Informatyzacja zasobów podmiotów wykonujących działalność leczniczą. Interoperacyjność i ochrona danych – jak to działa?

Kajetan Wojsyk[1]

Celem niniejszego opracowania jest zwrócenie uwagi na specyfikę bardzo złożonego systemu, jakim jest system informacji w ochronie zdrowia, w ramach którego dochodzi do przetwarzania danych. Po pierwsze, chodzi tutaj o dane, których powszechne i bezwarunkowe udostępnienie stanowi korzyść społeczną i które mogą być wykorzystywane do różnych celów, niekoniecznie jedynie tego, dla którego system ten został stworzony. Po drugie, są to dane, które muszą być chronione, gdyż są danymi osobowymi, w tym danymi szczególnych kategorii.

Uwagi wstępne

System informacji w ochronie zdrowia regulowany jest ustawą z 28.4.2011 r. o systemie informacji w ochronie zdrowia[2]. Jego funkcjonalność jest uzależniona od jakości i kompletności elementów składowych – różnego rodzaju rejestrów podmiotowych i przedmiotowych, w tym także rejestrów funkcjonujących w ramach odrębnych systemów. Rejestry te należy traktować jako swoiste zbiory danych gromadzonych dla osiągnięcia konkretnych celów, również regulowanych ustawowo. Trzeba równocześnie umieć świadomość, że owe rejestry tworzone były w różnym czasie, w oparciu na różne podstawy prawne oraz technologie – i co do zasady są autonomiczne. Jednak systematyczna informatyzacja obszarów bezpośrednio niezwiązanych z ochroną zdrowia (np. ewidencji działalności gospodarczej, ewidencji ludności, ewidencji podatników, statystyki) pozwala na kreowanie większych przestrzeni informacyjnych, w których można tworzyć systemy o znacznie większej przydatności i użyteczności funkcjonalnej. W tym kontekście niezwykle istotne było wprowadzenie podstawy prawnej tzw. interoperacyjności systemów[3]. Interoperacyjność to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych[4].

Separacja danych, szyfrowanie, bezpieczne przechowywanie danych oraz dokumentów

Systemu informacji w ochronie zdrowia nie należy pojmować jako jednolitego systemu o ściśle określonej strukturze, systemu, którego poszczególne elementy składowe daje się jednoznacznie i raz na zawsze opisać. Jest on raczej stale zmieniającym się systemem rozproszonym, którego granice systematycznie się poszerzają, a elementy składowe muszą podlegać stałej poprawie jakości. Aby dokładniej wyobrazić sobie specyfikę tego systemu, wystarczy przyjąć, że jego istotą jest gromadzenie i przetwarzanie danych dotyczących stanu zdrowia i historii leczenia osób fizycznych, z uwzględnieniem nie tylko tych danych, ale także danych opisujących miejsca wykonywania działalności leczniczej, osób wykonujących tę działalność (pracowników medycznych i pracowników pomocniczych), przepływu środków finansowych związanych z realizacją poszczególnych procedur leczniczych, rejestracji okresów niezdolności do pracy i wielu jeszcze innych danych.

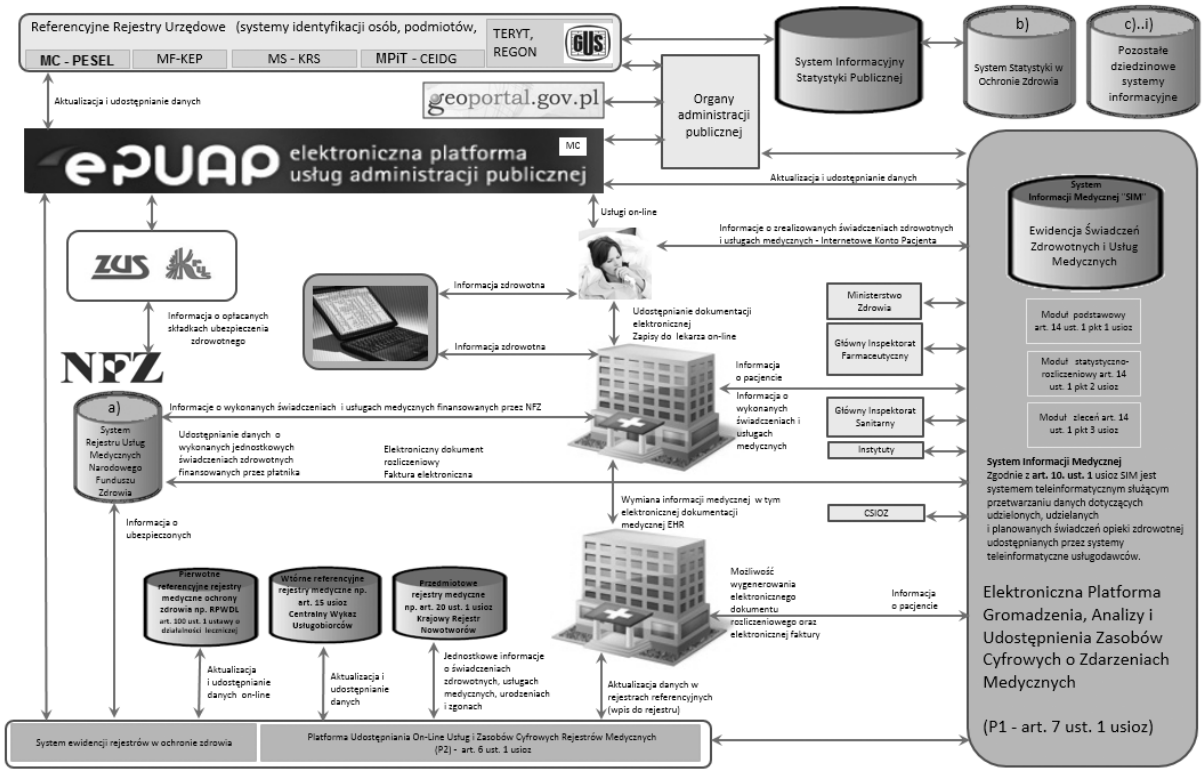
Jest kwestią oczywistą, że owa różnorodność danych wymaga odpowiedniej organizacji sposobu ich gromadzenia, porządkowania, bezpiecznego przechowywania i udostępniania osobom uprawnionym. Wymagane jest też pewne i wyraźne kanalizowanie przepływu danych i informacji, by zachować funkcjonalność, jaką jest separacja danych chronionych, a z drugiej strony zapewnić możliwość organizacji danych w jednolite zbiory, z których system pozwoli tworzyć zestawienia, raporty i dokumenty adekwatne do rzeczywistych potrzeb odbiorców informacji.

[1] Autor jest ekspertem do spraw jakości danych w Centrum Systemów Informacyjnych Ochrony Zdrowia w Warszawie, pełnomocnikiem Ministra Zdrowia ds. otwartości danych publicznych.

[2] T.j. Dz.U. z 2017 r. poz. 1845 ze zm.

[3] Rozporządzenie Rady Ministrów z 12.4.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247 ze zm.).

[4] Ustawa z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2017 r. poz. 570 ze zm.).



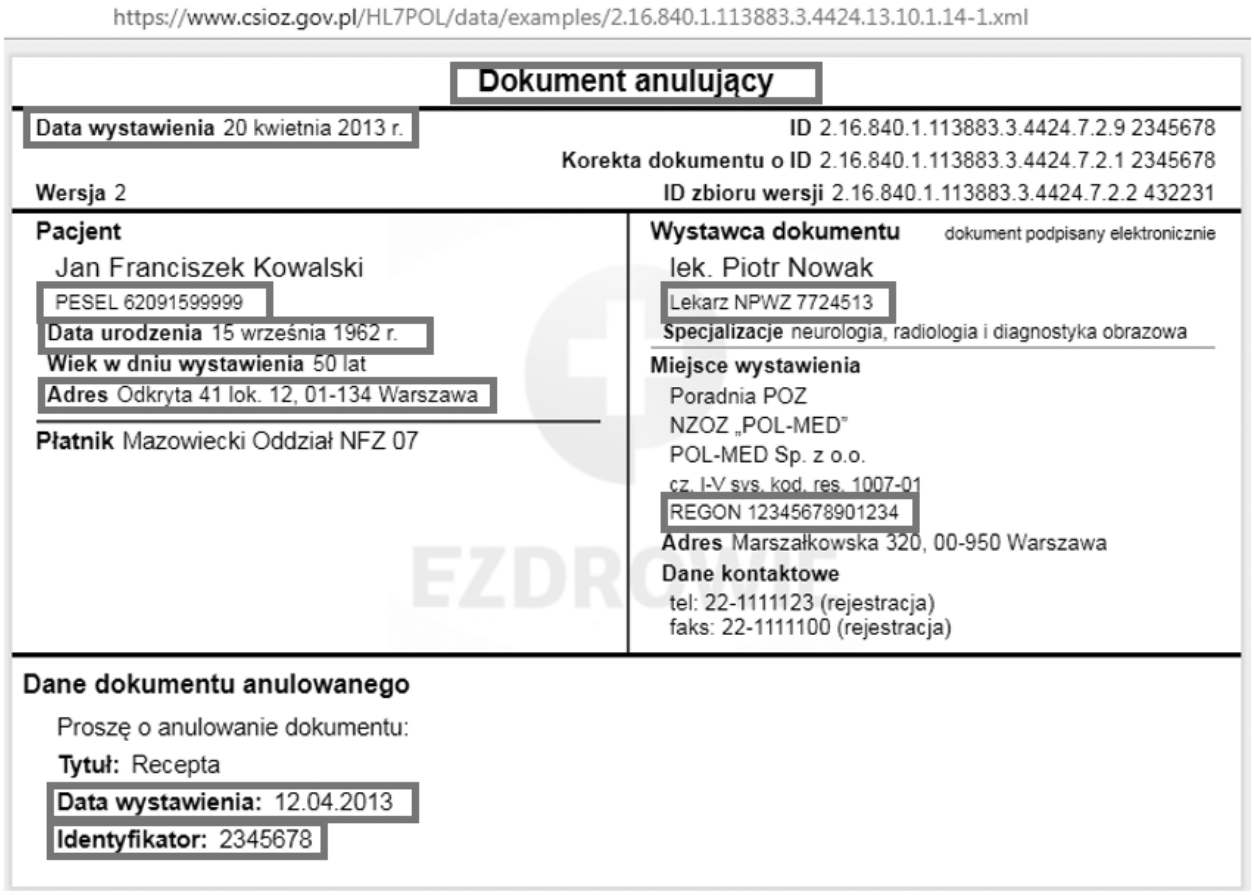
Rys. 1. Schemat systemu informacji w ochronie zdrowia[5] (opr. własne) przedstawia schematycznie (skrótowo) przepływy danych między jego własnymi i obcymi rejestrami oraz bazami danych

Na rys. 1 pokazano schemat (opr. własne), z którego wynika, że budowa systemu informacji w ochronie zdrowia jest przedsięwzięciem niezwykle skomplikowanym. Jest to podyktowane nie tylko rozległością terytorialną, różnorodnością elementów składowych, tym, że poszczególne elementy zarządzane są przez niezależne podmioty nawet pozornie niemające nic wspólnego z ochroną zdrowia, ale również tym, że budowa tego systemu jest działaniem niekończącym się, w trakcie którego pojawiają się (dołączane są) nowe systemy. Faktem jest, że niektóre zbiory danych, rejestry wchodzące w skład systemu informacji w ochronie zdrowia, opublikowane w portalu https://dane.gov.pl aktualizowane są w trybie codziennym, gdyż niemal każdego dnia pojawiają się lub są likwidowane gabinety lekarskie, apteki, ewentualnie zmienia się tylko miejsce działalności (adres), własność lub nazwa. W czasie tej niekończącej się rozbudowy powstają nowe relacje, nowe połączenia międzysystemowe, które mogą – jeśli proces ten nie będzie odpowiednio nadzorowany, prowadzić do naruszenia ochrony danych, ujawnienia informacji i dokumentów ustawowo podlegających ochronie. Ochronie podlegają nie tylko dane, ale przede wszystkim relacje między nimi, co właśnie ujawniają dokumenty. Skuteczna ochrona danych polega m.in. na zarządzaniu relacjami między danymi – ich tworzeniu lub zrywaniu. Należy jednak pamiętać, że można coś zobaczyć, ale nie da się tego procesu odwrócić („odzobaczyć") – informacji uwolnionej nie można z powrotem utajnić. Z tego powodu dokumenty przesyłane poza systemem powinny być zabezpieczane np. przez ich szyfrowanie lub silne hasło.

Dokumenty w ochronie zdrowia mają swoją specyfikę, niezależną od tego, czy występują w postaci papierowej czy elektronicznej. Ich zawartość informacyjną (dane i informacje) określają przepisy prawa. I tak np. pojęcie elektronicznej dokumentacji medycznej wprowadza ustawa o systemie informacji w ochronie zdrowia. Specyfika dokumentów w postaci elektronicznej wynika z ich budowy strukturalnej, umożliwiającej utworzenie dokumentu zgodnego ze wzorem zdefiniowanym w określonym, międzynarodowym standardzie (HL7 CDA), oraz maszynowe odczytanie danych zawartych w tym dokumencie i ich przetworzenie. W Polsce podmiotem powołanym do publikowania wzorów dokumentów medycznych jest Centrum Systemów Informacyjnych Ochrony Zdrowia[6].

[5] Ten sam system, lecz zobrazowany nieco inaczej (w mniejszym uproszczeniu, czyli bardziej szczegółowy – w papierowej wersji artykułu byłby całkowicie nieczytelny) został zamieszczony na stronie internetowej Centrum Systemów Informacyjnych Ochrony Zdrowia pod adresem: https://www.csioz.gov.pl/fileadmin/user_upload/Broszury/schemat_systemu_informacji_w_ochronie_zdrowia_56b0c687980a6.pdf. (dostęp z 11.1.2019 r.).

[6] Wzory dokumentów medycznych publikowane są na stronie: https://www.csioz.gov.pl/HL7POL/pl-cda-html-pl-PL/ (dostęp z 11.1.2019 r.).


https://www.csioz.gov.pl/HL7POL/data/examples/2.16.840.1.113883.3.4424.13.10.1.14-1.xml

Dokument anulujący

Data wystawienia 20 kwietnia 2013 r.

ID 2.16.840.1.113883.3.4424.7.2.9 2345678

Korekta dokumentu o ID 2.16.840.1.113883.3.4424.7.2.1 2345678

Wersja 2

ID zbioru wersji 2.16.840.1.113883.3.4424.7.2.2 432231

Pacjent

Jan Franciszek Kowalski

PESEL 62091599999

Data urodzenia 15 września 1962 r.

Wiek w dniu wystawienia 50 lat

Adres Odkryta 41 lok. 12, 01-134 Warszawa

Płatnik Mazowiecki Oddział NFZ 07

Wystawca dokumentu dokument podpisany elektronicznie

lek. Piotr Nowak

Lekarz NPWZ 7724513

Specjalizacje neurologia, radiologia i diagnostyka obrazowa

Miejsce wystawienia

Poradnia POZ
NZOZ „POL-MED"
POL-MED Sp. z o.o.
cz. I-V sys. kod. res. 1007-01
REGON 12345678901234
Adres Marszałkowska 320, 00-950 Warszawa

Dane kontaktowe

tel: 22-1111123 (rejestracja)
faks: 22-1111100 (rejestracja)

Dane dokumentu anulowanego

Proszę o anulowanie dokumentu:

Tytuł: Recepta

Data wystawienia: 12.04.2013

Identyfikator: 2345678

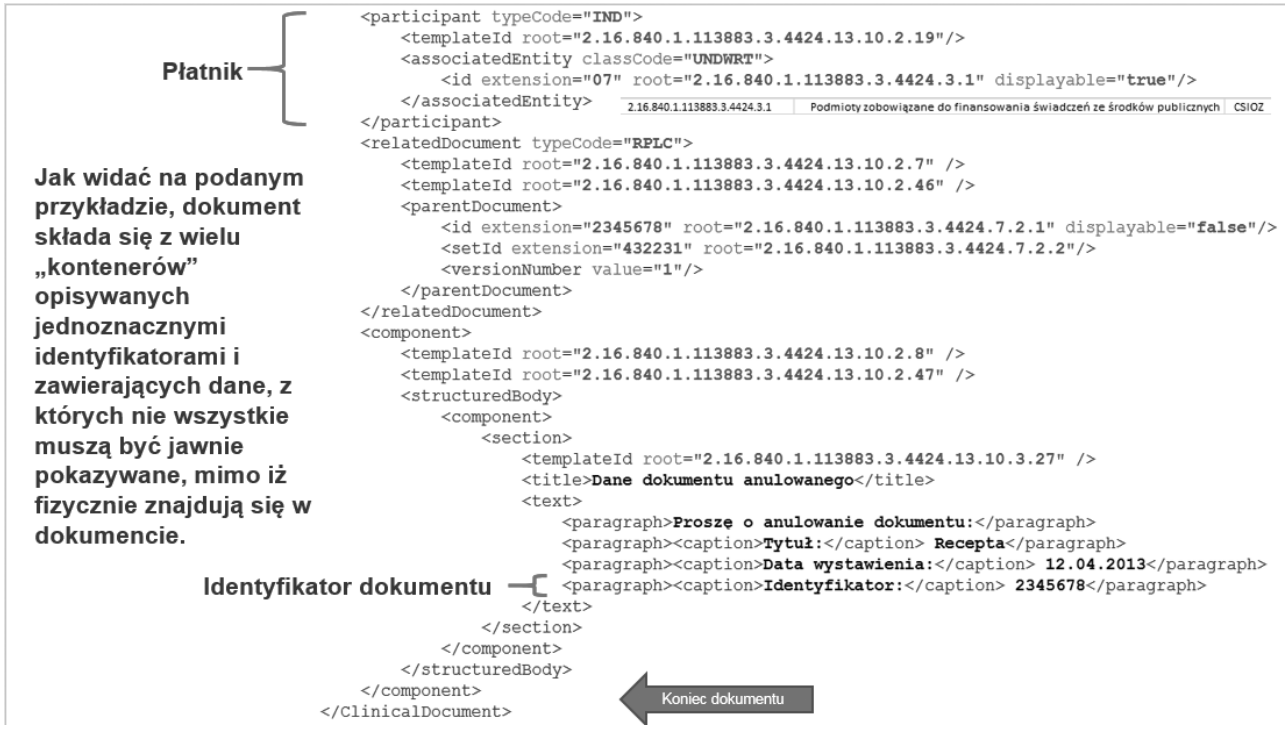
Rys. 2. Wygląd dokumentu anulującego receptę o numerze 2345678 z 12.4.2013 r.

```
<?xml version="1.0" encoding="UTF-8"?>
<?xml-stylesheet href="CDA PL IG 1.2.xsl" type="text/xsl"?>
<ClinicalDocument
        xmlns="urn:hl7-org:v3"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:extPL="http://www.csioz.gov.pl/xsd/extPL/r1"
        xsi:type="extPL:ClinicalDocument">
    <!-- Anulowanie recepty na Enarenal -->
    <typeId extension="POCD_HD000040" root="2.16.840.1.113883.1.3"/>
    <templateId root="2.16.840.1.113883.3.4424.13.10.1.1"/>
    <templateId root="2.16.840.1.113883.3.4424.13.10.1.14" extension="1.1.1"/>
    <id extension="2345678" root="2.16.840.1.113883.3.4424.7.2.9" displayable="true"/>
    <code code="51851-4" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC" displayName="Administrative note">
        <translation code="08.80" codeSystem="2.16.840.1.113883.3.4424.11.1.32" codeSystemName="KLAS_DOK_P1" displayName="Dokument
        anulujący"/>
    </code>
    <title>Dokument anulujący</title>
    <effectiveTime value="20130420"/>
    <confidentialityCode code="N" codeSystem="2.16.840.1.113883.5.25"/>
    <languageCode code="pl-PL"/>
    <setId extension="432231" root="2.16.840.1.113883.3.4424.7.2.2"/>
    <versionNumber value="2"/>
    <recordTarget>
        <templateId root="2.16.840.1.113883.3.4424.13.10.2.3"/>
        <patientRole>
            <id extension="12345" root="2.16.840.1.113883.3.4424.2.7.0.17.1" displayable="false"/>
            <id extension="62091599999" root="2.16.840.1.113883.3.4424.1.1.616" displayable="true"/>
            <addr>
                <city>Warszawa</city>
                <postalCode>01-134</postalCode>
                <streetName>Odkryta</streetName>
                <houseNumber>41</houseNumber>
                <unitID>12</unitID>
            </addr>
```

Początek dokumentu

Wewnętrzna struktura dokumentu pokazanego na poprzednim slajdzie

Rys. 3. Fragment kodu dokumentu anulującego receptę – widoczny PESEL – identyfikator pacjenta



Rys. 4. Dalszy fragment kodu dokumentu anulującego receptę – widoczny identyfikator dokumentu, który ma być anulowany

Na rys. 2 pokazano pochodzący ze wskazanej w poprzednim zdaniu strony dokument anulujący wystawioną receptę, której numer i datę wystawienia, wystawcę oraz pacjenta i wiele innych danych jednoznacznie można odczytać, gdyż wizualizacja przeznaczona jest dla człowieka. Tak wygląda wydruk dokumentu anulującego wystawioną receptę – bez względu na to, czy będzie on wydrukowany na papierze, czy zostanie utworzony jako plik w formacie pdf. Na rys. 3 pokazano fragment tego samego dokumentu, ale jako kodu odczytywalnego przez system informatyczny, interpretujący odpowiednio dane. Niektóre z danych zaznaczono ramkami, by ułatwić Czytelnikowi porównanie danych przedstawionych na rys. 3 z danymi na rys. 2. Na rys. 4 pokazano dalszą część kodu tego samego dokumentu ze wskazaniem miejsc dotyczących konkretnych osób związanych z dokumentem, a więc jego wystawcy – lekarza – i pacjenta. W tym momencie należy wskazać na fakt, że taki sposób zapisu danych – w postaci elektronicznej ze znacznikami otaczającymi dane – pozwala tworzyć różnego rodzaju relacje (powiązania) między odrębnymi dokumentami. Te relacje występują pomiędzy jednoznacznymi identyfikatorami każdego z dokumentów. Najogólniej bowiem rzecz ujmując, każdy obiekt w systemie musi posiadać swój jednoznaczny identyfikator, pozwalający zidentyfikować go w całym zbiorze obiektów tego samego rodzaju. Przykładowo dla pacjenta będzie to numer PESEL (jako identyfikator globalny w jakimkolwiek zbiorze zawierającym dane osób fizycznych), dla lekarza – numer prawa wykonywania zawodu (NPWZ), niezależnie od numeru PESEL lekarza, który też może być pacjentem. Właściwe identyfikatory używane są bowiem zależnie od kontekstu.

Jeśli więc przyjmiemy wspomnianą wyżej zasadę, że wszystkie obiekty (osoby fizyczne, podmioty lecznicze, dokumenty, choroby, procedury medyczne, leki, poszczególne dane itd.) mają jednoznacznie identyfikujące je identyfikatory, wtedy mamy już możliwość tworzenia zarządzalnych relacji między tymi obiektami.

Naturalną konsekwencją muszą być zasady zarządzania tymi relacjami, co *de facto* oznacza zarządzanie uprawnieniami dostępu do danych i dokumentów. Poziomy tych uprawnień (zakres dostępu, możliwość odczytu lub odczytu i zapisu, komentowanie, dodawanie metadanych itp.) muszą być uwarunkowane celowościowo.

Uwarunkowania celowościowe

Podstawowym celem działania systemu ochrony zdrowia jest ochrona zdrowia i życia osób fizycznych. Na pierwszym miejscu jest pacjent, a nie opisujące go dane. Osiągnięcie tego celu wymaga gromadzenia i przetwarzania danych opisujących stan zdrowia pacjenta i utrwalania tych danych w dokumentacji medycznej do przyszłego wykorzystania (cele naukowe, statystyczne, ekonomiczne itp., ale z zachowaniem poufności).

Gromadzone dane i dokumenty muszą być dostępne dla pracowników medycznych zaangażowanych w proces leczenia – i to niezależnie od lokalizacji miejsca udzielania świadczenia medycznego, gdyż pacjent może leczyć się w miejscach nawet bardzo terytorialnie odległych.

Powyższe implikuje potrzebę stosowania takich sposobów zapisu danych (czasowy) i dokumentów (trwały), by – niezależnie od stosowanego w danym podmiocie systemu – dane i dokumenty dało się nie tylko jednoznacznie odczytać, ale także upewnić się co do ich autentyczności – wszystko to w czasie długości trwania życia człowieka, czyli w perspektywie kilku dziesiątków lat. Jest to ogromne wyzwanie, zwłaszcza jeżeli chodzi o okres, gdy dane były zapisywane jedynie w dokumentach papierowych. Co prawda ich wygląd w zasadzie się nie zmieniał, jednak występowały problemy związane z niekompletnością, nieczytelnością pisma odręcznego lekarza i związane z tym zagrożenia wydania niewłaściwego leku lub potrzeby powrotu do lekarza w celu uczytelnienia wpisu. Ponadto tworzenie jakichkolwiek relacji między dokumentami było, jeśli nie niemożliwe, to znacząco utrudnione. Dokumenty gromadzone w teczkach, segregatorach, łączone spinaczami i zszywaczami nie nadają się do analiz statystycznych, gdyż pracochłonność związana z ich obróbką jest nieadekwatnie wysoka w stosunku do wyników przetwarzania, nie mówiąc o całkowicie realnych zagrożeniach poufności osobowych danych medycznych.

Jeśli chodzi o dane, informacje i dokumenty w postaci elektronicznej rzecz ma się zdecydowanie lepiej. Możliwe jest bowiem (w sensie technicznym) tworzenie systemów, w których jest zapewniona rozliczalność działania osób posiadających uprawnienia do ich wykorzystywania i to na różnych poziomach uprawnień, a także zapewniona jest poufność danych medycznych pacjentów. Tajemnica lekarska przestaje być całkowicie iluzoryczna, to system zapewnia bowiem dostęp osoby uprawnionej z jednoczesną rejestracją faktu udostępnienia (analogicznie, jak to jest w elektronicznych systemach zarządzania dokumentami zgodnymi z rozporządzeniem w sprawie instrukcji kancelaryjnej[7]). W systemach takich dane medyczne pacjentów są dostępne jedynie dla uprawnionych pracowników, posiadających dostęp warunkowany zarówno prawami dostępu, nadanymi przez kierownika podmiotu, jak i posiadaniem odpowiednich narzędzi – elektronicznego certyfikatu/klucza sprzętowego i hasła. Nie jest fizycznie możliwe zalogowanie się do systemu bez posiadania ww. narzędzi. Należy też uświadomić sobie fakt, że w momencie cofnięcia uprawnień dostępu do zasobów nawet posiadanie klucza sprzętowego i hasła nie pozwoli na zalogowanie się w systemie. Gdyby bowiem doszło do sytuacji, w której lekarz np. zgubi elektroniczną kartę z certyfikatem, wystarczy telefon do administratora – i ten może zablokować dostęp do zagrożonego konta do momentu wygenerowania nowego certyfikatu i ustalenia nowego hasła przez lekarza.

Z kolei pacjent może w każdej chwili uzyskać wszystkie dotyczące go dokumenty medyczne – zabezpieczone elektronicznie (zaszyfrowane, elektronicznie podpisane – są różne możliwości ich pobrania z systemu i przesłania do miejsca docelowego wykorzystania).

Ważnym, choć wydaje się, że ciągle jeszcze niedocenianym elementem każdego lokalnego lub – lepiej – regionalnego systemu przechowującego dokumenty (nie dane, ale właśnie dokumenty, które w sobie mają zapisane dane wraz z opisującymi je metadanymi) są repozytoria oraz archiwa głębokie.

Między repozytorium a archiwum głębokim istnieje bufor, który zabezpiecza je całkowicie przed nieuprawnionym wejściem, przeszukiwaniem czy pobraniem dokumentów. Repozytorium pozwala na przechowywanie plików (dokumentów) przez zadany okres (np. dwa lata). Jednocześnie pliki w trybie codziennym przed północą przesyłane są do archiwum głębokiego, gdzie mogą być składowane dziesiątki lat. Pliki starsze niż wymagany okres przechowywania są automatycznie usuwane z repozytorium. Nie ma potrzeby dłuższego ich przechowywania, gdyż pociągałoby to za sobą niepotrzebne rozbudowywanie owego repozytorium o kolejne dyski (całkowicie zbędne koszty materiałowe, koszty konserwacji). Pliki zawarte w repozytorium, jak już wcześniej wspomniano, są kopiowane do archiwum głębokiego tego samego dnia, w którym zostały utworzone. Jeśli zaistnieje taka potrzeba, mogą zostać na żądanie pobrane z archiwum na normalnych zasadach: żądanie osoby uprawnionej oraz rejestracja faktu wydania dokumentu z archiwum. Oczywiście wydana będzie jedynie kopia zero-jedynkowo zgodna z plikiem zapisanym w archiwum. Dokumenty zapisane w archiwum nigdy go nie opuszczają.

Inaczej rzecz ma się z repozytorium. Dokumenty zapisane w repozytorium w czasie tworzenia – dopóki nie zostaną ukończone (czyli elektronicznie podpisane), dopóty są dokumentami roboczymi, operacyjnymi dostępnymi do edycji bezpośrednio, on-line dla lekarza i uprawnionych osób mogących dokonywać wpisów we właściwych polach dokumentu. Dokument może mieć np. wygląd formularza zawierającego pola, w których powinny znaleźć się określone dane. Formularz jest jednak – jak to już pokazano na przykładzie dokumentu anulującego receptę – jedynie pewną wizualizacją ułatwiającą stwierdzenie, czy wszystkie wymagane dane zostały już zgromadzone. Jednak dane nie są zapisane w formularzu, a w pliku XML w kontenerach opisanych właściwymi znacznikami. Taka konstrukcja dokumentów (ściśle zdefiniowana i uporządkowana struktura właściwa dla

[7] Rozporządzenie Prezesa Rady Ministrów z 18.1.2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. Nr 14, poz. 67 ze zm.).

każdego wzoru) pozwala na operacje całkowicie niemożliwe do wykonania w odniesieniu do dokumentów papierowych. Umożliwia mianowicie selektywne wybieranie danych do badań naukowych i sprawozdań statystycznych bez naruszania poufności danych medycznych, czyli w oderwaniu od danych osobowych pacjentów. Przenosi to bezpieczeństwo osobowych danych medycznych na całkowicie inny poziom[8].

Z kolei archiwum głębokie to takie archiwum elektroniczne, które służy do składowania dokumentów medycznych (generalnie plików w różnych formatach, także obrazów, filmów, plików tekstowych i multimedialnych) w środowisku zapewniającym kontrolę nośników, stanu dysków, zapisów danych ze stosowną nadmiarowością, tak by w razie uszkodzenia, utraty pojedynczych bitów możliwe było odtworzenie zapisanego dokumentu bez zniekształceń niesionej treści. Szczegółowe opisanie zastosowanych w tym celu mechanizmów znacznie przekraczałoby ramy niniejszego artykułu. Istotne jest jednak to, że istnieją już obecnie krajowe rozwiązania techniczne, możliwe do praktycznego zastosowania i znacznie tańsze niż technologicznie już przestarzałe powszechnie stosowane rozwiązania (nie należy mylić archiwum wieczystego z systemem backupowym, służącym do odtwarzania danych po awariach systemu).

Ochrona danych osobowych medycznych obejmuje różne obszary, takie jak:
- ochrona przed nieuprawnionym pozyskaniem czy wglądem;
- ochrona przed zafałszowaniem;
- ochrona przed uszkodzeniem, zniszczeniem;
- ochrona przed utratą.

Wiele zależy od postaci nośnika, na którym zapisywane są informacje/dane (postać dokumentu). Jak już wcześniej wspomniano, ochrona danych i dokumentów w postaci elektronicznej, z uwagi na rozliczalność uzyskaną dzięki silnym mechanizmom weryfikacji tożsamości użytkownika systemu, jest zdecydowanie silniejsza. Ważniejsza jednak od ochrony danych jest ochrona osób fizycznych, których te dane dotyczą, co niejako jest wskazane w samym tytule aktu prawnego odnoszącego się do tej problematyki, czyli rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[9].

Należy także pamiętać, że przy tworzeniu i rozbudowie systemu informacji w ochronie zdrowia należy zachować pewne warunki, takie jak:
- poprawa danych w rejestrach (słownikowanie, usuwanie niezgodności, uzupełnianie braków);
- przy tworzeniu nowych systemów stosowanie zasad „*privacy by design*", a przy nadawaniu uprawnień dostępu do danych i dokumentów zasady „*privacy by default*";
- wprowadzanie identyfikatorów elektronicznych, certyfikatów dostępowych i certyfikatów służących do składania podpisów.

Ostatni z ww. warunków może być realizowany w różny sposób. Jakiekolwiek prawne regulowanie koniecznych do zastosowania środków technicznych byłoby bowiem pozbawione sensu z uwagi na stale zmieniającą się i doskonaloną technologię (łącznie z możliwością zastosowania silnych biometrii), która umożliwia z jednej strony coraz prostsze, a z drugiej coraz pewniejsze sposoby wiarygodnego „przedstawienia się" systemowi teleinformatycznemu. Wykonywanie jakiejś czynności po zalogowaniu się do systemu skutkuje automatycznym zapisem czynności zalogowanego użytkownika, który – oprócz różnych danych opisujących szczegółowo jego uprawnienia, stanowisko, imię i nazwisko, kontekst, w jakim działa (ten sam pracownik w systemie może mieć różne uprawnienia w zależności od kontekstu, roli, w jakiej występuje, i od jednostki organizacyjnej, w ramach której w danym momencie pracuje) – jest zawsze identyfikowalny dzięki posiadaniu jednoznacznego identyfikatora, jakim jest numer PESEL. Podobnie podmiot, w ramach którego ów użytkownik wykonuje swoje zadania, musi być jednoznacznie identyfikowany – przez numer REGON. Sprawy jednoznacznej identyfikacji oraz przenaszalności danych i dokumentów między systemami uregulowane zostały rozporządzeniem w sprawie Krajowych Ram Interoperacyjności. Warunki osiągania interoperacyjności opisane w powołanym akcie częstokroć nie są jednak znane i przestrzegane przez podmioty inne niż te, których dotyczy ustawa o informatyzacji. Podmioty te traktują zasady interoperacyjności jako zbędne obciążenie czy ograniczenie ich swobody oraz źródło zbędnych kosztów dostosowania ich systemów do bliżej nieokreślonych systemów podmiotów realizujących zadania publiczne. Jest to jednak dość krótkowzroczne podejście, gdyż tak jak np. systemy niepublicznych zakładów ochrony zdrowia zasilać mogą danymi system informacji w ochronie zdrowia, tak systemy zarządzane przez podmioty realizujące zadania publiczne zasilać mogą systemy podmiotów niepublicznych. Celowi temu służy program otwierania danych publicznych. W konsekwencji powstał portal (pierwotnie danepubliczne.gov.pl, aktualnie dane.gov.pl), na którym znajdują się zarówno dane, jak i aplikacje służące do bardzo różnych celów – czyli takie, które mogą być wykorzystywane nie tylko w celu, dla którego zostały zebrane, ale także w jakimkolwiek innym.

Związek wspomnianego portalu z systemami ochrony zdrowia jest dość istotny – można w nim odszukać poprawnie zapisane zbiory adresowe (zbiór „Dane adresowe gmin") oraz aplikację do sprawdzania adresu uniwersalnego

[8] *K. Anders* i in., Ochrona danych osobowych medycznych, wyd. 2, Warszawa 2018, *passim*.

[9] Dz.Urz. UE L 119, s. 1; dalej jako: RODO.

(http:/ itia.pl/adres). Podmioty lecznicze, samorząd lekarski i pielęgniarski, farmaceuci, wprowadzając do prowadzonych i zarządzanych przez siebie systemów jakikolwiek adres fizyczny (w terenie), powinni za pomocą wspomnianej wyżej aplikacji zweryfikować adres, który zamierzają wprowadzić np. do wniosku rejestracyjnego.

W czasie wprowadzania adresu (ściślej, wyboru poszczególnych składowych adresu z list wyboru) można ustalić poprawną konstrukcję adresu i zobaczyć punkt adresowy na wygenerowanej mapce.

W tym konkretnym przypadku dane źródłowe, pochodzące z gmin zasilają rejestry centralne prowadzone przez GUS (TERYT – rejestr podziału terytorialnego kraju) oraz GUGiK (Państwowy Rejestr Granic). Aplikacja do sprawdzania adresu uniwersalnego wiąże ze sobą dane obu wyżej wspomnianych rejestrów. Dzięki temu, że w danych PRG osadzone są kody terytorialne (oraz dodatkowo kody pocztowe PNA), możliwe jest wzajemne ich powiązanie i wygenerowanie adresu uniwersalnego, łączącego w sobie wszystkie elementy niezbędne zarówno do wygenerowania adresu uniwersalnego, jak i poprawnego adresu fizycznego rzeczywiście istniejącego obiektu. W ochronie zdrowia poprawność wskazania adresu może decydować o tym, czy ekipa pogotowia ratunkowego dojedzie do wskazanego miejsca jeszcze za życia osoby poszkodowanej.

Rys. 5. Nazwa ulicy dla tego samego punktu adresowego zapisana w systemach niezależnych od siebie

Na rys. 5 pokazano przykład punktu adresowego, dla którego nazwa ulicy ma wprawdzie różne brzmienie w powołanych wyżej rejestrach centralnych (co jest oczywistym błędem urzędników, gdyż źródłem nazwy jest ta sama rada gminy i nazwa jednoznacznie zapisana jest w uchwale), ale dzięki temu, że w obu wersjach nazwy występuje wspólny element „Łukasińskiego", system potrafi wskazać na mapie poszukiwany punkt adresowy. W rzeczywistości istnieją różne, inne jeszcze przypadki zakłóceń, takie jak np. występowanie w tej samej miejscowości dwóch różnych, oddalonych od siebie ulic (np. ul. Wilanowska w Warszawie), które jednak – dzięki odmiennemu kodowi pocztowemu – także można od siebie odróżnić. Niemniej problem niespójności adresów jest problemem stałym i jedynie upowszechnianie wiedzy o zagrożeniach stwarzanych przez niespójne dane czy ich brak w systemach teleinformatycznych oraz rejestrach może spowodować zwiększoną uwagę przy wprowadzaniu danych do rejestrów systemów informacyjnych mających interoperacyjnie współdziałać ze sobą.

Wdrożenie interoperacyjnych i bezpiecznych e-usług wymaga zdecydowanego uporządkowania zawartości rejestrów stosowanych w administracji publicznej, w szczególności rejestrów centralnych zarówno w zakresie ich kompletności, jak i zawartości informacyjnej. Należy doprowadzić do zmiany przepisów prawa utrudniających lub uniemożliwiających uspójnienie danych oraz wymuszających ich powielanie (te same dane w tym samym czasie nie mogą mieć w różnych rejestrach różnej wartości – aktualnie jest to niemal norma). Obecnie administrator systemu widzi błędy, ale niedostosowane do realiów prawo nie pozwala mu ich usunąć. Z kolei

administrator danych lub ich właściciel mógłby usunąć błędy, ale ich nie dostrzega, a najczęściej nie ma także świadomości ich istnienia (mimo że sam dane do rejestrów wprowadza). Dane rejestrowe powinny być wiązane z jednoznacznymi identyfikatorami – zgodnie z Krajowymi Ramami Interoperacyjności. Wiązałoby się to jednak ze zmianą zakresu podmiotowego ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne – i także jej nazwy. Znowelizowana ustawa o informatyzacji musiałaby bowiem objąć także rejestry podmiotów niepublicznych – w tym rejestry prowadzone przez samorządy zawodowe, jeśli stanowią one źródło danych dla rejestrów centralnych, jak ma to np. miejsce w przypadku Rejestru Podmiotów Wykonujących Działalność Leczniczą[10]. W rejestrze tym ujęte są nie tylko podmioty, dla których organem rejestrowym jest wojewoda, ale także indywidualne i grupowe praktyki lekarzy i lekarzy dentystów oraz indywidualne i grupowe praktyki pielęgniarek i położnych. Z jednej strony ustawa z 15.4.2011 r. o działalności leczniczej[11] w art. 106 wskazuje organy rejestrowe, a z drugiej traktuje je nierówno, dyskryminacyjnie, gdyż nakładając obowiązki, nie zapewnia narzędzi realizacji zadań (jak np. nie nadaje funkcjonalności podmiotu publicznego okręgowym izbom lekarskim i pielęgniarskim pozwalającym we właściwy sposób wykorzystywać Elektroniczne Skrzynki Podawcze na platformie ePUAP). Naruszona jest zasada równoważności w zakresie nadawania praw i nakładania obowiązków. Organ rejestrowy, jakim jest wojewoda, funkcjonalność taką uzyska, ponieważ urząd wojewódzki jest podmiotem realizującym zadania publiczne, a okręgowe (i naczelne) izby samorządów zawodowych – mimo że ustawowo zmuszone zostały do prowadzenia rejestrów, funkcjonalności takiej nie uzyskały. Dyskryminacja i nierówne traktowanie różnych podmiotów, mimo iż niektóre z nich tworzone są z mocy ustawy i ewidentnie wykonują zadania społecznie potrzebne, widoczne są doskonale np. w wykazie Elektronicznych Skrzynek Podawczych, w którym jedynie Naczelna Izba Lekarska oraz trzy Okręgowe Izby Lekarskie uzyskały funkcjonalność podmiotu publicznego, podobnie jak kilka niepublicznych zakładów opieki zdrowotnej, a kilkadziesiąt innych organów rejestrowych – mimo że składały wnioski o nadanie funkcjonalności podmiotu publicznego – już nie.

Sytuacja taka jest ewidentną przeszkodą w tworzeniu bezpiecznego i spójnego elektronicznego środowiska przetwarzania danych i przesyłania dokumentów w postaci elektronicznej.

Podsumowanie

Stworzenie bezpiecznego, sprawnego środowiska przetwarzania danych i wykorzystywania dokumentów w postaci elektronicznej wymaga spełnienia pewnych warunków dotyczących spójnego i niedyskryminacyjnego stosowania prawa, zachowania równowagi w nakładaniu obowiązków i przyznawania praw, jak też spełnienia całkowicie realnych warunków technicznych, związanych z zapewnieniem interoperacyjności systemów wszelkich podmiotów zasilających danymi rejestry współpracujące z systemem informacji w ochronie zdrowia, lub do niego należącymi. Bez spełnienia powyższych warunków jego budowa będzie nadmiernie kosztowna, a sam system ciągle będzie generował czy ujawniał błędy różnego rodzaju i nie będzie w pełni realizował oczekiwań względem jego funkcjonalności. Należy sobie uświadomić, że sprawny system informacji w ochronie zdrowia umożliwi nie tylko tworzenie e-usług, ale także realizację programu otwierania danych publicznych[12] – a to z kolei ma znaczenie dla podmiotów świadczących usługi medyczne.

[10] Zob. https://rpwdl.csioz.gov.pl (dostęp z 11.1.2019 r.).
[11] T.j. Dz.U. z 2018 r. poz. 160 ze zm.
[12] Uchwała Nr 107/2016 Rady Ministrów z 20.9.2016 r. w sprawie ustanowienia „Programu otwierania danych publicznych", https://mc.bip.gov.pl/programy-realizowane-w-mc/programu-otwierania-danych-publicznych.html (dostęp z 11.1.2019 r.).

Słowa kluczowe: ochrona danych medycznych, otwieranie danych, interoperacyjność, rejestry publiczne, informacja w ochronie zdrowia, dokumenty medyczne, repozytorium, archiwum głębokie.

Computerization of resources of entities running medical activity. Interoperability and data protection – how does it work?

The aim of the present study is to point out specification of a very complex system of information in health protection within which there is processing of data. Firstly, the issue concerns data of which common and unconditional sharing is a social benefit and the data may be used for different purposes, not necessarily for the one that system has been built. Secondly, this data has to be protected because it is personal data, including data of special category.

Keywords: protection of medical data, opening data, interoperability, public register, information in health protection, medical documents, repository, deep archive.