowe rozwiązania np. przez rozpisanie regionalnych przetargów na pomoc podmiotom wdrażającym nowe rozwiązania bądź na dostarczeniu rozwiązań chmurowych oferujących program do prowadzenia dokumentacji medycznej.

Literatura

[1] *Grupa robocza ds. rejestrów rozproszonych i blockchain - Cyfryzacja KPRM - Portal Gov.pl*, https://www.gov.pl/web/cyfryzacja/blockchain (data odczytu 12.03.2020).

[2] Kostro M., Tabor M., *Identyfikacja i Uwierzytelnienie w Usługach Elektronicznych*, Związek Banków Polskich, Warszawa 2020, https://www.zbp.pl/getmedia/860b8ebd-4a6a-4fc9-a944-ddb8e9918f2a/ZBP_przewodnik_2020_v6 (data odczytu 16.03.2021).

[3] Makuch J., Guziak M., *Cyberbezpieczeństwo sektora ochrony zdrowia. Przypadek Polski na tle tendencji światowych*, „Rocznik Bezpieczeństwa Międzynarodowego" 2020, Tom 14, nr 2, s. 86-102, https://doi.org/10.34862/rbm.2020.2.6. (data odczytu 16.03.2021).

[4] Najwyższa Izba Kontroli, *Wdrożenie Przez Podmioty Lecznicze Regulacji Dotyczących Ochrony Danych Osobowych*, Warszawa, 14 listopad 2019.

[5] *Raport: Przełom w Usługach Online. Rozwój Usług Zaufania w Polsce. 2017*. Obserwatorium.biz, https://obserwatorium.biz/wp-content/uploads/2019/01/Raport_Us%C5%82ugiZaufania_List2017.pdf (data odczytu 16.03.2021).

[6] *Raport: TRUSTED ECONOMY w Nowej Rzeczywistości. Ograniczanie Ryzyka Związanego z Szybką Cyfryzacją.* Obserwatorium.biz, https://obserwatorium.biz/wp-

[25] M. Wikarjak, *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (data odczytu 16.03.2021).

content/uploads/2020/09/RAPORT_TRUSTED_ECONOMY.pdf (data odczytu 16.03.2021).
[7] Rozporządzenie Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2020 poz. 666).
[8] Rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej (Dz.U. 2018 poz. 941).
[9] Rozporządzenie Ministra Zdrowia z dnia 12 sierpnia 2020 r. w sprawie standardu organizacyjnego teleporady w ramach podstawowej opieki zdrowotnej (Dz.U. 2020 poz. 1395).
[10] Rozporządzenie Ministra Zdrowia z dnia 31 października 2019 r. zmieniające rozporządzenie w sprawie świadczeń gwarantowanych z zakresu podstawowej opieki zdrowotnej (Dz.U. 2019 poz. 2120).
[11] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
[12] Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (Dz.U. 2020 poz. 374).
[13] Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016 poz. 1579).
[14] Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. 2020 poz. 2320).
[15] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. 2011 nr 113 poz. 657).
[16] Wikarjak M., *Ustawa o doręczeniach elektronicznych to także nowe obowiązki dla firm*. „Dziennik Gazeta Prawna" 1 listopad 2020, https://biznes.gazetaprawna.pl/artykuly/1494598,ustawa-o-doreczeniach-elektronicznych-administrator-e-mail.html (data odczytu 16.03.2021).
[17] *Zwykły, zaawansowany czy kwalifikowany podpis elektroniczny? Sprawdź jakie są różnice! | OSnews.pl.* http://osnews.pl/zwykly-zaawansowany-czy-kwalifikowany-podpis-elektroniczny-sprawdz-jakie-sa-roznice/ (data odczytu 16.03.2021).

Streszczenie

Postępująca transformacja dokumentacji medycznej z postaci papierowej na elektroniczną będącą wynikiem regulacji prawnych oraz zmian organizacyjnych wciąż jest wyznawaniem dla podmiotów medycznych. Jak pokazują kontrole, instytucje lecznicze popełniają wiele błędów, co może prowadzić do zagrożenia cybernetycznego. Dodatkowo powstają nowe (dla sektora ochrony zdrowia) rozwiązania technologiczne takie jak usługi zaufania czy rejestrowane doręczenie elektroniczne, które usprawniają działanie systemu informacyjnego ochrony zdrowia, ale wymagają dostawania zarówno po stronie prawodawcy jak i samych podmiotów medycznych.

Słowa kluczowe

Bezpieczeństwo danych, elektroniczna dokumentacja medyczna, usługi zaufania, teleporady, systemu informacyjnego ochrony zdrowia