Magdalena ZAMROCZYŃSKA[1]

DOI : 10.32055/mw.2021.16.3

Cyberbezpieczeństwo w ochronie zdrowia a udzielanie świadczeń telemedycznych

Wstęp

Transformacja cyfrowa systemu ochrony zdrowia jest jednym z obecnych priorytetów polskiej polityki zdrowotnej. Wprowadzono e-zwolnienia, e-recepty, e-skierowania oraz teleporady. Informatyzacja opieki zdrowotnej zmierza do całkowitego odejścia od papieru i przeniesienia danych dotyczących zdrowia Polaków do systemów informatycznych. Ma to na celu usprawnienie pracy kadry medycznej. Jednakże, informatyzacja ochrony zdrowia powinna przede wszystkim zapewniać ochronę danych wrażliwych, w szczególności w obliczu wymiany dokumentacji medycznej między podmiotami leczniczymi. System telemedyczny składa się z trzech głównych elementów: płatnika, świadczeniodawcy lub systemu opieki zdrowotnej oraz dostawcy usług. Każdy z nich musi zapewnić bezpieczeństwo swojej części systemu informatycznego w zakresie przetwarzania i przechowywania danych pacjentów. Wysiłki należy koncentrować na likwidowaniu zagrożeń i minimalizowaniu przestrzeni podatnych na błędy systemowe. Należy zatem oczekiwać, że w konsekwencji rozwoju telemedycyny i wykorzystywania zgromadzonych danych, wdrożone zostaną odpowiednie przepisy prawne dotyczące bezpieczeństwa cybernetycznego i prywatności pacjentów[2].

Jednakże, szybki rozwój usług telemedycznych przez rosnącą liczbę prywatnych i publicznych dostawców wiąże się również z nasileniem ataków cybernetycznych na sektor opieki zdrowotnej. Zatem, wszystkie podmioty zapewniające te usługi zobowiązane są zadbać o kwestię bezpieczeństwa cybernetycznego, gdyż są współodpowiedzialne za zapewnienie optymalnych korzyści przy minimalnym ryzyku dla prywatności i bezpieczeństwa danych, i systemów, w których są one świadczone. Dyscyplina cyberbezpieczeństwa w złożonym, połączonym środowisku, jakim jest opieka zdrowotna, jest wieloaspektowa i wymaga zwrócenia uwagi na podatność na zagrożenia cybernetyczne w całym łańcuchu dostarczanych usług. W celu ustalenia standardów postępowania, przede wszystkim należy dokonać przeglądu potencjalnych zagrożeń bezpieczeństwa cybernetycznego związanych z wykorzystaniem i zarządzaniem telemedycyną.

---

[1] Doktor nauk prawnych, asystent, Katedra i Zakład Prawa Medycznego i Farmaceutycznego, Wydział Medyczny, Uniwersytet Medyczny im. Karola Marcinkowskiego w Poznaniu, ORCID: 0000-0001-6760-1386.

[2] J. Siebert, J. Rumiński, *Telemedycyna*, „Forum Medycyny Rodzinnej" 2007, t. 1, nr 1, s. 1–10, Via Medica ISSN 1897–3590.

Telemedycyna w polskich przepisach prawnych

W polskim ustawodawstwie nie ma jednoznacznej definicji telemedycyny, zatem w pierwszej kolejności należy wskazać na definicję Światowej Organizacji Zdrowia (WHO), zgodnie z którą telemedycyna to „dostarczanie przez specjalistów usług medycznych, w przypadku, gdy dystans jest kluczowym czynnikiem, wykorzystując technologie komunikacyjne do wymiany istotnych informacji dla diagnozy, leczenia, profilaktyki, badań, konsultacji czy wiedzy medycznej w celu polepszenia zdrowia pacjenta". Natomiast, Amerykańskie Stowarzyszenie Telemedycyny (ATA) definiuje telemedycynę jako „formę wymiany informacji medycznych pomiędzy dwoma stronami, przebiegającą przy wykorzystaniu narzędzi telekomunikacyjnych, której celem jest poprawa stanu zdrowia pacjenta"[3].

Pomimo powszechnego dostępu do usług telemedycznych, jak również jej dynamicznego rozwoju, telemedycyna nie doczekała się jeszcze kompleksowej regulacji prawnej. Prawodawca dopuścił możliwość udzielania świadczeń telemedycznych na podstawie bardzo ogólnej regulacji zawartej w ustawie o działalności leczniczej[4]. Zgodnie z treścią art. 3 ust. 1 ustawy o działalności leczniczej: działalność lecznicza polega na udzielaniu świadczeń zdrowotnych. Świadczenia zdrowotne mogą być udzielane za pośrednictwem systemów teleinformatycznych lub systemów łączności.

Ponadto, należy wskazać, że wspomniano o możliwości zastosowania telemedycyny w ustawach regulujących niektóre zawody medyczne. Ustawa o zawodach lekarza i lekarza dentysty[5] stanowi, że wykonywanie zawodu lekarza polega na udzielaniu przez osobę posiadającą wymagane kwalifikacje, potwierdzone odpowiednimi dokumentami, świadczeń zdrowotnych. Lekarz i lekarz dentysta mogą wykonywać czynności zawodowe m.in. za pośrednictwem systemów teleinformatycznych lub systemów łączności (art. 2 ust. 4). Co więcej, treść art. 42 ust. 1 ustawy o zawodach lekarza i lekarza dentysty stanowi, że lekarz orzeka o stanie zdrowia określonej osoby po uprzednim, osobistym jej zbadaniu lub zbadaniu jej za pośrednictwem systemów teleinformatycznych lub systemów łączności. Także art. 11 ustawy o zawodach pielęgniarki i położnej[6] wskazuje, że pielęgniarka i położna wykonują zawód, z należytą starannością, zgodnie z zasadami etyki zawodowej, poszanowaniem praw pacjenta, dbałością o jego bezpieczeństwo, wykorzystując wskazania aktualnej wiedzy medycznej oraz pośrednictwo systemów teleinformatycznych lub systemów łączności. Podobnie, w art. 2a ust. 2a ustawy o izbach aptekarskich[7] dopuszcza, by niektóre usługi farmaceutyczne były udzielane przez farmaceutę za pośrednictwem systemów teleinformatycznych lub systemów łączności, m.in. w zakresie sprawowania opieki farmaceutycznej w celu uzyskania określonych jej efektów poprawiających jakość życia pacjenta. Na marginesie należy podkreślić, że pozostałe zawody medyczne, tj.

[3] https://www.americantelemed.org/, 30.11.2021.

[4] Ustawa z 15 kwietnia 2011 r. *o działalności leczniczej*, Dz. U. 2011, Nr 112, poz. 654 ze zm.

[5] Ustawa z 5 grudnia 1996 r. *o zawodach lekarza i lekarza dentysty*, Dz. U. 1997, Nr 28, poz. 152 ze zm.

[6] Ustawa z 15 lipca 2011 r. *o zawodach pielęgniarki i położnej*, Dz. U. 2011, Nr 174, poz. 1039 ze zm.

[7] Ustawa z 19 kwietnia 1991 r. *o izbach aptekarskich*, Dz. U. 1991, Nr 41, poz. 179 ze zm.

ratownicy medyczni, diagności laboratoryjni czy też fizjoterapeuci nie zostały objęte podobnymi regulacjami, lecz nie oznacza to, że nie mogą oni korzystać ze środków telemedycyny, gdyż podstawową regulacją wprowadzającą możliwość wykonywania zawodów medycznych z zastosowaniem telemedycyny jest wspomniany powyżej art. 3 ustawy o działalności leczniczej, który jednoznacznie wskazuje na możliwość wykonywania działalności leczniczej z użyciem środków informatycznych w zakresie udzielania świadczeń zdrowotnych. Inna interpretacja obowiązujących przepisów doprowadziłaby do kuriozalnych sytuacji decyzyjnych w zakresie opieki nad pacjentem, a w konsekwencji do utrudnienia wykonywania pracy przez np. ratowników medycznych współpracujących z lekarzami czy też pielęgniarkami wykorzystującymi systemy teleinformatyczne do świadczenia usług opieki zdrowotnej[8].

Bezpieczeństwo cyfrowe związane z udzielaniem świadczeń telemedycznych

Wykorzystanie telemedycyny wiąże się z przetwarzaniem danych osobowych pacjentów podlegających szczególnej ochronie prawnej[9]. Przetwarzane są zarówno dane identyfikacyjne, takie jak: imię i nazwisko czy też miejsce zamieszkania, jak również dane wrażliwe, np. informacja o grupie krwi lub wyniki badań diagnostycznych. Zasady przetwarzania danych osobowych gromadzonych przy okazji udzielania świadczeń telemedycznych oraz prowadzenia dokumentacji medycznej są uregulowane w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta[10], ustawie o ochronie danych osobowych[11] oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (ogólne rozporządzenie o ochronie danych osobowych, tzw. RODO)[12]. Nie ulega żadnej wątpliwości, że zapewnienie odpowiedniego poziomu bezpieczeństwa gromadzonych informacji jest kluczowe dla istnienia i właściwego świadczenia usług telemedycznych w zakresie ochrony zdrowia[13].

Podczas oceny rozwiązań telemedycznych należy wziąć pod uwagę obszary ryzyka związanego z bezpieczeństwem cybernetycznym w łańcuchu dostaw: wybór technologii, która ma być wykorzystana, projektowanie przepływu usług między świadczeniodawcami a świadczeniobiorcami oraz sposób przetwarzania danych. Zatem, po

[8] Telemedyczna Grupa Robocza, *Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia?*, Warszawa 2018, http://telemedycyna-raport.pl/#raport, 30.11.2021.

[9] A. Romaszewski, W. Trąbka, *Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2014, nr 33, s. 37–38.

[10] Ustawa z dnia 6 listopada 2008 r. *o prawach pacjenta i Rzeczniku Praw Pacjenta*, Dz. U. 2020, poz. 849.

[11] Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych*, Dz. U. 2018, poz. 1000.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 z 2016, nr 119, str. 1* (ogólne rozporządzenie o ochronie danych, tzw. RODO).

[13] A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Wolters Kluwer Polska, wydanie I, 2018, s. 98–152.

pierwsze wdrażanie technologii powinno obejmować rozważania w zakresie ryzyka, jakie mogą nieść ze sobą rozwiązania technologiczne w dziedzinie telemedycyny, należy zwrócić uwagę na nadrzędne kwestie związane z procesem oceny technologii i sposobu, w jaki będzie ona wdrażana i zarządzana od początku do końca, a także powinny obejmować odpowiednie testy administracyjne i testy bezpieczeństwa przed użyciem. Planowanie poprawek, konserwacji, aktualizacji, tworzenia kopii zapasowych oraz tymczasowych i wycofania technologii z eksploatacji musi być proaktywne. Należy w tym miejscu również wspomnieć o konieczności rozważenia perspektywy odpowiedniej reakcji na ewentualne awarie i wyłączenia systemu, zwłaszcza w okresie nasilenia cybernetycznych włamań z zewnątrz, a w konsekwencji wskazać na rozwiązania alternatywne. Częścią planu operacyjnego powinno być również stałe monitorowanie technologii i bieżące rozwiązywanie problemów takich jak zmiany w konfiguracji systemu, zmiany kont, zmiany uprawnień administratorów. Istotne jest również ciągłe szkolenie i świadomość użytkowników systemu, których z wyprzedzeniem należy odpowiednio poinstruować w zakresie zastosowanych rozwiązań, wytycznych dotyczących użytkowania oraz uwierzytelniania danych i weryfikacji tożsamości (np. pacjenta), tak aby nie powodowali oni niezamierzonych negatywnych konsekwencji w postaci incydentów związanych z niewłaściwym dostępem czy też ujawnieniem informacji. Na koniec należy skontrolować zabezpieczenia w zakresie poufności zgodnie z rodzajem danych, które będą wykorzystywane, udostępniane i zarządzane w związku z korzystaniem z cyfrowego rozwiązania zdrowotnego, a także wymagania dotyczące rozwiązania lub procesu wymiany informacji pomiędzy świadczeniodawcą a użytkownikiem końcowym, czyli pacjentem, jak również sposób ochrony takich informacji, np. poprzez wykorzystanie szyfrowania danych.

W celu uregulowania problematyki cyberbezpieczeństwa w Polsce, również w odniesieniu do służby zdrowia, uchwalono ustawę o krajowym systemie cyberbezpieczeństwa[14]. Ustawa ta za cyberbezpieczeństwo (art. 2 pkt 4 ustawy) uznała odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych w nich danych lub związanych z nimi usług (a więc także medycznych i farmaceutycznych, świadczonych w sposób tradycyjny oraz w ramach telemedycyny). Ustawa ta koresponduje w zakresie zagadnienia cyberbezpieczeństwa z unormowaniami dotyczącymi przetwarzania danych osobowych wskazanymi w ustawie o ochronie danych osobowych oraz rozporządzeniu RODO. Ponadto, zdefiniowano w omawianej ustawie nie tylko na cyberbezpieczeństwo, ale również incydent „zwykły", incydent krytyczny, incydent poważny czy też incydent istotny. Ponadto, ustawa reguluje również funkcjonowanie operatorów usług kluczowych, czyli m.in. największych banków, firm z sektora energetycznego, przewoźników lotniczych i kolejowych, armatorów, szpitali; funkcjonowanie dostawców usług kluczowych, czyli m.in. internetowych platform handlowych; organów właściwych, czyli instytucji publicznych, w których kompetencjach jest nadzór nad danym istotnym sektorem dla polskiej gospodarki; funkcjonowanie Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego. Podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa mają w założeniu tworzyć spójny

[14] Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa*, Dz. U. 2018, poz. 1560.

system pozwalający na podejmowanie różnorodnych i skutecznych działań zarówno przeciwdziałających zagrożeniom, jak i zapewniających skuteczne reagowanie w przypadku wystąpienia incydentów. W załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa wskazano na sektor ochrony zdrowia, w którym wyróżniono podmioty, do których odnosi się analizowana regulacja prawna (jako tzw. operatorów usług kluczowych). Zgodnie z treścią załącznika nr 1 są to: podmioty lecznicze – będące przedsiębiorcami prowadzącymi działalność na podstawie ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. W tym przypadku chodzi o wszystkie formy organizacyjne przewidziane dla prowadzenia tego rodzaju działalności gospodarczej (zarówno indywidualnej, jak i w formie np. spółek prawa handlowego); Centrum Systemów Informacyjnych Ochrony Zdrowia, jako jednostka podległa ministrowi zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia (w tym wdrażanie rozwiązań z zakresu tzw. e-zdrowia: elektronicznej dokumentacji medycznej i e-recept[15]); Narodowy Fundusz Zdrowia (w szczególności, jako administrator danych osób podlegających ubezpieczeniu zdrowotnemu); podmiot leczniczy, w przedsiębiorstwie, którego (tj. w szpitalu) funkcjonuje dział farmacji szpitalnej lub apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne; przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy Prawo farmaceutyczne; przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego; importer i wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy Prawo farmaceutyczne; importer równoległy i dystrybutor substancji czynnej w rozumieniu ww. ustawy; przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy Prawo farmaceutyczne[16].

Ustawa o krajowym systemie cyberbezpieczeństwa jest wsparta licznymi rozporządzeniami, do najistotniejszych należą:

1. Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[17] – ustawa o krajowym systemie cyberbezpieczeństwa nakłada na operatorów usług kluczowych obowiązki dotyczące m.in. szacowania ryzyka wystąpienia incydentu, stosowania właściwych środków bezpieczeństwa oraz obsługi i zarządzania incydentami; o uznaniu danego podmiotu za operatora usługi kluczowej zdecydują, kompetentne dla danego sektora, organy właściwe (w drodze decyzji administracyjnej); usługi kluczowe wymienione w rozporządzeniu obejmują następujące sektory: energię (m.in. energia elektryczna, ciepło, ropa i gaz);

[15] A. Romaszewski, W. Trąbka, M. Kielar, K. Gajda, *Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2017, nr 44, s. 14.

[16] K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Wolters Kluwer Polska 2019, wyd. I.

[17] Rozporządzenie Rady Ministrów z dnia 11 września 2018 r. *w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych*, Dz. U. 2018, poz. 1806.

transport (z podziałem na wodny, lądowy i powietrzny); bankowość i infrastrukturę rynków finansowych; uzdatnianie wody i odprowadzanie ścieków; ochronę zdrowia (w tym szpitale i przemysł farmaceutyczny); infrastrukturę cyfrową.

2. Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny[18] – zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa operatorzy usług kluczowych mają obowiązek zgłaszać incydenty bezpieczeństwa, które dotyczą świadczonych przez nich usług kluczowych, w szczególności w zakresie incydentów poważnych, tzn. takich, które powodują lub mogą spowodować poważnego obniżenia jakości lub przerwania ciągłości świadczenia usługi kluczowej; rozporządzenie ustala progi, które określają warunki, kiedy należy uznać dany incydent za poważny. W przypadku ochrony zdrowia poza przyjmowanymi również dla innych sektorów funkcjonowania państwa wartościami czasu utrzymywania się braku dostępności danej usługi, wyróżniono również czynniki charakterystyczne tylko dla systemu zdrowotnego. We wskazanym rozporządzeniu wyróżniono takie incydenty. Odnoszą się one do:
   - systemu udzielania świadczeń opieki zdrowotnej dla zdefiniowanych progów w postaci braku dostępności do takich świadczeń powyżej 24 godzin (np. świadczeń lekarza podstawowej opieki zdrowotnej) oraz braku poufności lub integralności danych przetwarzanych w tej usłudze (np. „wyciek" części danych osobowych pacjentów);
   - gromadzenia i udostępniania Elektronicznej Dokumentacji Medycznej dla progów w postaci braku dostępności do takiej dokumentacji powyżej 1 godziny, braku poufności lub integralności danych przetwarzanych w tej usłudze (np. udostępnienie dokumentacji medycznej pacjenta[19] osobie przez niego nieuprawnionej);
   - zarządzania danymi epidemiologicznymi dla progów w postaci braku dostępności do takich danych powyżej 2 godzin, braku poufności lub integralności danych przetwarzanych w tej usłudze;
   - obrotu i dystrybucji produktów leczniczych dla progów w postaci braku dostępności do takich produktów powyżej 24 godzin, braku poufności lub integralności danych przetwarzanych w tej usłudze;
   - dowodzenia jednostkami systemu Państwowego Ratownictwa Medycznego dla progów w postaci braku dostępności do usług powyżej 1 godziny; – spowodowania, co najmniej jednej z okoliczności: śmierci człowieka, ciężkiego uszczerbku na zdrowiu, innego niż ciężki uszczerbek na zdrowiu więcej niż jednej osoby oraz braku poufności i integralności danych przetwarzanych w tej usłudze (np. nieuzasadniany dostęp do kart medycznych czynności ratunkowych, jako części dokumentacji medycznej pacjenta)[19].
3. Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wy-

[18] Rozporządzenie Rady Ministrów z dnia 31 października 2018 r. *w sprawie progów uznania incydentu za poważny*, Dz. U. 2018, poz. 2180.

[19] P. Lipowski, *Uwarunkowanie prawne cyberbezpieczeństwa w placówkach ochrony zdrowia – wybrane zagadnienia*, „Polski Przegląd Nauk o Zdrowiu" 2019, nr 3 (60), s. 204–209.

korzystywanego do świadczenia usługi kluczowej[20] – rozporządzenie wskazuje rodzaje i zawartość dokumentacji, którą zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, powinien posiadać każdy operator usługi kluczowej. Rozporządzenie wskazuje dwa główne rodzaje dokumentacji: normatywną i operacyjną. Dokumentacja normatywna to dokumentacja dotycząca: systemu zarządzania bezpieczeństwem informacji, ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa, systemu zarządzania ciągłością działania usługi kluczowej, systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Z punktu widzenia ustawy istotna jest tylko dokumentacja dotycząca usługi kluczowej. Natomiast, dokumentacja operacyjna reguluje procedury, instrukcje i czynności wynikające z dokumentacji normatywnej.

4. Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu[21] – wśród obowiązków nakładanych na operatorów usług kluczowych ustawa wymienia audyty systemów bezpieczeństwa. Systemy bezpieczeństwa są indywidualne dla każdego przedsiębiorcy objętego regulacją, dlatego nie wskazano zakresu audytu. Może być on różny dla operatorów w zależności od sektora, a sposób przeprowadzenia audytu wybiera operator usługi kluczowej i to on decyduje, która droga będzie dla niego najbardziej odpowiednia. Czynnikami, które powinien brać pod uwagę, jest wielkość działalności, jej obszar, rodzaj świadczonych usług oraz wykorzystywane systemy teleinformatyczne. Sposób przeprowadzenia audytu powinien być adekwatny do działalności operatora.
5. Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[22] – rozporządzenie umożliwia optymalny dobór zabezpieczeń do różnorodnych warunków, w których świadczone są usługi kluczowe. Największym udogodnieniem dla przedsiębiorców jest możliwość realizacji zadań z zakresu cyberbezpieczeństwa poza bezpiecznymi pomieszczeniami i wykonywania tej pracy zdalnie, co ułatwia pracę i obniża jej koszty. Sprecyzowano również istniejące wymogi, które są teraz ściśle związane z realizowanymi obowiązkami, a także wyraźnie określono obowiązek stosowania zabezpieczeń adekwatnych do oszacowanego ryzyka w danej instytucji.

Wskazane powyżej akty prawne zostały zainicjowane w 2018 roku, a rozwiązania w nich przyjęte mają być systematycznie wdrażane w ramach krajowego systemu cy-

[20] Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej*, Dz. U. 2018, poz. 2080.

[21] Rozporządzenie Ministra Cyfryzacji z dnia 12 października 2018 r. *w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu*, Dz. U. 2018, poz. 1999.

[22] Rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. *w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*, Dz. U. 2019, poz. 2479.

berbezpieczeństwa. Ochrona zdrowia została uwzględniona w ramach tych przepisów, ale nie są to przepisy skoncentrowane na służbie zdrowia. W związku z pandemią COVID-19, aby zabezpieczyć pacjentów w zakresie przetwarzania ich danych osobowych i dynamicznym rozwojem telemedycyny, Ministerstwo Cyfryzacji sporządziło w kwietniu 2020 roku „Rekomendacje cyberbezpieczeństwa dla podmiotów sektora ochrony zdrowia", zastrzegając jednocześnie, że jest to poradnik, który nie wyczerpuje „listy wszystkich środków, które można wdrożyć w celu ochrony przed zagrożeniem systemów informacyjnych, ale są przygotowane w celu szybkiego wdrożenia minimalnych zaleceń bezpieczeństwa, z uwagi na wyjątkową sytuację związaną z pandemią COVID-19 i krytycznym znaczeniem zapewnienia niezakłóconego świadczenia usług przez placówki ochrony zdrowia"[23].

We wskazanym dokumencie przestawiono następujący zestaw rekomendowanych środków przeciwdziałających oraz ograniczających skutki incydentu związanego z cyberbezpieczeństwem:

1) wskazano, że należy blokować możliwość uruchamiania, szczególnie w dokumentach *.doc* i *.docx*, „*active content*" i „makr", przy użyciu ustawień systemowych, gdyż są one wykorzystywane do dystrybucji *malware*;
2) konieczność pozostawienia aktywnych tylko tych usług, które są niezbędne dla funkcjonowania organizacji. Usługi te obejmują w szczególności komunikację, która jest: niezbędna do funkcjonowania usług opartych na danym systemie; niezbędna dla bezpieczeństwa samego systemu (zdalne monitorowanie, aktualizacje bezpieczeństwa systemów itp.); niezbędna do informowania opinii publicznej (komunikacja *e-mail* itp.); niezbędna do obsługi infrastruktury łączności (sprawdzanie ważności certyfikatów itp.);
3) obowiązek tworzenia kopii zapasowych *offline* i weryfikacji przesłanych danych poza środowiskiem produkcyjnym pod względem spójności i funkcjonalności. Procedura ta jest kluczowa dla zapewnienia, że kopie zapasowe nie zostaną utracone, jeśli serwer kopii zapasowych lub platforma wirtualna zostaną naruszone (lub zaszyfrowane) np. w wyniku ataku typu *ransomware*. Kroki te należy podjąć w przypadku najbardziej krytycznych systemów, a podczas badania plików kopii zapasowych nie należy ignorować żadnych wzajemnych zależności;
4) instalacja i zapewnienie aktualizacji oprogramowania antywirusowego w celu ochrony przed złośliwym kodem (program antywirusowy czy *antymalware*) powinno być zainstalowane we wszystkich możliwych systemach operacyjnych;
5) pozostałe rekomendacje, które można wdrożyć, aby zapobiec skutkom incydentu lub je ograniczyć**:**
   a) wymuszenie zmiany haseł wszystkich kont uprzywilejowanych,
   b) kontrola wszystkich kont uprzywilejowanych i blokowanie tych, które nie są już używane lub usunięcie uprawnień dla tych kont, które nie potrzebują tych uprawnień,

[23] *Poradnik – rekomendacje cyberbezpieczeństwa dla podmiotów sektora ochrony zdrowia. Zestaw rekomendowanych minimalnych środków przeciwdziałających skutkom incydentu cyberbezpieczeństwa* (Kwiecień 2020 r.), https://www.gov.pl/web/baza-wiedzy/poradnik---rekomendacje-cyberbezpieczenstwa-dla-podmiotow-sektora-ochrony-zdrowia-kwiecien-2020-r, 30.11.2021.

c) uniemożliwienie administratorom domen logowania się na dowolnych stacjach roboczych i serwerach, a w konsekwencji uniemożliwienie atakującemu przejęcie konta uprzywilejowanego,
d) oddzielenie systemu tworzenia kopii zapasowych od innych systemów, aby nawet uzyskanie „*highest-level"* uprawnień autoryzacyjnych do systemu, dla którego utworzono kopię zapasową, nie pozwoliło na usunięcie albo uszkodzenie kopii zapasowych,
e) zapobieganie wszelkim dostępom i wzajemnym połączeniom między systemami ważnymi dla zapewnienia funkcjonowania organizacji i systemów lub sieci, które nie są ważne dla świadczenia usług lub bezpieczeństwa systemu,
f) sprawdzenie segmentacji sieci i zarządzania ruchem między segmentami (porty między segmentami, ograniczenia dotyczące dozwolonych usług), co może znacząco ograniczyć skutki potencjalnego zdarzenia związanego z incydentem,
g) aktualizacja i przetestowanie wszystkich dostępnych systemów, w celu zwiększenia ich bezpieczeństwa i odporności na incydenty. Jeżeli istnieje niepodważalny powód, aby nie dokonywać aktualizacji systemu (na przykład, aktualizacja spowodowałaby unieważnienie gwarancji, system mógłby się rozpaść, przestać działać lub mogłyby wystąpić inne niedopuszczalne skutki), nie ma potrzeby dokonywania aktualizacji takiego systemu. Konieczne będzie jednak podjęcie zastępczych środków bezpieczeństwa,
h) zbadanie planów ciągłości działania i planów działania na wypadek awarii związanych z funkcjonowaniem systemów, aby zweryfikować ich ważność, skuteczność i przydatność, w szczególności w odniesieniu do możliwej niedostępności tych systemów, jak również zagwarantowanie, aby były one przechowywane oddzielnie od systemów, dla których plany te są przetwarzane (np. na oddzielnym nośniku pamięci, w formie drukowanej itp.),
i) nieusuwanie żadnych danych dotyczących incydentu bez zgody organów ścigania, a ponadto należy poinformować wszystkich administratorów oraz wszystkich zajmujących się w danej jednostce bezpieczeństwem i bezpieczeństwem IT w zakresie tego obowiązku;

6. wyłącznie dla podmiotów świadczących usługi zdrowotne: odseparowanie sprzętu medycznego np. tomografów komputerowych, urządzeń rentgenowskich, od reszty sieci, aby ograniczyć rozprzestrzenianie się *malware*. W celu umożliwienia kontynuacji świadczenia wymaganych usług nawet po incydencie, sprzęt medyczny musi być oddzielony od innych systemów w taki sposób, aby sprzęt ten był sprawny nawet po odłączeniu od reszty sieci. Otwarte porty między sieciami są dozwolone, ale muszą być zarządzane za pomocą listy dozwolonej łączności. Środki te są istotne dla zachowania bezpieczeństwa tych systemów.

Zakończenie

Opieka zdrowotna staje obecnie w obliczu coraz większych problemów związanych z wymaganiami dotyczącymi autoryzacji użytkowników, uwierzytelniania i rozliczal-

ności – wszystkie te kwestie są również powszechne w innych branżach, takich jak bankowość. Ponieważ telemedycyna wiąże się z gromadzeniem i przesyłaniem osobistych, intymnych informacji zdrowotnych oraz informacji umożliwiających identyfikację osób-pacjentów, nieuchronnie stanowią one dla hakerów niezwykle cenny cel. Usługi składające się na telemedycynę będą celem ataków w cyberprzestrzeni, po pierwsze dlatego, że jest to po prostu, łatwy cel, szczególnie z powodu typowej podatności na próby przechwycenia przetwarzanych (a więc będących w ruchu) danych elektronicznych oraz integracji wielu sieci i technologii. Integracja wielu sieci/technologii oznacza brak ujednoliconej polityki bezpieczeństwa oraz brak centralnego zarządzania, co sprawia, że bezpieczeństwo systemu zależy od najsłabszego ogniwa. Po drugie, przetwarzane dane są niezwykle prywatne i intymne, więc są one interesujące dla osób chcących manipulować tymi danymi albo chcących wykorzystać je do szantażu czy też dla okupu, w szczególności w sytuacji, gdy dotyczyć one będą osób kluczowych z punktu widzenia rządzenia państwem.

Podczas opracowywania systemu telemedycznego należy zwrócić uwagę na liczne kwestie związane z bezpieczeństwem cybernetycznym. System telemedyczny składa się z trzech głównych elementów: płatnika, świadczeniodawcy lub systemu opieki zdrowotnej oraz dostawcy usług telemedycznych. Każdy z nich musi zapewnić bezpieczeństwo swojej części programu. Każdy z nich musi ustanowić skuteczny program bezpieczeństwa cybernetycznego, który może chronić systemy przetwarzające lub przechowujące dane zdrowotne. Organizacje powinny traktować bezpieczeństwo cybernetyczne jako podstawową zasadę. Stosowanie przepisów dotyczących ochrony danych osobowych oraz rozwijanie ochrony systemów informatycznych przed cyberatakami poprzez wdrażanie krajowego systemu cyberbezepieczeństwa jest niezbędne z uwagi nie tylko na stały rozwój i zwiększanie zastosowania telemedycyny, ale również powszechną informatyzację administracji państwowej. Wykorzystywanie telemedycyny świadczy o zrozumieniu i otwarciu się na możliwości oferowane przez nowoczesne rozwiązania technologiczne mogące przynieść korzyść pacjentom, jednakże bezpieczne korzystanie z tych narządzi wymaga nie tylko przestrzegania wspomnianych powyżej, już istniejących przepisów prawnych, ale również ustanowienie jednolitego zestawu standardów cyberbezpieczeństwa.

Streszczenie

Telemedycyna, jako forma udzielania świadczeń zdrowotnych, niewątpliwie ułatwia kontakt lekarza z pacjentem, ale niesie ze sobą również pewne zagrożenia wynikające z przekazywania danych wrażliwych dotyczących pacjentów. Niewątpliwie telemedycyna jest formą uzupełnienia medycyny tradycyjnej, która nie może się rozwijać bez wytycznych i standardów organizacyjnych, w szczególności wobec pandemii COVID-19, która spopularyzowała usługi e-zdrowia. Celem artykułu jest przedstawienie rozwiązań prawnych obowiązujących w Polsce w zakresie cyberbezpieczeństwa oraz zagrożeń związanych z ujawnieniem danych pacjentów podczas udzielania świadczeń telemedycznych.

Słowa kluczowe: bezpieczeństwo cyfrowe, etyka, telemedycyna

Cyber security in health care and the provision of telemedicine services

Summary

Telemedicine undoubtedly facilitates the contact between the physician and the patient as a form of providing health services. Still, it also carries certain risks resulting from the transfer of sensitive data concerning patients. Undoubtedly, telemedicine is a form of complementing traditional medicine, which cannot develop without guidelines and organisational standards, especially in view of the COVID-19 pandemic, which popularised e-health services. The article aims to present legal solutions binding in Poland in the scope of cyber security and threats connected with disclosing patients' data during the provision of telemedicine services.

Key words: digital security, ethics, telemedicine