

MODEL REALIZACYJNY DLA WYKONAWCÓW

Projekt:

„Zachodniopomorskie e-Zdrowie”

Regionalny Program Operacyjny

Województwa Zachodniopomorskiego na lata 2014-2020

Oś priorytetowa 9 Infrastruktura publiczna

Działanie 9.10 Wsparcie rozwoju e-usług publicznych

Warszawa, listopad 2022 r.



**Rzeczpospolita
Polska**



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Spis treści

1. Uwagi wstępne.....	12
1.1 Cel dokumentu	12
1.2 Informacja o Projekcie ZeZ	12
1.3 Powiązanie e-usług, funkcjonalności i produktów w Projekcie	13
2. Uwarunkowania realizacji Projektu	16
2.1 Interoperacyjność z systemami zewnętrznymi.....	16
2.2 Rekomendacje CeZ w zakresie minimalnych wymagań technicznych i funkcjonalnych	17
2.3 Wymagania technologiczne	17
2.4 Wymagania związane z dostępem do Internetu	18
2.5 Wymagania funkcjonalne	18
2.6 Rekomendacje CeZ w zakresie stosowanych rozwiązań technologicznych oraz bezpieczeństwa	21
2.7 Modele architektury bezpiecznego przetwarzania dokumentacji medycznej	22
2.8 Przetwarzanie dokumentacji medycznej w postaci elektronicznej - zagrożenia.....	25
2.9 Cyberbezpieczeństwo przetwarzania dokumentacji medycznej w postaci elektronicznej	29
2.10 Dokumentacja integracyjna.....	31
2.10.1 Zdarzenia medyczne (ZM)	31
2.10.2 Elektroniczna Dokumentacja Medyczna (EDM)	31
2.10.3 Nadawanie dostępu do danych medycznych pacjenta.....	31
2.10.4 Odczyt zgód pacjenta	32
2.10.5 e-Recepta.....	32
2.10.6 e-Skierowanie	33
2.10.7 e-Rejestracja	33
2.11 Rekomendacje Rady ds. Interoperacyjności.....	33
2.12 Współpraca z platformą P1 - założenia	34
2.13 Domenowość	35
2.14 Zgody	36
3. Profile oraz transakcje IHE w Projekcie	39
4. Elektroniczna Dokumentacja Medyczna w Projekcie	39
4.1 Metody uwierzytelniania dokumentów medycznych	41
5. Zdarzenia Medyczne w Projekcie	42
5.1 Informacje ogólne.....	42
Założenia - podstawy prawne.....	42
5.2 Zakres danych zdarzenia medycznego przetwarzanego w systemie informacji	43
5.3 Dane usługodawcy	44
5.4 Dane usługobiorcy	44
5.5 Dane dotyczące świadczenia zdrowotnego	44
5.6 Dane miejsca udzielenia świadczenia zdrowotnego.....	45

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaPomorze
ZachodnieUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

5.7	Dane pracownika medycznego udzielającego świadczenia zdrowotnego	46
5.8	Dane dotyczące dokumentacji medycznej.....	46
5.9	Inne dane pozwalające na identyfikację zdarzenia medycznego	46
5.10	Wymiana informacji o zdarzeniach medycznych	48
6.	Architektura funkcjonalna Systemu ZeZ	52
6.1	Kluczowe założenia i pryncypia	52
6.2	Model architektury aplikacyjnej	55
6.3	Portal Projektu ZeZ	56
6.4	Wymiana dokumentacji medycznej EDM.....	56
6.5	Architektura aplikacyjna obszaru wymiany dokumentacji medycznej EDM	57
6.6	Domenowość	59
6.7	Rejestr indeksów (metadanych) EDM.....	59
6.8	Dostęp do dokumentów i elektroniczne zgody pacjenta	59
6.9	Lokalne Repozytoria EDM	60
6.10	Regionalne Repozytorium EDM.....	60
6.11	Wytwarzanie EDM w systemach Partnerów	60
6.12	Systemy Analityczne	60
6.13	Zdarzenia medyczne.....	61
6.14	e-Rejestracja	62
6.15	Powiadomienia.....	64
6.16	e-Dzienniczek Pacjenta.....	65
6.17	Zapisywanie zdarzeń na potrzeby audytu.....	67
6.18	Panel administracyjny	68
6.19	Moduł uwierzytelniania i autoryzacji.....	68
6.20	Narzędzia ZEZ API	68
6.21	Integracja z systemem HIS w zakresie interfejsu użytkownika.....	68
7.	Specyfikacja e-usług w Projekcie, analiza procesów biznesowych, wskazanie profili IHE	69
7.1	Specyfikacja e-usług	69
7.1.1	e-Uслуги - Wymagania нефункционалне.....	69
7.2	Portal Projektu ZeZ	70
7.3	e-Rejestracja	71
7.4	EDM	81
7.5	e-Dzienniczek pacjenta	87
7.6	Systemy analityczne	89
7.6.1	System Analizy Sprawozdawczej SAS	89
7.7	Zbiornicze zestawienie e-usług.....	103
8.	Zasady komunikacji dla usług e-Rejestracji i EDM.....	104
8.1	Zasady komunikacji - e-Rejestracja lokalna	104
8.1.1	Transakcja rezerwacji wolnego terminu dokonana z poziomu systemu HIS:	104

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

8.1.2	Transakcja wyszukiwania wolnego terminu dokonana z poziomu strony www Partnera Projektu:	105
8.1.3	Transakcja rezerwacji wolnego terminu dokonana z poziomu strony www Partnera Projektu:	105
8.1.4	Transakcja anulowania zarezerwowanego terminu dokonana z poziomu HIS:	107
8.1.5	Transakcja anulowania zarezerwowanego terminu dokonana z poziomu strony www Partnera Projektu:.....	107
8.1.6	Transakcja modyfikacji zarezerwowanego terminu dokonana z poziomu HIS:	108
8.1.7	Transakcja modyfikacji zarezerwowanego terminu dokonana z poziomu strony www Partnera Projektu:.....	109
8.2	Zasady komunikacji - Elektroniczna Dokumentacja Medyczna	109
8.2.1	Wyszukanie dokumentu medycznego przez Pracownika Medycznego (PM) z poziomu systemu HIS podmiotu należącego do Projektu	110
8.2.2	Pobranie dokumentu przez Pracownika Medycznego (PM) z poziomu systemu HIS podmiotu należącego do Projektu	111
8.2.3	Dodanie dokumentu medycznego przez Pracownika Medycznego (PM) z poziomu systemu HIS	112
8.2.4	Dodanie dokumentu medycznego wytworzonego przez e-Uслуги	113
9.	Architektura infrastruktury teleinformatycznej	115
9.1	Warstwa regionalna – założenia projektowe	115
9.1.1	Opis rozwiązania	117
9.1.2	Wyposażenie poszczególnych lokalizacji	121
9.2	Warstwa lokalna	124
9.2.1	Opis środowiska referencyjnego	124
10.	Założenia i wytyczne dotyczące bezpieczeństwa	125
10.1	Uwarunkowania prawne	125
10.2	Szczegółowe wymagania – bezpieczeństwo fizyczne	128
10.3	Szczegółowe wymagania – bezpieczeństwo systemów informatycznych	129
10.4	Bezpieczeństwo systemów informatycznych w cyberprzestrzeni	131
10.5	Szczegółowe wymagania proceduralne oraz techniczne	131

Spis ilustracji:

Rys.1. Podział kontroli pomiędzy usługodawcą a podmiotem zewnętrznym w modelach przetwarzania danych w chmurze obliczeniowej. (źródło: CSIOZ)	24
Rys. 2. Diagram rejestracja Zdarzenia Medycznego (źródło: opracowanie własne)	49
Rys. 3. Diagram Wymiana Zdarzenia Medycznego i Elektronicznej Dokumentacji Medycznej (źródło: Centrum e-Zdrowia)	50
Rys. 4. Model poglądowy architektury systemu	54
Rys. 5. Architektura aplikacyjna ZeZ	55
Rys. 6. Realizacja e-Usługi Wymiana EDM	57
Rys. 7. Architektura aplikacyjna obszaru wymiany dokumentacji medycznej EDM.....	58
Rys. 8. Realizacja usługi e-Rejestracja	63
Rys. 9. Integracje modułu e-Rejestracja	64
Rys. 10. Realizacja usługi e-Dzienniczek Pacjenta.....	65
Rys.....	66
Rys. 12. Interakcje obszaru Regionalnego repozytorium zdarzeń na potrzeby audytu	67
Rys. 13. Diagram: Portal Projektu ZeZ.....	71
Rys. 14. Diagram: Rejestracja.....	75
Rys. 15. Diagram: e-Rejestracja.....	78
Rys. 16. Diagram: e-Powiadomienia – zmiana terminu wizyty	80
Rys. 17. Diagram: Elektroniczna Dokumentacja Medyczna	86
Rys. 18. e-Dzienniczek.....	89
Rys. 19. Diagram: System Analizy Sprawozdawczej SAS.....	91
Rys. 21. Diagram: Rezerwacja wolnego terminu dokonana z poziomu systemu HIS	104
Rys. 22. Diagram: Rezerwacja wolnego terminu ze strony www podmiotu leczniczego	106
Rys. 23. Diagram: Anulowanie zarezerwowanego terminu z systemu HIS	107
Rys. 24. Diagram: Anulowanie zarezerwowanego terminu z Portalu Pacjenta	108
Rys. 25. Diagram: Modyfikacja zarezerwowanego terminu z systemu HIS.....	109
Rys. 26. Diagram: Modyfikacja zarezerwowanego terminu	109
Rys. 27. Diagram: Pobranie dokumentu medycznego przez HIS	110
Rys. 28. Diagram: Pobranie dokumentu medycznego przez HIS	112
Rys. 29. Diagram: Dodanie dokumentu medycznego przez HIS	113
Rys. 31. Schemat topologii sieci przy rozwiązaniu tradycyjnym	118

Wykorzystywane skróty i terminy

Lp.	Skrót / termin	Wyjaśnienie skrótu / terminu
1.	Autoryzacja uprawnień	Nadanie dostępu do danych recept, skierowań, zdarzeń medycznych, elektronicznej dokumentacji medycznej Usługobiorcy realizowane za pośrednictwem usługi sieciowej dostępnej dla systemów zewnętrznych podmiotów leczniczych.
2.	CSIOZ	Centrum Systemów Informacyjnych Ochrony Zdrowia.
3.	CeZ	Centrum e-Zdrowia
4.	Certyfikat, certyfikat do uwierzytelnienia systemu	Certyfikat zdefiniowany w Art. 2 ust. 3a) Ustawy o SIOZ, używany do uwierzytelnienia systemu zewnętrznego w warstwie transportowej (TLS).
5.	Certyfikat do uwierzytelnienia danych	Certyfikat zdefiniowany w Art. 2 ust. 3) Ustawy o SIOZ, używany do potwierdzenia pochodzenia i integralności danych przesyłanych przez system zewnętrzny (podpis komunikatu WS-Security).
6.	Certyfikat obecności	Certyfikat obecności jest używany do identyfikacji osoby oraz do weryfikacji podpisu składanego z wykorzystaniem interfejsu bezstykowego elektronicznego dowodu osobistego (eDO)
7.	Centrum Certyfikacji P1	Komponent systemu P1 wystawiający certyfikaty cyfrowe na potrzeby komunikacji systemów zewnętrznych z systemem P1 oraz wzajemnego uwierzytelniania systemów teleinformatycznych Usługodawców.
8.	Deklaracja POZ	Deklaracja wyboru lekarza, pielęgniarki, położnej Podstawowej Opieki Zdrowotnej
9.	DICOM	Obrazowanie cyfrowe i wymiana obrazów w medycynie (ang. Digital Imaging and Communications in Medicine)
10.	eDO	Elektroniczny dowód osobisty
11.	Elektroniczne skierowanie, e-Skierowanie	Dokument elektroniczny skierowania zgodny z PIK HL7 CDA (wymagany format podpisu elektronicznego dla dokumentów XML to XAdES-BES).
12.	Elektroniczna Dokumentacja Medyczna (w skrócie EDM)	Dokumentacja prowadzona w postaci elektronicznej. Obowiązkowi rejestracji w Systemie P1 podlegają dokumenty medyczne określone w rozporządzeniu Ministra Zdrowia z dnia 2018-05-08 w sprawie rodzajów elektronicznej dokumentacji medycznej wydanego na podstawie art. 13a ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia.
13.	Elektroniczna recepta, e-Recepta	Dokument elektroniczny recepty zgodny z PIK HL7 CDA (wymagany format podpisu elektronicznego dla dokumentów XML to XAdES-BES). Recepta elektroniczna obejmuje tylko jedną pozycję leku lub produktu leczniczego (do systemu P1 przekazywany jest pakiet recept). Jest podpisywana w sposób określony w <i>art. 96a ustawy z dnia 6 września 2001 prawo farmaceutyczne (Dz. U. 2001, nr 126, poz. 1381 z późn. zm.)</i> .
14.	FHIR	Fast Healthcare Interoperability Resources – rozszerzalny model danych standaryzujący semantykę i wymianę danych pomiędzy systemami gromadzącymi informacje w dziedzinie służby zdrowia. Standard interoperacyjności z rodziny HL7.

Lp.	Skrót / termin	Wyjaśnienie skrótu / terminu
15.	HIS	(ang. Hospital Information System) - Kompleksowy, zintegrowany system informacyjny przeznaczony do zarządzania wszystkimi aspektami szeregu czynności w szpitalu. Wspiera działanie obszarów głównie medycznych, ale także administracyjnych, finansowych, prawnych i odpowiedniego przetwarzania usług. W podmiotach leczniczych wchodzi w skład tzw. części „białej” Szpitalnego Systemu Informacyjnego.
16.	HL7	HL7(ang. Health Level Seven) – standard elektronicznej wymiany informacji w środowiskach medycznych. Opracowany w celu zapewnienia właściwej komunikacji między systemami medycznymi.
17.	HL7 CDA PIK HL7 CDA	HL7 CDA jest standardem obejmującym kwestie związane ze składnią i semantyką dokumentów klinicznych. HL7 CDA wstępuje w poziomach 1, 2 oraz 3. Rekomendowana do stosowania przez CeZ i publikowana w www.cez.gov.pl jest Polska Implementacja Krajowa HL7 CDA (PIK), która jest doprecyzowaniem standardu HL7® CDA™ (Clinical Document Architecture) Release 2 do warunków Polski.
18.	Harmonogram	Pakiet, zbiór wolnych slotów pogrupowanych wg. określonego kryterium (np. gabinetu lub pracownika medycznego)
19.	IHE	(ang. (Integrating the Healthcare Enterprise) Profile Integracji opisujące zbiór niezbędnych informacji klinicznych lub przepływy danych oraz użycie standardów do wymiany informacji w celu zapewnienia interoperacyjności.
20.	IKP	Internetowe Konto Pacjenta w projekcie centralnym P1
21.	Kanały komunikacji	Zakres zdefiniowanych kanałów komunikacji (E-MAIL, SMS) przez Usługobiorcę.
22.	Krajowa domena XDS.b	Domena XDS (ang. XDS Affinity Domain) powołana na szczeblu krajowym, w ramach której System P1 pełni rolę Rejestru XDS dla usługodawców zrzeszonych w Krajowej Domenie XDS w zakresie dokumentów podlegających rejestracji w P1.
23.	Kontroler Polityki Indeksacji Dokumentów	Komponent systemu określający na podstawie konfiguracji reguły indeksowania dokumentów w rejestrze krajowym P1.
24.	Kontroler polityki dostępu	Komponent systemu określający na podstawie konfiguracji i zadeklarowanego trybu dostępu możliwość dostępu do dokumentu oraz zasady sprawdzania zgody na udostępnianie dokumentów w Rejestrze Zgód P1.
25.	LIS	(ang. Laboratory Information System) – system zarządzania informacjami laboratoryjnymi.
26.	Miejsce udzielania świadczeń (MUŚ)	Podmiot albo Jednostka albo Komórka albo Praktyka, które są powiązane funkcjonalnie i organizacyjnie w celu udzielania świadczeń określonego zakresu.
27.	System podmiotu (System MUŚ)	Zestaw narzędzi teleinformatycznych służących do zarządzania harmonogramami oraz wizytami lokalnie przez MUŚ.
28.	Odbiorca/Konsument Dokumentów	Aktor profilu XDS.b (ang. Document Consumer), używa metadanych do wyszukiwania i pobierania dokumentów.
29.	OID	(ang. object identifier) Unikatowy identyfikator obiektu wykorzystywany w ramach Systemu P1.
30.	Partner Projektu	Bezpośredni uczestnik Projektu, który podpisał umowę partnerstwa.

Lp.	Skrót / termin	Wyjaśnienie skrótu / terminu
31.	PACS	(ang. Picture archiving and communication system) – System do zarządzania obrazami medycznymi.
32.	PM	Pracownik medyczny (lekarz, lekarz dentyista, pielęgniarka, położna, farmaceuta, felczer)
33.	Podmiot Lecznicy	Podmiot mający zdolność do wykonywania działań związanych z udzielaniem świadczeń medycznych.
34.	P1, Projekt P1	Projekt pn. „Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych”.
35.	P2, Projekt P2	Projekt pn. „Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych”.
36.	Preautoryzacja uprawnień	Nadanie dostępu do danych recept, skierowań, zdarzeń medycznych Usługobiorcy realizowane za pośrednictwem Internetowego Konta Pacjenta.
37.	Profil	Profil jest to definicja zasobu określająca ograniczenia lub rozszerzenia atrybutów zasobu oraz ich typu.
38.	Projekt	Projekt pn. „Zachodniopomorskie e-Zdrowie”
39.	Rejestr XDS, Rejestr EDM	Aktor profilu XDS. Miejsce przechowywania Indeksów Dokumentów Medycznych, informacji o wysyłce, folderach i asocjacjiach pomiędzy tymi encjami. Rejestr XDS.b umożliwia wyszukiwanie indeksów przy zastosowaniu predefiniowanych zapytań. Dostęp do danych rejestru XDS chronione są za pomocą rejestru zgód.
40.	Repozytorium XDS, Repozytorium EDM	Aktor profilu XDS. Miejsce przechowywania dokumentów medycznych. Operacja przekazania dokumentów medycznych do Repozytorium XDS.b zawiera treść tych dokumentów i całą treść komunikatu żądania wysyłki. Po zapisaniu dokumentów medycznych w Repozytorium XDS.b treść komunikatu żądania wysyłki przekazywana jest do Rejestru XDS.b celem 'zaindeksowania' tych dokumentów w rejestrze. Repozytorium Regionalne przechowuje kopie dokumentów medycznych, które zostały wytworzone w podmiocie leczniczym.
41.	Regionalne repozytorium EDM, RREDM	Repozytorium XDS realizowane na poziomie regionu, przechowujące typy dokumentów przeznaczone do wymiany zgodne z konfiguracją.
42.	Lokalne repozytorium EDM, LREDM	Repozytorium XDS istniejące w ramach szpitala i przechowujące dokumenty z określonego szpitala. Każdy elektroniczny dokument medyczny wytworzony w szpitalu powinien znaleźć się w Lokalnym Repozytorium EDM.
43.	RIS	Radiological Information System – Radiologiczny System Informacyjny
44.	System ZeZ	System informatyczny budowany i wdrożony w ramach realizacji Projektu „Zachodniopomorskie e-Zdrowie”.
45.	System zewnętrzny	System Usługodawcy lub innego podmiotu komunikujący się z systemem P1.
46.	System Elektronicznej Rejestracji, SER	Platforma uruchomiona w ramach realizacji Projektu P1, której zadaniem jest gromadzenie harmonogramów przesyłanych przez Podmioty Lecznicy, zarządzanie wizytami oraz umożliwienie synchronizacji i wymiany danych w trybie online z Systemami Oprogramowania Podmiotów Leczniczych.

Lp.	Skrót / termin	Wyjaśnienie skrótu / terminu
47.	BI, System BI	ang. System Business Intelligence – system gromadzenia danych pozwalający tworzyć raporty i analizy z różnych zestawieniach, układach i przekrojach).
48.	SAS	System Analizy Sprawozdawczej – element systemu BI – system tworzenia i dostarczania raportów obejmujących monitorowanie oraz analizę stanu wykorzystywania systemu regionalnego ZeZ.
49.	SAZ	System Analiz Zarządczych – element systemu BI - system analityczny wspomagający bieżące operacyjne zarządzanie podmiotem leczniczym. Wspiera także podejmowanie decyzji z zakresu kreowania polityki zdrowotnej regionu z poziomu organu właścicielskiego/tworzącego.
50.	SIM, System Informacji Medycznej	System teleinformatyczny służący przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców.
51.	SZAR	System Zarządzania Adresami Repozytoriów - pełni rolę centralnego rejestru repozytoriów dokumentów wraz z ich identyfikatorami OID oraz udostępnia usługę tłumaczącą OID na adres usług sieciowych repozytorium wykorzystywanych do pobierania dokumentów.
52.	Świadczeniobiorca (Pacjent)	Podmiot wykonujący działalność leczniczą lub uprawniona osoba fizyczna, w rozumieniu ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135)
53.	Świadczeniodawca	Osoby na rzecz który realizowane jest świadczenie, w rozumieniu ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135)
54.	XDS.b	Profil integracyjny IHE wykorzystywany do obsługi wymiany EDM, w tym do rejestrowania informacji o dokumentach medycznych wytworzonych w ramach Zdarzeń Medycznych.
55.	Wolny slot	Obiekt reprezentujący termin (datę i czas) dla danego świadczenia, który MUŚ zgłasza do Systemu Elektronicznej Rejestracji w celu umożliwienia przypisania do niego pacjenta.
56.	Wizyta (zajęty slot)	Wolny slot, do którego został przypisany Pacjent.
57.	Zapisanie na wizytę	Przypisanie przez Algorytm lub samodzielnie przez świadczeniobiorcę lub przez pracownika MUŚ danego pacjenta do Wolnego slotu.
58.	Ustawa o SIOZ, SIOZ	Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.
59.	Usługodawca, Podmiot Leczniczy	Podmiot w rozumieniu art. 2 pkt 15 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. 2011, nr 113, poz. 657 z późn. zm.).
60.	Usługobiorca	Osoba fizyczna korzystająca lub uprawniona do korzystania ze świadczeń opieki zdrowotnej, w tym Świadczeniobiorca w rozumieniu Ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004, nr 210, poz. 2135, art. 2 ust. 1; art. 2 ust. 2; art. 13).

Lp.	Skrót / termin	Wyjaśnienie skrótu / terminu
61.	Zasób	Pakiet danych odnoszący się do różnych pojęć klinicznych obejmujący: problemy zdrowotne, leczenie, diagnostykę, plany opieki, problemy finansowe a także pojęcia administracyjne takie jak: szczepienia, alergie, listy problemów, urządzenia, operacje, grupę krwi i historię ciąży.
62.	Zdarzenia audytowe	Błąd w działaniu aplikacji, naruszenie bezpieczeństwa, lub wywołanie aktora profilu XDS.b przez innego aktora profilu XDS.b w ramach jednej z transakcji tego profilu, wymagające zapisania w logu zgodnym z profilem ATNA.
63.	ZD, Zdarzenie Medyczne	Świadczenie zdrowotne, o którym mowa w ustawie z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, tj działanie służące profilaktyce, zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działanie medyczne wynikające z procesu leczenia lub przepisów odrębnych regulujących zasady ich udzielania. Zdarzenia medyczne podlegają rejestracji w Systemie P1.
64.	Zgoda na dostęp do informacji o stanie zdrowia	Oświadczenie pacjenta lub jego ustawowego przedstawiciela na przekazanie osobie wymienionej w zgodzie informacji o stanie zdrowia, udzielonych świadczeniach, rozpoznaniu, proponowanych oraz możliwych metodach diagnostycznych i leczniczych, dających się przewidzieć następstwach ich zastosowania albo zaniechania, wynikach leczenia oraz rokowaniu.
65.	Zgoda na dostęp do dokumentacji medycznej	Oświadczenie pacjenta o zgodzie na udostępnienie wskazanej w zgodzie osobie dokumentacji medycznej dotyczącej pacjenta.
66.	Zgoda na świadczenie medyczne	Oświadczenie pacjenta o zgodzie na wykonanie zabiegu medycznego zgodnie z treścią przekazaną przez Usługodawcę.
67.	Źródło Dokumentów	Aktor profilu XDS.b. (ang. Document Source), tworzy dokumenty i odpowiada za wysyłkę metadanych i dokumentów do rejestru i repozytorium.
68.	Żądanie certyfikacyjne, CSR	(ang. <i>Certificate Signing Request</i>) Wniosek o wydanie certyfikatu cyfrowego przekazywany do centrum certyfikacji, zawierający klucz publiczny oraz dane identyfikujące posiadacza certyfikatu – dot. docelowego środowiska produkcyjnego P1 (Centrum Certyfikacji P1 obsługuje żądania certyfikacyjne w formacie PKCS#10).



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



1. Uwagi wstępne

1.1 Cel dokumentu

Celem przygotowania Modelu realizacyjnego jest określenie ostatecznego kształtu Systemu Zachodniopomorskie e-Zdrowie, jego e-usług i funkcjonalności oraz uzyskanie dokumentacji technicznej, niezbędnej do przygotowania postępowań przetargowych na elementy Projektu ZeZ na rzecz Lidera i Partnerów Projektu.

1.2 Informacja o Projekcie ZeZ¹

Celem głównym Projektu Zachodniopomorskie e-Zdrowie jest realizacja niezbędnych działań w podmiotach leczniczych umożliwiających wdrożenie usług elektronicznych w zakresie ochrony zdrowia świadczonych przez podmioty lecznicze biorące udział w projekcie na rzecz pacjentów i personelu medycznego oraz ich integracja z systemami centralnymi e-zdrowia. Cel Projektu jest zgodny z wymogami Priorytetu Inwestycyjnego 2c: Wzmocnienie zastosowań TIK dla e-administracji, e-uczenia się, e-włączenia społecznego, e-kultury i e-zdrowia, m.in. poprzez realizację Celu szczegółowego 6: Zwiększona dostępność do e-usług publicznych.

¹ Studium Wykonalności projektu „Zachodniopomorskie e-Zdrowie”



1.3 Powiązanie e-usług, funkcjonalności i produktów w Projekcie

Tabelaryczne Zestawienie powiązań między e-usługami i ich funkcjonalnościami oraz operatorem i odpowiedzialnym a interesariuszami oraz modułami oprogramowania systemów składających się na System ZeZ stanowiący przedmiot projektu „Zachodniopomorskie e-Zdrowie”.

e-Usługa	Funkcjonalność	Operator technologiczny funkcjonalności	Operator merytoryczny funkcjonalności	Podmioty odpowiedzialne za funkcjonowanie i zarządzanie	Interesariusze	Moduły oprogramowania
EDM	Repozytorium EDM -regionalne	Warstwa Regionalna: Operator Techniczny Warstwy Regionalnej (DataCenter) Warstwa Lokalna: Zespoły IT Partnerów	Warstwa Regionalna: brak Warstwa Lokalna: Personel medyczny systemu lokalnego	Warstwa Regionalna: Wydział Zdrowia UM Warstwa Lokalna: 12 Partnerów Projektu – bez WSPR Szczecin	- Warstwa centralna – system P1 - Pacjent i osoba upoważniona przez pacjenta, - Pracownicy podmiotów leczniczych,	Lokalne repozytorium EDM
	-Zdarzenia medyczne -Metadane (indeksy) EDM -Zdarzenia audytowe	Warstwa Regionalna: brak Warstwa Lokalna: Zespoły IT Partnerów Warstwa centralna: Zespoły IT operatora platformy P1	Warstwa Regionalna: brak Warstwa Lokalna: Personel medyczny systemu lokalnego Warstwa centralna: CeZ/Min. Zdrowia	Warstwa Regionalna: brak Warstwa Lokalna: 12 Partnerów Projektu – bez WSPR Szczecin Warstwa centralna: CeZ/Min. Zdrowia	- Warstwa centralna – system P1 - Pacjent i osoba upoważniona przez pacjenta, Pracownicy podmiotów leczniczych,	Komponent obsługujący raportowanie Zdarzeń Medycznych ZM - Moduł systemu HIS
	EDM dla lekarza	Warstwa Regionalna: brak Warstwa Lokalna: Zespoły IT Partnerów Warstwa centralna:	Warstwa Regionalna: brak Warstwa Lokalna: Personel medyczny systemu lokalnego Warstwa centralna:	Warstwa Regionalna: brak Warstwa Lokalna: 12 Partnerów Projektu – bez WSPR Szczecin Warstwa centralna:	Pracownicy podmiotów leczniczych	Komponent wytwarzający EDM - Moduł systemu HIS lub nowy moduł części białej, Lokalne

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

e-Usługa	Funkcjonalność	Operator technologiczny funkcjonalności	Operator merytoryczny funkcjonalności	Podmioty odpowiedzialne za funkcjonowanie i zarządzanie	Interesariusze	Moduły oprogramowania
		Zespoły IT operatora platformy P1	CeZ/Min. Zdrowia	CeZ/Min. Zdrowia		repozytorium EDM
	EDM dla pacjenta	Warstwa Regionalna: brak Warstwa Lokalna: Zespoły IT Partnerów Warstwa centralna: Zespoły IT operatora platformy P1	Warstwa Regionalna: brak Warstwa Lokalna: Personel medyczny systemu lokalnego Warstwa centralna: CeZ/Min. Zdrowia	Warstwa Regionalna: brak Warstwa Lokalna: 12 Partnerów Projektu – bez WSPR Szczecin Warstwa centralna: CeZ/Min. Zdrowia	Pacjent i osoba upoważniona przez pacjenta	Komponent wytwarzający EDM, Lokalne repozytorium EDM, Lokalny kontroler polityki dostępu Moduł funkcjonalny IKP
e-Rejestracja	e-Rejestracja (elektroniczna rejestracja)	Warstwa Regionalna: brak Warstwa Lokalna: Zespoły IT Partnerów (SMS / e-mail do Pacjenta)	Warstwa Regionalna: brak Warstwa Lokalna: Personel medyczny systemu lokalnego odpowiedzialny za prowadzenie terminarzy wizyt	Warstwa Regionalna: brak Warstwa Lokalna: 12 Partnerów Projektu– bez WSPR Szczecin	Pacjent i osoby upoważniona przez pacjenta	Lokalna e-Rejestracja integracja z centralną e-usługą e-Rejestracja planowaną w P1 w zakresie wynikającym z rekomendacji CeZ.
Portal Projektu ZeZ	Portal Projektu ZeZ	Warstwa Regionalna: Operator Techniczny Warstwy Regionalnej (DataCenter) Warstwa Lokalna: brak	Warstwa Regionalna: - Biuro Eksploatacji Projektu, - Inne wydziały UMWZ, - Podmioty związane z ochroną zdrowia. Warstwa Lokalna: Na poziomie lokalnym	Warstwa Regionalna: Biuro Eksploatacji Projektu Warstwa Lokalna: brak	- Pacjenci, - Pracownicy podmiotów leczniczych, - Podmioty związane z ochroną zdrowia	Dedykowany portal e-Zdrowie

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

e-Usługa	Funkcjonalność	Operator technologiczny funkcjonalności	Operator merytoryczny funkcjonalności	Podmioty odpowiedzialne za funkcjonowanie i zarządzanie	Interesariusze	Moduły oprogramowania
Systemy analityczne	SAS – analizy sprawozdawcze	Warstwa Regionalna: Operator Techniczny Warstwy Regionalnej (DataCenter)	Warstwa Regionalna: Biuro Eksploatacji Projektu	Warstwa Regionalna: UMWZ	- Pracownicy podmiotów leczniczych, - Podmioty związane z ochroną zdrowia	Dedykowane oprogramowanie klasy BI
	System Analiz Zarządczych BI - Business Intelligence	Warstwa Regionalna: Operator Techniczny Warstwy Regionalnej (DataCenter) Warstwa Lokalna: Zespoły IT Partnerów	Warstwa Regionalna: Wydziały merytoryczne UMWZ Warstwa Lokalna: Zasilanie w informacje z poziomu Partnera	Warstwa Regionalna: Wydziały merytoryczne UMWZ jako odbiorcy informacji zarządczej dotycząca szpitali Warstwa Lokalna: Wszyscy 13 Partnerzy Projektu	- kadra zarządcza UMWZ, - kadra zarządcza szpitali, - odbiorcy informacji statystycznej w części dot. informacji publiczne	
	Platforma Zakupowa SPZOZ /Grupowe Zamówienia	Warstwa Regionalna: Operator Techniczny Warstwy Regionalnej (DataCenter) Warstwa Lokalna: Zespoły IT Partnerów	Warstwa Regionalna: Wydział Zdrowia UMWZ Warstwa Lokalna: Zasilanie w informacje z poziomu Partnera	Warstwa Regionalna: Wydział OiRZL organizujący i przeprowadzający przetargi, Warstwa Lokalna: Wszyscy 13 Partnerzy Projektu	- kadra zarządcza UMWZ, - kadra zarządcza szpitali, - odbiorcy informacji statystycznej w części dot. informacji publiczne	

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

2. Uwarunkowania realizacji Projektu

Realizacja Projektu odnosi się do opracowania i wdrożenia systemu, który dla implementowanych funkcji oraz zakresu informacyjnego musi uwzględniać określone wymagania obowiązujących aktów prawnych, standardów i zaleceń technicznych. W szczególności dotyczy to wymagań związanych z zakresem informacyjnym systemu, w tym reguł gromadzenia, przetwarzania i udostępniania danych.

Wdrażane rozwiązania spełniać będą wymogi wynikające z europejskich oraz polskich przepisów prawa. Zapewniona zostanie pełna zgodność funkcjonalności systemów z regulacjami branżowymi.

System musi więc uwzględniać aktualne przepisy prawa związane z „ustawowymi” kompetencjami. W przypadku ogłoszenia zmian, aktualizacji, poprawek do aktów prawnych, rekomendacji, dokumentacji integracyjnej, norm, standardów wykorzystywanych do realizacji Projektu ZeZ, Wykonawcy są zobowiązani do ich stosowania. Powyższe ma zastosowanie w odniesieniu do:

- a) wszelkich, obowiązujących aktów prawnych, które dotyczyć mogą zakresu informacyjnego oraz funkcji systemu,
- b) dokumentów strategicznych, takich jak strategie, dyrektywy, wytyczne, polskie oraz unijne,
- c) norm i standardów implementacyjnych, integracyjnych oraz pozostałych
- d) klasyfikacji
- e) rekomendacji, wymagań technicznych oraz obowiązującej dokumentacji integracyjnej
- f) obowiązujących definicji interoperacyjności
- g) standardów gromadzenia i wymiany danych medycznych

2.1 Interoperacyjność z systemami zewnętrznymi

Wdrażane w ramach Projektu ZeZ systemy muszą zapewnić integrację - jak również gotowość do integracji w przyszłości, z racji dynamicznego rozwoju systemów zewnętrznych, których budowa jest koordynowana przez Centrum e-Zdrowia - z platformami/systemami zewnętrznymi.

Są to następujące systemy:

- 1) Platforma P1 - Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych,
- 2) IKP - Internetowe Konto Pacjenta – funkcjonalność realizowana w projekcie P1, zawiera spersonalizowane informacje o danych medycznych pacjenta,
- 3) Platforma Rejestrów Medycznych - udostępnia rejestry funkcjonujące w systemie Ochrony Zdrowia m.in. z możliwością przeszukiwania i składania wniosków o wpis/zezwoleń:
 - a) Rejestr Podmiotów Wykonujących Działalność Leczniczą - rejestr podmiotów leczniczych, rejestr praktyk zawodowych lekarzy i lekarzy dentystów oraz pielęgniarek i położnych,
 - b) Rejestr Aptek - rejestr aptek ogólnodostępnych, punktów aptecznych, aptek szpitalnych, aptek zakładowych oraz działów farmacji szpitalnej,
 - c) Rejestr Hurtowni Farmaceutycznych - rejestr hurtowni farmaceutycznych posiadających zezwolenie na prowadzenie obrotu hurtowego lekami w naszym kraju,

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- d) Rejestr Systemów Kodowania - zbiór słowników medycznych, mający eliminować nieporozumienia wynikające ze stosowania terminów medycznych,

Ponadto system ZeZ osiągnie interoperacyjność z innymi portalami regionalnymi i konsorcyjnymi innych podmiotów dzięki zastosowaniu powszechnie obowiązujących standardów wymiany danych.

2.2 Rekomendacje CeZ w zakresie minimalnych wymagań technicznych i funkcjonalnych

Wdrażane w ramach Projektu ZeZ systemy muszą spełniać w zakresie technicznym i funkcjonalnym wymagania określone przez Centrum e-Zdrowia.

Wymagania te odnoszą się do komunikacji z systemem P1, systemem NFZ do obsługi zlecenia na zaopatrzenie w wyroby medyczne oraz oprogramowaniem komunikacyjnym ZUS służącym do odbioru dokumentów elektronicznych. Zamieszczone są w dokumencie pn. *Minimalne wymagania techniczne i funkcjonalne dla Systemów Usługodawców*.

Przedstawione wymagania minimalne są związane z obecnym etapem realizacji Projektu P1, w którym uruchomiono obsługę e-recept i e-skierowań, obsługę zdarzeń medycznych (ZM) oraz wymiany elektronicznej dokumentacji medycznej (EDM). Rozwiązania informatyczne Narodowego Funduszu Zdrowia (NFZ) wspierające procesy elektronicznego potwierdzania zlecenia na zaopatrzenie pacjenta w wyrób medyczny oraz obsługę elektronicznych zwolnień lekarskich przy wykorzystaniu usług udostępnianych przez ZUS. W fazie pilotażu jest System Elektronicznej Rejestracji realizowany przez Ministerstwo Zdrowia.

2.3 Wymagania technologiczne

Podstawowym modelem wymiany danych Systemu Usługodawcy z Systemem P1 są interfejsy sieciowe. Usługodawca w celu wystawienia e-recepty, e-Skierowania, zgłoszenia zdarzenia medycznego bądź wymiany EDM oraz umawiania wizyt w Systemie Elektronicznej Rejestracji musi podłączyć swój system gabinetowy, szpitalny lub apteczny do Systemu P1.

System Usługodawcy musi mieć możliwość utworzenia dokumentu XML zgodnie z przyjętym standardem HL7 CDA, a następnie musi przesłać do Systemu P1.

Wszystkie usługi sieciowe systemu P1 są zabezpieczone z wykorzystaniem mechanizmów WS-Security. W komunikacji z systemem P1 wymagane jest użycie rozszerzenia Web Services Security i profilu Web Services Security X.509 Certificate Token Profile. W zakresie zdarzeń medycznych wykorzystywane jest REST API zgodne z HL7 FHIR i zabezpieczone tokenami JWT.

Uwierzytelnienie Systemu zewnętrznego wywołującego usługę systemu P1 następuje w warstwie transportowej połączenia za pomocą protokołu TLS z obustronnym uwierzytelnieniem - oprócz uwierzytelnienia serwera przez system zewnętrzny następuje uwierzytelnienie klienta (Systemu zewnętrznego) przez serwer. Do nawiązania połączenia TLS system zewnętrzny zobowiązany jest użyć certyfikatu do uwierzytelnienia systemu wydanego przez Centrum Certyfikacji P1. Do poprawnego wykonania usługi wymagane jest uwierzytelnienie pochodzenia komunikatu. System zewnętrzny

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

zobowiązany jest do podpisania komunikatu SOAP² z użyciem certyfikatu do uwierzytelnienia danych służącego do weryfikacji złożonego podpisu cyfrowego.

E-Recepta, e-Skierowanie oraz EDM muszą być podpisane jednym z poniższych:

- 1) kwalifikowanym podpisem elektronicznym,
- 2) podpisem zaufanym (Profil Zaufany),
- 3) podpisem osobistym,
- 4) z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych.

Podpis osobisty jest podpisem wprowadzonym przez Ustawę z dnia 6 grudnia 2018 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz.U. 2019 poz. 60).

2.4 Wymagania związane z dostępem do Internetu

Minimalna przepustowość łącza niezbędnego do komunikacji Systemu Usługodawcy z Systemem P1 to 2 Mb/s. Przepustowość ta umożliwia odczyt/zapis kilkunastu dokumentów w ciągu jednej sekundy (średnio około 24 KB na e-Receptę).

Rekomendowana przepustowość łącza umożliwiającego swobodną pracę większej liczbie użytkowników to 90 Mb/s, łącze symetryczne.

2.5 Wymagania funkcjonalne

W celu komunikacji z Systemem P1 System Usługodawcy musi spełnić poniższe wymagania. Poszczególne wymagania muszą być implementowane w zależności od rodzaju świadczeń zdrowotnych udzielanych przez Usługodawcę. Poniżej przedstawia się poszczególne obszary, niemniej przedstawione wymagania muszą być zgodne z Dokumentacją Integracyjną publikowaną przez komórkę właściwą ds. informatyzacji w ochronie zdrowia, powołaną przez Ministra Zdrowia.

a) W obszarze e-Recepty

System podmiotu wykonującego działalność leczniczą:

- 1) wystawienie e-Recepty,
- 2) weryfikacja pakietu e-Recept w P1,
- 3) wydruk i ponowny wydruk kodów i kluczy pakietu e-Recept,
- 4) przeglądanie i pobieranie historycznych e-Recept,
- 5) anulowanie e-Recepty,
- 6) pobranie dokumentu anulowania.

b) W obszarze e-Skierowanie

Wystawienie e-Skierowania:

- 1) wystawienie e-Skierowania,
- 2) weryfikacja e-Skierowania w P1,
- 3) wydruk i ponowny wydruk kodu i klucza e-Skierowania,
- 4) przeglądanie historycznych e-Skierowań pobranych z P1,
- 5) anulowanie e-Skierowania,

² (ang. *Simple Object Access Protocol*) – protokół komunikacyjny wykorzystujący XML do kodowania wywołań i najczęściej protokół HTTP do ich przesyłania.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



6) pobranie dokumentu anulowania.

Realizacja e-Skierowania

- 1) odmowa realizacji e-Skierowania,
- 2) przyjęcie e-Skierowania do realizacji,
- 3) zgłoszenie informacji o braku w dokumentacji,
- 4) rezygnacja z realizacji e-Skierowania,
- 5) zamknięcie realizacji e-Skierowania,
- 6) przeglądanie historycznych e-Skierowań.

Zgodnie z ustawą SIOZ skierowania mogą być wystawiane w postaci papierowej do końca 2020 r.

c) W obszarze Elektronicznej Dokumentacji Medycznej (EDM)

Prowadzenie i wymiana EDM

Zgodnie z art. 13a ustawy SIOZ listę elektronicznych dokumentów medycznych określa rozporządzenie (rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów dokumentacji medycznej). Dokumenty te muszą być prowadzone zgodnie z PIK HL7 CDA. System Usługodawcy musi umożliwiać:

- 1) utworzenie dokumentu,
- 2) podpisanie dokumentu (wszystkimi z poniższych):
 - a) kwalifikowanym podpisem elektronicznym,
 - b) podpisem zaufanym (Profil Zaufany) – podmioty, które zgodnie z obowiązującymi regulacjami mają możliwość integracji z systemem Profilu Zaufanego,
 - c) podpisem osobistym,
 - d) z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych.
- 3) utworzenie nowej wersji dokumentu z zachowaniem poprzedniej, przeglądanie historii dokumentu.
- 4) wyświetlenie dokumentu zgodnie z wizualizacją określoną w PIK HL7 CDA,
- 5) implementacja dokumentów musi być zgodna z pryncypiami standardu HL7 CDA, PIK HL7 CDA oraz regułami opisanymi w instrukcji stosowania,
- 6) po uruchomieniu funkcjonalności P1 związanych z wymianą EDM rejestrowanie co najmniej dokumentów wchodzących w skład EDM w Systemie P1 oraz umożliwienie wymiany tych dokumentów poprzez wyżej wskazany system innym Usługodawcom, udostępnianie usługobiorcom zgodnie z regułami przyjętymi w systemie P1.

d) W obszarze Zdarzeń Medycznych (ZM)

Zgodnie z art. 11 ust. 4a ustawy SIOZ szczegółowy zakres danych zdarzenia medycznego przetwarzanego w systemie informacji, o których mowa w ust. 4 ustawy SIOZ oraz sposób i terminy przekazywania tych danych do SIM, określi w drodze rozporządzenia minister właściwy do spraw zdrowia.

Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. z 2020 r. poz. 1253 z późn. zm.) opisuje szczegółowy zakres danych zdarzenia medycznego przetwarzanego w systemie informacji w ochronie zdrowia. Obejmują one następujące dane:

- 1) dane usługodawcy,
- 2) dane usługobiorcy,
- 3) dane identyfikujące świadczenie zdrowotne,
- 4) dane miejsca udzielenia świadczenia zdrowotnego,
- 5) dane pracownika medycznego udzielającego świadczenia zdrowotnego lub odpowiedzialnego za jego udzielenie, a w przypadku wykonania operacji lub zabiegu w oddziale szpitalnym – dane pracownika medycznego kierującego wykonaniem tej operacji albo zabiegu (operatora),
- 6) dane dotyczące dokumentacji medycznej prowadzonej w postaci elektronicznej zgodnie ze standardem HL7 oraz – w odniesieniu do dokumentacji obrazowej – w formacie DICOM, wytworzonej w związku z udzielonym świadczeniem zdrowotnym,
- 7) inne dane pozwalające na identyfikację zdarzenia medycznego.

Powyższe dane zdarzenia medycznego są traktowane w systemie jako zasoby.

System Usługodawcy musi umożliwiać wykonanie następujących operacji na zasobach dotyczących zdarzeń medycznych:

- 1) operacje rejestracji zasobu,
- 2) operacje odczytu zasobu,
- 3) operacje wyszukania zasobu,
- 4) operacje aktualizacji zasobu,
- 5) operacje usunięcia zasobu.

e) W obszarze Systemu Elektronicznej Rejestracji

System Usługodawcy musi umożliwiać wykonanie następujących operacji na zasobach dotyczących Systemu Elektronicznej Rejestracji:

- 1) przesyłanie do Systemu Elektronicznej Rejestracji (SER) harmonogramów zawierających wolne sloty,
- 2) możliwość dowolnej modyfikacji i usuwania przesłanych harmonogramów do czasu gdy do danego wolnego slotu nie zostanie przypisany pacjent (zapisana wizyta),
- 3) w oparciu o uruchamiany przez SER minimum raz dziennie algorytm dokonujący wyboru pacjentów zgodnie z ich zapisanymi kryteriami dostępności, ustalający ich kolejność na podstawie wag, następnie dokonuje ich przypisania do poszczególnych wolnych slotów zgłoszonych w ramach harmonogramów przez Podmiot,
- 4) przed rozpoczęciem pracy System Podmiotu Leczniczego odpytuje SER w celu pobrania informacji o zapisanych na wizyty pacjentach i zsynchronizowania ich w swoim systemie,
- 5) po uzyskaniu danych osobowych pacjenta przez dany Podmiot (MUŚ), dalsza komunikacja między Podmiotem, a pacjentem realizowana jest bez udziału Systemu Elektronicznej Rejestracji.

f) W obszarze oświadczeń usługobiorcy o których mowa w art. 7 i 7a ustawy SIOZ



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Dotyczy możliwości złożenia przez pacjenta oświadczeń woli, w tym upoważnień i zgód o których mowa w ustawie z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta.

System usługodawcy musi mieć możliwość co najmniej:

- 1) obsłużyć autoryzację na dostęp do dokumentacji elektronicznej poprzez wysłanie zapytania do P1 i rejestrację odebranego kodu SMS,
- 2) obsłużyć komunikację z systemem P1 w celu pobrania informacji o zgodzie na dostęp do dokumentacji medycznej (zgodnie z art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318 i 1524 oraz z 2018 r. poz. 1115 z późn. zm.), lub o wyrażeniu zgody na udostępnienie danych, o której mowa w art. 35 ust. 1, lub o jej wycofaniu) – operacja odczytu zgody na dostęp do dokumentacji medycznej pacjenta,
- 3) obsłużyć komunikację z systemem P1 w celu pobrania informacji o zgodzie na dostęp do informacji o stanie zdrowia Pacjenta (zgodnie z art. 9 ust. 3 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318 i 1524 oraz z 2018 r. poz. 1115 z późn. zm.), lub o jej wycofaniu) – operacja odczytu zgody na dostęp do informacji o stanie zdrowia pacjenta,
- 4) obsłużyć zgody na realizację świadczeń (zgodnie z art. 16-18 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2017 r. poz. 1318 i 1524 oraz z 2018 r. poz. 1115 z późn. zm.), lub o jej odmowie (uruchamia się nie później niż do dnia 30 września 2019 r.).

g) Zaświadczenia o niezdolności do pracy – zwolnienia lekarskie

Wystawiane wyłącznie w postaci elektronicznej. Aktualnie lekarz może wystawiać zwolnienia elektroniczne (e-ZLA):

- 1) na swoim profilu na Platformie Usług Elektronicznych ZUS (PUE ZUS)
- 2) w aplikacji gabinetowej używanej w placówce, w której lekarz przyjmuje pacjentów.

Elektroniczne zwolnienie lekarskie musi być podpisane elektronicznie.

Metody podpisywania e-ZLA:

- 1) podpisem zaufanym (PZ PUAP),
- 2) podpisem osobistym,
- 3) kwalifikowanym podpisem elektronicznym,
- 4) Certyfikatem z ZUS.

Usługodawcy, są obowiązani do zgłoszenia gotowości podłączenia swoich systemów do systemu P1 oraz do podłączenia się do tego systemu. Warunkiem spełnienia powyższego jest złożenie wniosku o założenie konta w P1 i wygenerowanie certyfikatu elektronicznego w Rejestrze Podmiotów Wykonujących Działalność Leczniczą oraz podłączenie do P1.

2.6 Rekomendacje CeZ w zakresie stosowanych rozwiązań technologicznych oraz bezpieczeństwa

Wdrażane w ramach Projektu ZeZ systemy, w zakresie bezpieczeństwa informacji i ochrony danych osobowych oraz stosowanych rozwiązań technologicznych podczas przetwarzania dokumentacji

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

medycznej w postaci elektronicznej muszą spełniać wymagania określone przez Centrum e-Zdrowia w formie rekomendacji.

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Rekomendacje Centrum Systemów Informacyjnych Ochrony Zdrowia w zakresie bezpieczeństwa oraz rozwiązań technologicznych stosowanych podczas przetwarzania dokumentacji medycznej w postaci elektronicznej* oraz w dokumencie pn. *Plan działania w zakresie cyberbezpieczeństwa w ochronie zdrowia - zestaw rekomendacji funkcjonalnych oraz organizacyjnych*

Celem opracowania jest przedstawienie rekomendacji dla usługodawców w zakresie budowania i stosowania systemu bezpiecznego przetwarzania danych medycznych dla podmiotów, w których jest już przetwarzana dokumentacja medyczna w postaci elektronicznej, jak również dla podmiotów, które przygotowują się lub też wdrażają w swoich placówkach systemy informatyczne przetwarzające dokumentację medyczną w postaci elektronicznej.

Dokument skupia się na kwestii przetwarzania dokumentacji medycznej w podmiotach wykonujących działalność leczniczą lub przez podmioty działające w ich imieniu.

Opracowanie zawiera informacje w zakresie rozwiązań technicznych umożliwiających przetwarzanie dokumentacji medycznej w postaci elektronicznej. W dokumencie przedstawione są wymagania organizacyjne oraz wskazano odpowiedzialność za przetwarzanie informacji w tym danych osobowych wrażliwych zawartych w dokumentacji medycznej.

Dokument może mieć zastosowanie do wszystkich systemów przetwarzających dokumentację medyczną w postaci elektronicznej, zarówno systemów dedykowanych do przetwarzania Elektronicznej Dokumentacji Medycznej typu Rejestry i Repozytoria, a także do wszystkich systemów, w których przetwarzana jest dokumentacja medyczna, w tym do systemów szpitalnych i gabinetowych.

2.7 Modele architektury bezpiecznego przetwarzania dokumentacji medycznej

Centrum e-Zdrowia wskazuje jako możliwe do stosowania następujące rozwiązania w obszarze przetwarzania przez usługodawców dokumentacji medycznej w postaci elektronicznej:

- 1) klasyczny model przetwarzania danych,
- 2) modele wykorzystywane w ramach korzystania z możliwości outsourcingu (kolokacja, hosting),
- 3) model przetwarzania w chmurze obliczeniowej.

Decydując się na wybór jednego z modeli przetwarzania danych usługodawca określa tym samym podział i poziom odpowiedzialności za przetwarzanie danych oraz za wykorzystywane zasoby IT pomiędzy sobą, a podmiotem zewnętrznym.

Rekomendacja CeZ przedstawia wymagany podział kontroli i odpowiedzialności pomiędzy usługodawcą a podmiotem zewnętrznym w poszczególnych modelach przetwarzania dokumentacji medycznej.

Model klasyczny

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

W modelu klasycznym usługodawca posiada własną infrastrukturę informatyczną i w związku z tym ponosi koszt zakupu serwerów, infrastruktury sieciowej, oprogramowania, zapewnienia pomieszczenia odpowiednio przygotowanego do pracy serwera, zapewnienia zespołu zajmującego się konserwacją sprzętu, usuwaniem awarii.

Niezależnie od architektury technicznej oraz logicznej rozwiązania, w modelu klasycznym całość odpowiedzialności za bezpieczeństwo danych i zapewnienie ciągłości działania usług leży po stronie usługodawcy (właściciela systemu informatycznego). Szczegółowy opis zawierający minimalne wymagania i zalecenia dotyczące bezpiecznego przetwarzania dokumentacji medycznej w postaci elektronicznej dla modelu klasycznego przedstawiony został w załączniku nr 1 do przedmiotowej Rekomendacji.

Outsourcing

W tym modelu ma miejsce wydzielenie ze struktury organizacyjnej przedsiębiorstwa realizowanych przez nie funkcji i przekazaniu ich do realizacji innym podmiotom często gospodarczym.

Kolokacja: W modelu kolokacji usługodawca przekazuje firmie zewnętrznej serwery lub inne urządzenia teleinformatyczne do przeznaczonych do tego celu pomieszczeń (serwerowni). Podmiot zewnętrzny odpowiada również za zapewnienie odpowiedniego łącza.

Hosting: W modelu hostingu usługodawca dzierżawi od podmiotu zewnętrznego serwer lub określoną objętość dysku twardego, maksymalną ilość danych do przesłania przez łącza internetowe serwerowni i maksymalną moc obliczeniową.

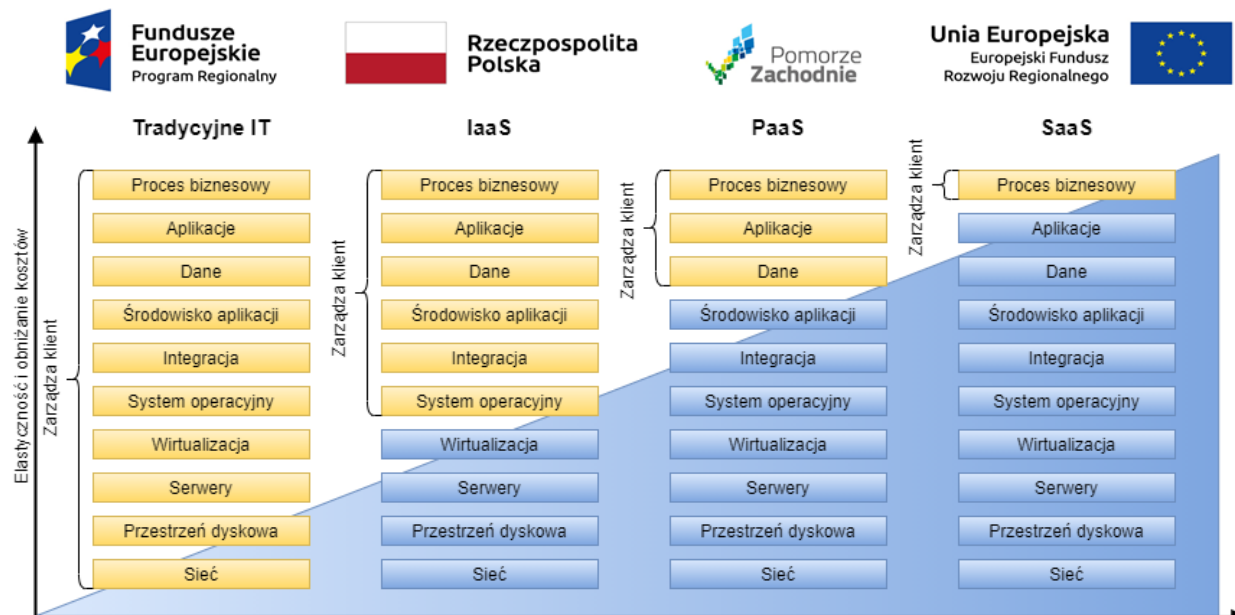
Cloud computing (chmura obliczeniowa)

W tym modelu firmy nie ponoszą nakładów na własną infrastrukturę informatyczną, lecz korzystają z wynajętej infrastruktury lub aplikacji za pośrednictwem sieci. W modelu tym komputery stają się wyłącznie terminalami do prezentacji wyników operacji przeprowadzanych przez centra przetwarzania danych. Chmurę stanowi więc cały zbiór serwerów, oprogramowania, sieci itd., do którego dostęp uzyskuje się za pośrednictwem Internetu.

W zależności od stopnia złożoności dostarczanych usług rozróżnia się następujące rodzaje cloud computingu:

- 1) Infrastructure as a Service – IaaS (Infrastruktura jako usługa),
- 2) Platform as a Service – PaaS (Platforma jako usługa),
- 3) Software as a Service – SaaS (Oprogramowanie jako usługa).

Poniższy rysunek przedstawia podział kontroli pomiędzy usługodawcą a podmiotem zewnętrznym w poszczególnych modelach przetwarzania danych z zastosowaniem rozwiązań chmury obliczeniowej.



Rys.1. Podział kontroli pomiędzy usługodawcą a podmiotem zewnętrznym w modelach przetwarzania danych w chmurze obliczeniowej. (źródło: CSIOZ)

W modelu chmury obliczeniowej typu PaaS, w stosunku do typu IaaS oraz modelu klasycznego, zwiększa się zakres kontroli podmiotu zewnętrznego, który dostarcza środowisko, w którym usługodawca może zarządzać zainstalowanymi aplikacjami.

Z kolei w modelu chmury obliczeniowej typu SaaS usługodawca ma najmniejszy zakres kontroli. Zachowuje on jedynie kontrolę nad danymi. Całość infrastruktury wraz z oprogramowaniem pozostaje pod kontrolą podmiotu zewnętrznego, który odpowiada za ich bezawaryjne działanie.

Chmura prywatna a chmura publiczna (cloud computing)

W zależności od stopnia kontroli zasobów informatycznych udostępnianych w formie usługi rozróżnia się następujące rodzaje cloud computingu:

- 1) public cloud computing (publiczna chmura obliczeniowa),
- 2) private cloud computing (prywatna chmura obliczeniowa).

Chmura publiczna korzysta się ze współdzielonej infrastruktury udostępnianej przez podmioty zewnętrzne za pośrednictwem Internetu. Podstawową cechą chmury publicznej jest jej ogólnodostępny charakter. Podmiot oferujący usługę w ramach chmury publicznej umożliwia dostęp dla wielu odbiorców na tych samych warunkach, zachowując bezpieczeństwo świadczenia usług.

W przypadku tego rozwiązania szczególne znaczenie ma szybkość i niezawodność łącza internetowego w placówce medycznej, ponieważ w przypadku zerwania połączenia nie posiada ona dostępu do danych i możliwości korzystania z systemu. Zapewnienie łącza o odpowiednio dużej przepustowości ma podstawowe znaczenie w przypadku przesyłania plików o dużych rozmiarach np. z diagnostyki obrazowej.

Chmura prywatna jest projektowana dla danej organizacji. W tym przypadku infrastruktura informatyczna jest dedykowana na potrzeby określonej organizacji i jest wyłączona ze współdzielenia z innymi podmiotami. Infrastruktura ta może być zlokalizowana w siedzibie organizacji lub poza nią (przykładowo serwery mogą być kolokowane, tj. mogą znajdować się w serwerowni w podmiocie zewnętrznym, lub ze względów bezpieczeństwa mogą być rozmieszczone w kilku miejscach).

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

W przypadku rozwiązań chmurowych dostęp do danych możliwy jest dla dostawcy rozwiązań. Dlatego wymagane jest stosowanie mechanizmów kryptograficznych w celu zabezpieczenia przed udostępnieniem danych osobom nieupoważnionym oraz zapewnienia pełnej poufności danych.

Przetwarzanie danych w chmurze obliczeniowej to obecnie jedna z najszybciej rozwijających się usług informatycznych. Z punktu widzenia jednostek sektora finansów publicznych istotnego znaczenia w kontekście kierunków rozwoju modeli przetwarzania danych, w tym rozwiązań chmurowych nabiera przyjęty przez Radę Ministrów Program „Wspólna Infrastruktura Informatyczna Państwa” (WIIP)³. Program obejmuje szereg działań organizacyjnych oraz inwestycyjnych w zakresie dostaw infrastruktury informatycznej jako usług w modelu chmury obliczeniowej.

Na Program składają się m. in. następujące strumienie realizacyjne:

- 1) zapewnienie podmiotom administracji publicznej możliwości nabywania usług przetwarzania w Publicznych Chmurach Obliczeniowych (PChO),
- 2) budowa, rozwój i utrzymanie Rządowej Chmury Obliczeniowej (RChO),
- 3) budowa, rozwój i utrzymanie Rządowego Klastra Bezpieczeństwa (RKB), który jest elementem bezpieczeństwa Rządowej Chmury Obliczeniowej,
- 4) opracowanie i wdrożenie Standardów Cyberbezpieczeństwa Chmur Obliczeniowych.

Wśród strategicznych kierunków, jakie wyznacza Program WIIP jest m.in. upowszechnienie modelu przetwarzania w chmurach obliczeniowych, jako głównego sposobu realizacji systemów teleinformatycznych państwa (w tym również zmiana technologii wytwarzania oprogramowania).

Usługi przetwarzania w modelach chmur obliczeniowych będą stanowiły element krajowego systemu stąd konieczne jest dostosowanie do zasad i wymagań zdefiniowanych w ustawie o krajowym systemie cyberbezpieczeństwa oraz rozporządzeń do tej ustawy, w szczególności regulujących kwestie realizacji usług cyberbezpieczeństwa.

Jednym z pierwszych rezultatów programu jest System Zapewniania Usług Chmurowych (ZUCH)⁴ - portal oferowania i pozyskiwania usług chmurowych dla administracji publicznej i dostawców zewnętrznych. Za pośrednictwem Systemu, każda jednostka będzie mogła dokonać zakupu wybranych e-usług, ale też uzyskać pomoc w zakresie wyboru odpowiedniego katalogu usług – Rządowej Chmury Obliczeniowej (RChO) lub Publicznych Chmur Obliczeniowych (PChO).

2.8 Przetwarzanie dokumentacji medycznej w postaci elektronicznej - zagrożenia

Zakres zagrożeń związanych z przetwarzaniem dokumentacji medycznej w postaci elektronicznej dotyczy naruszeń podstawowych atrybutów bezpieczeństwa przetwarzania informacji tj. naruszenie poufności, integralności i dostępności danych medycznych. Wynika wprost z normy PN-EN ISO 27799:2016 Informatyka w ochronie zdrowia -- Zarządzanie bezpieczeństwem informacji w ochronie zdrowia z wykorzystaniem ISO/IEC 27002. W niniejszej Normie Międzynarodowej określono wytyczne, mające na celu wsparcie interpretacji i wdrożenia ISO/IEC 27002 w informatyce w ochronie zdrowia; niniejsza norma jest dla niej normą towarzyszącą.

³ Uchwała nr 97 Rady Ministrów z dnia 11 września 2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” - <http://monitorpolski.gov.pl/mp/2019/862/1>

⁴ <https://chmura.gov.pl/zuch>

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Norma zawiera wskazówki dotyczące wdrażania zabezpieczeń, opisanych w ISO/IEC 27002 i uzupełnia je w razie potrzeby, tak aby mogły być skutecznie wykorzystywane do zarządzania bezpieczeństwem informacji w ochronie zdrowia. Odnosi się do informacji w ochronie zdrowia we wszystkich aspektach, niezależnie od formy informacji (słowa i liczby, nagrania dźwiękowe, rysunki, nagrania wideo i obrazy medyczne), sposobu ich przechowywania (drukowanie lub zapisywanie na papierze, lub przechowywanie w formie elektronicznej) i bez względu na środki wykorzystywane do ich przesyłania (własnoręcznie, faksem, za pośrednictwem sieci komputerowych lub pocztą), ponieważ informacje mają być zawsze odpowiednio chronione.

Dzięki wdrożeniu niniejszej Normy podmioty opieki zdrowotnej i inni dysponenti informacji w opiece zdrowotnej będą w stanie zapewnić minimalny wymagany poziom bezpieczeństwa, który jest odpowiedni w przypadku ich organizacji i który zachowa poufność, integralność i dostępność informacji o stanie zdrowia indywidualnych osób, będących pod ich opieką.

Niniejsza Norma i Norma ISO/IEC 27002 razem określają, co jest wymagane pod względem bezpieczeństwa informacji w opiece zdrowotnej; nie określają, w jaki sposób te wymagania mają zostać spełnione. To oznacza, w najpełniejszym możliwym zakresie, że niniejsza Norma Międzynarodowa jest technologicznie neutralna.

Neutralność w odniesieniu do technologii wdrażania jest cechą istotną, gdyż pozostawia producentom i usługodawcom swobodę proponowania nowych lub rozwijających się technologii spełniających niezbędne wymagania opisane w niniejszej Normie Międzynarodowej.

Zgodnie z normą naruszenie podstawowych atrybutów bezpieczeństwa przetwarzania informacji obejmuje poniższe zagrożenia:

- 1) Nieuprawniony dostęp przez użytkowników polegający na zaistnieniu sytuacji, w której użytkownicy korzystają z kont, do których sami nie mają uprawnień albo korzystania przez wielu użytkowników z tego samego loginu użytkownika i hasła.

Przykładem takiego zwyczaju mogą być sytuacje, w których jeden pracownik medyczny (np. lekarz) może zastąpić innego na stanowisku pracy i kontynuuje prace na już zalogowanym koncie poprzednika co skutkuje brakiem potrzeby przelogowania. Pierwsze logowanie użytkownika pozwala na pracę w systemie i jednocześnie bez uprzedniego wylogowania pozwala na pracę przez innych użytkowników na koncie bieżącego użytkownika. Powyższy przykład zachowania powoduje poważne naruszenia poufności i niezaprzeczalności. Większość naruszeń poufności jest dokonywana przez użytkowników pracujących w danej organizacji a genezą ich powstania są uwarunkowania spowodowane w znacznym zakresie brakiem świadomości użytkowników o zagrożeniach z nich wynikających. W tym miejscu wskazać również należy, że nieuprawniony dostęp przez użytkowników może służyć do próby zatuszowania przypadków lub przypisania zdarzeń innej osobie, gdy zdarzenia takie powstały.

- 2) Nieuprawniony dostęp przez użytkowników (w tym usługodawcy uprawnieni na podstawie umów - personel obsługi technicznej - administratorzy oprogramowania i sprzętu, którzy mogą mieć uzasadniony powód dostępu do systemów i danych) posiadających uprzywilejowany dostęp do systemów i urządzeń polegający na uzyskaniu nieautoryzowanego dostępu do danych.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Działanie takie jest naruszeniem bezpiecznych rozwiązań wynikających z umów outsourcingowych. Nieuprawniony dostęp przez usługodawców może być także źródłem poważnych naruszeń poufności informacji, w tym danych medycznych.

- 3) Nieuprawniony dostęp przez osoby z zewnątrz organizacji - zaistnieje w sytuacji w której nieuprawnione osoby trzecie (hakerzy) posiadają dostęp do danych lub zasobów systemowych, albo poprzez podszywanie się jako autoryzowany użytkownik stanie się upoważnionym użytkownikiem (na przykład przez atak wykorzystujący metody socjotechniczne).
- 4) Nieuprawnione wykorzystanie aplikacji przetwarzającej informacje na temat zdrowia pacjentów skutkujące możliwością uzyskania nieautoryzowanego dostępu do aplikacji informatycznych systemu ochrony zdrowia (np. polegających na dostępie do systemu na niestrzeżonym stanowisku pracy w gabinecie lekarza i przeglądanie na ekranie informacji dotyczących pacjentów).
- 5) Możliwość uszkodzenia lub wprowadzenia do systemu destrukcyjnego oprogramowania obejmującego np. wirusy, lub inne „złośliwe” oprogramowanie).

Większość incydentów bezpieczeństwa IT wiąże się z wprowadzeniem do systemu wirusów komputerowych. Wprowadzenie szkodliwego lub uciążliwego oprogramowania może być spowodowane brakiem ochrony antywirusowej lub kontroli zmian oprogramowania.

- 6) Nadużywanie zasobów systemowych - jest zagrożeniem dla użytkowników systemów informacyjnych i usług korzystających z pracy zdalnej.

Praca zdalna przez wielu użytkowników może również wpływać na pogarszanie się dostępności systemu informacji, spowodowanym na przykład zmniejszeniem przepustowości. Jednocześnie wskazać należy, że nawiązywanie połączeń streamingu video lub audio w celach prywatnych może powodować nadużycia. Konieczne jest więc edukowanie użytkowników o wpływie i znaczeniu utrzymania integralności i dostępności zasobów informacyjnych opieki zdrowotnej.

- 7) Infiltracja komunikacji elektronicznej - występuje wówczas, gdy nieuprawniony użytkownik manipuluje w normalnym przepływie danych w sieci. Najczęstszym atakiem jest atak Denial of Service.
- 8) Przechwycenie komunikacji. W przypadku gdy przekazywanie danych nie następuje w formie zaszyfrowanej (kryptograficzna ochrona transmisji danych) podczas ich przesyłania, może zaistnieć sytuacja, w której zostaną one przechwycone przez nieuprawnioną osobę. Przechwytywanie komunikacji stanowi istotne zagrożenie w bezpieczeństwie komunikacji.
- 9) Brak niezaprzeczalności - zagrożenie, które stanowi, że podczas przetwarzania informacji dochodzi do jej odrzucenia z powodu braku niezaprzeczalności jej pochodzenia lub niezaprzeczalności użytkownika, który ją wysłał (odrzućcie nadania) lub otrzymał (odrzućcie odbioru).

Brak jednoznacznego ustalenia czy dane medyczne, przesyłane z jednego do drugiego podmiotu służby zdrowia, rzeczywiście zostały nadane i odebrane może być jedną z istotnych cech śledztw dotyczących błędów lekarskich. Negowanie może stanowić brak zastosowania elementów sterujących, takich jak podpisy elektroniczne na dokumentacji



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



medycznej (przykład odrzucenie pochodzenia) lub sterujące, takie jak wpływ na odczyt wiadomości e-mail (przykład odrzucenie odbioru).

10) Błąd połączenia (w tym awarie sieci informacyjnych zdrowia).

Wszystkie sieci są przedmiotem okresowych przerw serwisowych. Jakość usług jest głównym czynnikiem ciągłości usług sieciowych w zakresie opieki zdrowotnej. Błąd połączenia może wynikać z niedostępności usług sieciowych (na przykład złośliwe zmiany tablic routingu, które powodują przekierowanie ruchu sieciowego).

11) Osadzanie złośliwego kodu. Zagrożenie to obejmuje wirusy przesyłane w wiadomościach email i wykorzystanie złośliwego kodu mobilnego.

Zwiększenie wykorzystania technologii bezprzewodowych i komórkowych przez pracowników służby zdrowia zwiększa potencjał tego zagrożenia.

12) Przekierowanie połączenia.

Zagrożenie to obejmuje możliwość, że informacje przesyłane przez sieć informatyczną mogą być dostarczone do niewłaściwego adresata.

13) Awaria techniczna systemu lub infrastruktury sieciowej.

Zagrożenia te obejmują awarie sprzętu, awarie sieci lub braki w bazach danych. Takie problemy zwykle stanowią o awarii jednego lub większej liczby elementów powodując jego ograniczone działanie lub niedostępność. Utrata dostępności takich systemów może mieć zagrażające życiu skutki dla pacjentów.

14) Awaria środowiska wsparcia, w tym awarie zasilania i zakłócenia wynikające z oddziaływania fizycznego lub katastrof spowodowanych przez człowieka.

Systemy informacji zdrowotnej mogą być systemami krytycznymi, których naruszenie ciągłości działania podczas klęsk żywiołowych i innych zdarzeń może stanowić zagrożenie życia ludzi. Właściwa ocena zagrożenia i ryzyka informacji na temat zdrowia będzie zawierać wnioski, jak krytyczne są systemy funkcjonujące podczas klęski żywiołowej i jaka będzie ich ciągłość działania.

15) Awaria systemu lub oprogramowania sieciowego.

Ataki DoS są znacznie ułatwione dzięki słabościom lub błędom systemu operacyjnego lub oprogramowaniu sieciowemu.

16) Awaria oprogramowania aplikacji.

Błędy w oprogramowaniu aplikacyjnym mogą zostać wykorzystane na atak Denial of Service oraz mogą być również powodem utraty poufności danych chronionych.

17) Błędne operacje.

Błędy operatora odpowiadają za niewielki, ale znaczący procent niezamierzonych ujawnień poufnych informacji w tym tych dotyczących stanu zdrowia pacjentów

18) Odzyskiwanie po awarii.

19) Błąd konserwacji.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Błędy konserwacji są błędami wywoływanymi przez osoby odpowiedzialne za utrzymanie systemów, sprzętu i oprogramowania. Błędy konserwacyjne mogą być popełniane zarówno przez pracowników jak również przez osobę trzecią. Błędy te mogą jednocześnie zagrażać poufności chronionych danych.

20) Błąd użytkownika.

Błędy generowane przez użytkowników mogą na przykład prowadzić do przestania poufnych informacji do niewłaściwego odbiorcy. Błędne udostępnienie danych osobom nieuprawnionym skutkujące brakiem możliwości odwołania lub cofnięcia przestanych danych powoduje w dalszej kolejności brak kontroli w ich dalszej dystrybucji.

21) Niedobór personelu.

22) Kradzież przez użytkowników w tym kradzież sprzętu lub danych.

23) Kradzież przez osoby z zewnątrz (w tym kradzieży sprzętu lub danych).

24) Samowolne uszkodzenia przez użytkowników - obejmują akty wandalizmu oraz inne przypadki, w których szkoda fizyczna jest wyrządzona systemom informatycznym.

25) Samowolne uszkodzenia przez osoby z zewnątrz.

26) Terroryzm.

Zagrożenie terroryzmem obejmuje akty realizowane przez grupy ekstremistów, którzy mogą chcieć uszkodzić lub zakłócić pracę organizacji ochrony zdrowia albo zaszkodzić pracownikom służby zdrowia jak również zakłócić działanie systemów informacji zdrowotnej.

2.9 Cyberbezpieczeństwo przetwarzania dokumentacji medycznej w postaci elektronicznej

Postęp technologiczny powoduje zwiększone ryzyko utraty danych w wyniku działalności cyberprzestępców.

Dyrektywa NIS (Dyrektywa Parlamentu i Rady UE 2016/114820 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii przyjęta 6 lipca 2016 roku) zakłada poszerzenie współpracy państw członkowskich w kwestii cyberbezpieczeństwa. Jednym z sektorów objętych dyrektywą jest sektor e-zdrowia zawierający zagadnienia przetwarzania elektronicznej dokumentacji medycznej.

Zgodnie z Dyrektywą NIS konieczne jest zapewnienie przez poszczególne podmioty mające udział w przetwarzaniu EDM minimalnego poziomu ochrony dla infrastruktury, w tym sieci i systemów przetwarzających dokumentację medyczną.

Poprzez realizację tego wymogu należy rozumieć wdrożenie odpowiednich środków bezpieczeństwa w warstwie organizacyjnej, technicznej i systemowej oraz w przypadku wystąpienia poważnych incydentów bezpieczeństwa informacji, podjęcie odpowiednich działań ograniczających ich skutki, a także powiadomienie krajowego organu cyberbezpieczeństwa jakim jest CERT Polska.

Dyrektywa NIS nakłada na kraje członkowskie obowiązek zachowania ciągłości funkcjonowania infrastruktury krytycznej, a co za tym idzie nakłada na podmioty odpowiedzialność za:

- 1) ciągłość działania systemów informacji medycznej przetwarzających EDM,



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 2) dostępności repozytoriów danych, czyli bazy danych w jednostkach, w którym informacja jest przechowywana lokalnie,
- 3) dostępności dla użytkowników systemów informatycznych realizowanej między innymi poprzez ciągłość pracy serwerów odpowiedzialnych za uwierzytelnianie tj. przeprowadzenie kontroli dostępu i uwierzytelniania użytkowników,
- 4) ciągłości działania informatycznych systemów laboratoryjnych - Laboratory Information System (LIS),
- 5) ciągłości działania informatycznych systemów radiologicznych - Radiology Information Systems (RIS),
- 6) dostępności elektronicznej dokumentacji medycznej zawartych w elektronicznych kartach zdrowia,
- 7) kluczowych usług niezbędnych do świadczenia opieki zdrowotnej.

Zapisy Dyrektywy NIS na polskim gruncie są zawarte w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560). Ustawa reguluje zasady funkcjonowania krajowego systemu cyberbezpieczeństwa, którego zadaniem będzie zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług.

Efektom tych działań będzie podniesienie odporności kluczowych usług świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni. Tym samym przyczyni się do lepszego zapewnienia ciągłości działania tych usług, tak, aby zarówno obywatele jak i przedsiębiorstwa mieli do nich stały dostęp.

Przez krajowy system cyberbezpieczeństwa rozumie się wszystkie nowe podmioty w obrocie prawnym, realizujące techniczne i organizacyjne zadania w systemie. Regulacja ta również obejmuje świadczeniodawców, którzy zostali uznani za operatora usług kluczowych na podstawie decyzji administracyjnej wydanej przez organ właściwy ds. cyberbezpieczeństwa.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

2.10 Dokumentacja integracyjna

Dokumentacja integracyjna opracowana i udostępniona przez Centrum e-Zdrowia ma na celu dostarczenie dostawcom oprogramowania podlegającego integracji z Systemem P1 specyfikacji technicznej poszczególnych usług realizowanych w procesie integracji. **Wszystkie usługi i funkcjonalności w Projekcie muszą być w pełni zgodne z obowiązującą wersją Dokumentacji Integracyjnej.**

Dokumentacja na dzień dzisiejszy nie ma charakteru zamkniętego i skończonego. Jest na bieżąco uzupełniana i w sposób przyrostowy rozszerzana. Jest to wynikiem z jednej strony prowadzonych prac nad rozwojem rozwiązania, z drugiej jako wynik trwającego wdrożenia pilotażowego. Wykonawca jest zobowiązany do stosowania aktualnych wersji dokumentacji integracyjnej dla wdrażanych rozwiązań. Dokumentacja integracyjna publikowana jest przez Centrum e-Zdrowia na stronie ezdrowie.gov.pl

2.10.1 Zdarzenia medyczne (ZM)

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie obsługi ZM.*

Opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie obsługi Zdarzeń Medycznych i obejmuje swoim zakresem specyfikację usług związanych z rejestracją i odczytem Zdarzeń Medycznych w Systemie P1.

W dokumencie opisane zostały role, transakcje i struktury obsługiwane przez system P1.

2.10.2 Elektroniczna Dokumentacja Medyczna (EDM)

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie obsługi EDM.*

Opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie przekazywania i wyszukiwania indeksów EDM. W dokumencie opisane zostały role, transakcje i struktury obsługiwane przez system P1.

Dokument obejmuje swoim zakresem specyfikację usług związanych z zapisem i wyszukiwaniem indeksów EDM. Aspekty bezpieczeństwa, uwierzytelnienia, polityk i deklaracji zgód oraz dodatkowe transakcje będą opisane w kolejnych wersjach specyfikacji.

Celem dokumentu jest przedstawienie wymagań i założeń dot. funkcjonowania indeksowania EDM, dla których standard XDS.b określił tylko ramy (np. w zakresie identyfikatorów), albo które wykraczają poza standard, a ich znajomość jest konieczna do tego, żeby systemy zewnętrzne mogły w skuteczny sposób podłączyć się do systemu P1.

2.10.3 Nadawanie dostępu do danych medycznych pacjenta

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie nadawania dostępu do danych medycznych pacjenta (autoryzacja).*

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Opracowanie stanowi uzupełnienie dokumentacji technicznej dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie nadawania uprawnień dostępu do danych medycznych pacjenta dla pracowników medycznych, z wykorzystaniem autoryzacji SMS. Dodatkowo, usługa została rozszerzona o operację odczytu zdefiniowanych kanałów komunikacji przez Usługobiorcę.

Dokument obejmuje swoim zakresem specyfikację usług związanych z obsługą wniosku o nadanie uprawnień dostępu do danych medycznych pacjenta dla pracowników medycznych z wykorzystaniem autoryzacji SMS, tj. usługę złożenia wniosku o nadanie uprawnień dla pracownika medycznego, usługę autoryzacji wniosku za pomocą jednorazowego kodu autoryzacji oraz usługę odczyt kanałów komunikacji Usługobiorcy.

Usługa sieciowa w zakresie nadawania dostępu do danych medycznych pacjenta rozszerza wykaz usług na środowisku systemu P1, określonym w dokumentacji technicznej dla dostawców oprogramowania podlegającego integracji z systemem P1.

2.10.4 Odczyt zgód pacjenta

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie obsługi zgód pacjenta*.

Opracowanie stanowi uzupełnienie dokumentacji technicznej dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie obsługi zgód pacjenta na dostęp do informacji o stanie zdrowia, do dokumentacji medycznej oraz zgód na świadczenie medyczne.

Usługa sieciowa w zakresie obsługi zgód pacjenta rozszerza wykaz usług na środowisku systemu P1, określonym w dokumentacji technicznej dla dostawców oprogramowania podlegającego integracji z systemem P1.

Dokument obejmuje swoim zakresem specyfikację usług związanych z obsługą zgód pacjenta tj. usługę odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia zarejestrowanej w systemie P1, usługę odczytu zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1 oraz usługę zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne.

2.10.5 e-Recepta

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie e-Recepty*.

Opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie e-Recepty. W dokumencie przedstawione zostały procedury związane z uzyskaniem uprawnień do systemu P1 wraz z szablonem wniosku oraz opisem sposobu zgłaszania do CeZ błędów i zagadnień.

Dokument obejmuje swoim zakresem specyfikację usług związanych z zapisem, odczytem, realizacją, anulowaniem recept oraz korektami realizacji.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

2.10.6 e-Skierowanie

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna Systemu P1 w zakresie e-Skierowania*.

Opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie e-Skierowanie. W dokumencie przedstawione zostały procedury związane z uzyskaniem uprawnień do systemu P1 wraz z szablonem wniosku oraz opisem sposobu zgłaszania do CeZ błędów i zagadnień.

Dokument obejmuje swoim zakresem specyfikację usług związanych z zapisem, odczytem, realizacją i anulowaniem skierowania.

2.10.7 e-Rejestracja

Rekomendacje Centrum e-Zdrowia zamieszczone są w dokumencie pn. *Dokumentacja integracyjna systemu p1 w zakresie systemu elektronicznej rejestracji*.

Opracowanie stanowi dokumentację techniczną dla dostawców oprogramowania podlegającego integracji z systemem P1 w zakresie zarządzanie harmonogramami oraz wizytami w Systemie Elektronicznej Rejestracji. Ponadto w dokumencie przedstawione zostały procedury związane z uzyskaniem uprawnień do systemu P1.

Dokument obejmuje swoim zakresem specyfikację operacji oraz opisuje sposób uwierzytelnienia i autoryzacji.

2.11 Rekomendacje Rady ds. Interoperacyjności

Rada ds. Interoperacyjności jest organem doradczo-opiniodawczym Dyrektora Centrum e-Zdrowia. Zadaniem Rady jest rekomendowanie standardów interoperacyjności na poziomie technicznym, semantycznym czy organizacyjnym. Ponadto Rada wskazuje kierunki zmian systemu prawnego oraz strategii systemu ochrony zdrowia w zakresie niezbędnym dla osiągnięcia interoperacyjności legislacyjnej.

Rada ds. Interoperacyjności, w skład której wchodzi przedstawiciele wszystkich interesariuszy systemu ochrony zdrowia tj.: przedstawiciele samorządów, organizacji pozarządowych oraz dostawcy oprogramowania i regulatorzy wraz z NFZ, przyjęła oraz zaleca do stosowania Rekomendacje⁵ dotyczące kompleksowego wsparcia procesu implementacji interoperacyjnych rozwiązań IT. Znajdują się w nich zalecenia ekspertów w jaki sposób implementować profile IHE w systemach informatycznych na poziomie centralnym, a także w rozwiązaniach regionalnych i lokalnych.

Zgodnie z zaleceniami zawartymi w Rekomendacjach, interoperacyjność rozwiązań w oparciu o profile IHE w obszarze ochrony zdrowia w Polsce dotyczy następujących obszarów funkcjonalnych:

- 1) elektroniczne skierowanie,
- 2) wymiana elektronicznej dokumentacji medycznej.

⁵ Rekomendacja Rady ds. Interoperacyjności w zakresie wyboru profili IHE z dnia 20 czerwca 2018 r.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Ponadto Zespół Rady Interoperacyjności ds. Architektury rekomenduje wykorzystanie następujących profili IHE w Systemie P1 oraz w innych systemach wspierających wymianę dokumentów medycznych w postaci elektronicznej, w szczególności w Platformach Regionalnych i w systemach usługodawców:

- 1) XDS.b [Cross-Enterprise Document Sharing],
- 2) ATNA [Audit Trail and Node Authentication],
- 3) CT [Consistent Time Integration],
- 4) PIX [Patient Identifier Cross Referencing],
- 5) PDQ [Patient Demographics Query],
- 6) APPC [Advanced Patient Privacy Consent].

Jako uzupełnienie wykorzystania Profilu XDS.b rekomendowane jest zastosowanie Profilu XCA [Cross-Community Access] w celu umożliwienia wymiany elektronicznych dokumentów medycznych poza domeną XDS.b.

2.12 Współpraca z platformą P1 - założenia⁶

Dokumentem referencyjnym określającym wymagany zakres współpracy jest dokument pn. *P1-DZ Założenia współpracy regionów z P1* wydany przez CSIOZ.

Dokument wskazuje kierunki, w których obecnie wdrażane na szczeblu centralnym rozwiązania będą zmierzały tak w wymiarze funkcjonalnym jak również w sposobach realizacji zasad interoperacyjności. Horyzont czasowy to m.in. najbliższe dwa lata co jest zbieżne z okresem realizacji Projektu.

Zgodnie z zapisami regulaminu konkursu *Projekty z obszaru wspieranego w ramach P1 zapewniają integrację funkcjonalną z Elektroniczną Platformą Gromadzenia, Analizy i Udostępnienia Zasobów Cyfrowych o Zdarzeniach Medycznych (...)*.

Z kolei uchwała Nr 46/2018/XVIII Komitetu Sterującego do spraw koordynacji interwencji EFSI w sektorze zdrowia z dnia 25 września 2018 r. w sprawie rekomendacji dla kryteriów wyboru projektów z sektora zdrowia w ramach Priorytetu Inwestycyjnego 2c - Wzmocnienie zastosowań TIK dla e-administracji, e-uczenia się, e-włączenia społecznego, e-kultury i e-zdrowia w Załączniku do uchwały w punkcie II.1 przyjmuje następujące rekomendacje: (...) *projekty, w tym m.in. polegające na dostosowaniu systemów informatycznych świadczeniodawców do wymiany danych z Systemem Informacji Medycznej lub z systemami innych świadczeniodawców, będą weryfikowane pod kątem komplementarności, interoperacyjności oraz nie dublowania funkcjonalności przewidzianych w krajowych Platformach P1 lub P2 lub P4 lub eKrew.*

Mając powyższe na uwadze:

- 1) Projekt nie może powielać celów i funkcjonalności platform i systemów realizowanych na poziomie krajowym o ogólnokrajowej skali,
- 2) wdrożone rozwiązanie będzie musiało ulec dostosowaniu do zmian przepisów prawa,

⁶ CeZ (CSIOZ) P1-DZ Założenia współpracy regionów z P1

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 3) zakres wymaganych zmian będzie wynikał z wypracowanych przez CeZ standardów opublikowanymi z Biuletynie Informacji Publicznej ministra właściwego dla zdrowia.

Na dzień przygotowania niniejszego dokumentu CeZ określa następujące zasady oraz kierunki rozwoju systemów w obszarze e-Zdrowia, które muszą być uwzględnione w Projekcie tj.:

- 1) domenowość,
- 2) zgody,
- 3) Regionalny Portal Pacjenta.

2.13 Domenowość

1. Wszyscy usługodawcy wytwarzający dokumentację EDM podlegającą indeksowaniu w Systemie P1 zobowiązani są należeć do Krajowej Domeny XDS.
2. Obowiązek indeksowania przez usługodawców dokumentów w rejestrze Systemu P1, który wejdzie w życie w 2021 r., dotyczy dokumentów w postaci elektronicznej zgodnych z PIK HL7CDA oraz – w przypadku dokumentów obrazowych – w formacie DICOM. Powyższe będzie stanowiło element systemu raportowania tzw. zdarzeń medycznych, o którym mowa w ustawie SIOZ.
3. Poza dokumentami określonymi w pkt.2, indeksacji w rejestrze Systemu P1 podlegać będą wszystkie dokumenty medyczne prowadzone przez Usługodawców w postaci elektronicznej o ile będą zgodne z międzynarodowym standardem HL7 CDA.
4. Kluczową rekomendowaną funkcjonalnością platform regionalnych powinno być pełnienie roli repozytorium dla wytwarzanej przez usługodawców podłączonych do danej platformy regionalnej dokumentacji medycznej w postaci elektronicznej (w tym nie stanowiącej EDM).
5. W ramach platform regionalnych, lokalnych oraz korporacyjnych podmioty mają dowolność w zapisywaniu w repozytorium i zamieszczaniu w regionalnym /lokalnym /korporacyjnym rejestrze wszystkich dokumentów elektronicznych niezależnie od ich formatu.
6. Lokalne/regionalne/korporacyjne repozytoria dokumentów będą udostępniać dokumenty wymienione w pkt. 2 na potrzeby ich pobierania/prezentacji z poziomu Internetowego Konta Pacjenta (dalej: IKP) (pacjent.gov.pl) w Systemie P1.
7. W ramach platformy regionalnej wyszukiwanie i wymiana dokumentacji medycznej może być realizowana niezależnie od Systemu P1 (Krajowej Domeny XDS), przy czym w zależności od potrzeby rekomendowane jest wyszukiwanie w rejestrze Krajowej Domeny XDS w celu pozyskania pełnej informacji medycznej pacjenta w rozumieniu pkt. 2, przy uwzględnieniu zgód wydanych przez pacjenta dla podmiotów biorących udział w wymianie dla dokumentów innych niż wskazane w pkt. 2.
8. Usługodawca może być członkiem dowolnej liczby Domen XDS, tym samym spełniać obowiązki rejestracji dokumentów w każdym rejestrze domeny, wynikające ze specyfikacji.
9. Krajowa Domena XDS w obecnym kształcie nie zakłada wykorzystywania Profilu XCA dla wymiany EDM znajdujących się w Domenie Krajowej.
10. Krajowa Domena XDS będzie posiadała dostosowaną do potrzeb:
 - 1) Politykę wymiany informacji,
 - 2) Zestaw reguł dla zgód pacjenta.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



11. Decyzja w zakresie wykorzystania bramki XCA w funkcjonowaniu innych domen (poza domeną krajową) pozostaje każdorazowo w decyzji podmiotu prowadzącego rejestr.
12. W ramach komunikacji systemu regionalnego z systemem P1 należy wykorzystać certyfikaty poszczególnych podmiotów, tj. system regionalny współpracuje z systemem P1 w imieniu podmiotu leczniczego. W chwili obecnej P1 nie przewiduje wystawiania odrębnych certyfikatów systemom regionalnym.
13. System regionalny wraz z przyłączonymi do niego szpitalami tworzył będzie odrębną domenę XDS (Affinity Domain).

Uwaga: W Projekcie ZeZ zaimplementowane zostaną jedynie te rekomendacje CeZ spośród wymienionych powyżej, które mają charakter obligatoryjny. Nie będą miały zastosowania wymienione w punktach: 7, 13 co jest zgodne z Rekomendacjami Komitetu Sterującego.

2.14 Zgody

1. Elektroniczne zgody pacjenta na dostęp pracownika medycznego (dalej: PM) do dokumentacji można udzielać:
 - 1) w ramach preautoryzacji (w IKP),
 - 2) w ramach jednorazowej autoryzacji (w gabinecie lekarskim poprzez kod przesłany SMS),
 - 3) inny sposób uzupełniający w ramach rejestru zgód (przez portal pacjenta lub aplikację mobilną).
2. Prezentowany przez Centrum e-Zdrowia system zgód musi realizować poniższe zasady:
 - 1) dla **Pracownika medycznego (PM)**:
 - a) określona osoba będąca PM (lekarz, lekarz dentyista, pielęgniarka, położna, farmaceuta, felczer) będzie mieć dostęp do dokumentacji pacjenta, z wybranego przez pacjenta okresu leczenia,
 - b) w ramach nadawania zgody pacjent będzie w IKP wyszukiwał i wskazywał PM, któremu chce nadać dostęp.
 - 2) dla **Podmiotu leczniczego**:
 - a) wszyscy PM wskazanej przez pacjenta podmiotu leczniczego (szpitala, przychodni, poradni) będą mieli dostęp do dokumentacji z wybranego przez pacjenta okresu leczenia,
 - b) wyszukiwanie podmiotów leczniczych obecnie jest realizowane przez wskazania danych takich nazwa oraz przez podanie adresu podmiotu (miasto, nazwa ulicy),
 - c) w IKP będzie w przyszłości możliwe udzielenie zgody na pełen zakres dokumentacji medycznej (zarówno elektronicznej jak i papierowej).
3. W ramach IKP pacjent może udzielać innych zgód:
 - 1) na świadczenia medyczne wyrażona przed badaniami lub zabiegami - dodatkowo pacjent jest informowany o opisie zabiegu, rozpoznania, datach wystawienia i dacie planowanego zabiegu oraz danych PM i swoich danych (wprowadzonych przez podmiot medyczny, który potrzebuje uzyskać zgody). Zgoda przyjmuje w zależności od kroku w procesie różne statusy, niezbędne do jej dalszego procedowania. W IKP dostępna będzie prezentacja listy zgód dostępnych z poziomu pacjenta o określonych statusach,



Fundusze Europejskie
Program Regionalny



Rzeczpospolita
Polska



Pomorze
Zachodnie

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 2) dla wskazanej osoby do uzyskania od placówek medycznych informacji o stanie zdrowia pacjenta,
 - 3) dla wskazanej osoby do uzyskania od placówek medycznych dostępu do dokumentacji medycznej.
4. Ogólne zasady:
- 1) Zgody w Systemie P1 pacjent nadaje z poziomu IKP.
 - 2) System P1 nie wykorzystuje i nie wspiera wymiany artefaktów zgód (BPPC, APPC).
 - 3) Zakłada się udostępnienie funkcjonalności weryfikującej po wpisaniu identyfikatora pacjenta (PESEL):
 - a) istnienie dokumentacji pacjenta możliwej do udostępnienia i zgody na dostęp do niej,
 - b) istnienie dokumentacji pacjenta możliwej do udostępnienia, ale brak jest zgody pacjenta na dostęp do niej,
 - c) brak dokumentacji pacjenta możliwej do udostępnienia.
 - 4) Nie przewiduje się udostępniania zawartości nadanych w IKP zgód podmiotom czy przekazywania ich do regionów w celach przetwarzania. Weryfikacja zgód następuje tylko i wyłącznie na poziomie Systemu P1.
 - 5) Realizacja dostępu do dokumentacji medycznej indeksowanej w P1, jest możliwa tylko i wyłącznie przez odpytanie/pozyskanie z P1 informacji o zgodach na taki dostęp.
 - 6) Zgody wydane w danym podmiocie w formie papierowej są obowiązujące na poziomie podmiotu dla dokumentacji papierowej oraz elektronicznej wytworzonej w tym podmiocie.
5. W P1 zdefiniowane będą deklaracje zgody (określające kiedy, komu i co pacjent lub jego przedstawiciel ustawowy zgodził się udostępnić; np. wszystkie dokumenty swojemu pełnomocnikowi, określone dokumenty PM określonego podmiotu leczniczego).
6. Zgody automatyczne (polityki globalne) to:
- 1) dostęp do EDM bez ograniczenia czasowego dla pracownika medycznego, który wytworzył elektroniczną dokumentację medyczną zawierającą dane osobowe lub jednostkowe dane medyczne Usługobiorcy - weryfikacja realizowana w oparciu o dane wystawcy dokumentu,
 - 2) dostęp do EDM dla lekarza, pielęgniarki lub położnej udzielający usługobiorcy świadczeń opieki zdrowotnej w ramach umowy o udzielanie świadczeń opieki zdrowotnej z zakresu podstawowej opieki zdrowotnej,
 - 3) dostęp do EDM dla PM wykonujący zawód u usługodawcy, u którego została wytworzona elektroniczna dokumentacja medyczna zawierająca dane osobowe lub jednostkowe dane medyczne usługobiorcy, w związku z wykonywaniem przez niego zawodu u tego usługodawcy, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia, jeżeli jest to niezbędne do prowadzenia diagnostyki lub zapewnienia ciągłości leczenia - Funkcjonalność realizowana poprzez dodanie atrybutu deklaracji trybu dostępu (kontynuacja leczenia) w kontekście wyszukiwania dokumentu,



Fundusze Europejskie
Program Regionalny



**Rzeczpospolita
Polska**



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 4) dostęp do EDM dla każdego PM w sytuacji zagrożenia życia usługobiorcy - Funkcjonalność realizowana poprzez dodanie atrybutu deklaracji trybu dostępu (ratowanie życia) w kontekście wyszukiwania dokumentu,
- 5) w procesie wymiany dokumentów w trybie określonym w pkt.3, wymagane jest przekazanie do Systemu P1 logu z wymiany w formacie ATNA.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

3. Profile oraz transakcje IHE w Projekcie

Podstawowym założeniem Projektu ZeZ jest zapewnienie interoperacyjności systemów. Przyjęto, że wymiana danych będzie oparta o uznane międzynarodowe standardy i profile interoperacyjności w ochronie zdrowia oraz ich krajowe specyfikacje pochodne.

Wymiana danych pomiędzy poszczególnymi komponentami składającymi się na system informacji medycznej będzie odbywać się w oparciu o transakcje profili integracyjnych IHE w obszarach związanych z wymianą dokumentów medycznych.

W dalszej perspektywie – o ile będzie tego wymagał rozwój obszarów integracji - w sytuacjach nieobjętych zakresem profili integracyjnych IHE, istnieje możliwość opracowania własnych, dedykowanych specyfikacji interfejsów i operacji w oparciu o standard HL7 FHIR. Zastosowanie standardu FHIR umożliwia implementację interfejsów komponentów warstwy logiki biznesowej w sposób umożliwiający ich łatwe wykorzystanie przez komponenty warstwy prezentacyjnej.

Założono również wykorzystanie dostępnych profili IHE dotyczących bezpieczeństwa i poufności wymiany danych medycznych, zgodnych z obowiązującym opisem Systemu P1 w zakresie obsługi EDM.

4. Elektroniczna Dokumentacja Medyczna w Projekcie

Podstawowym aktem prawnym regulującym kwestie dokumentacji medycznej jest ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Ustawa w art. 30 ust. 1 zawiera delegację do rozporządzenia Ministra Zdrowia z dnia 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania określającego co stanowi dokumentację medyczną, w jaki sposób powinna być przetwarzana i udostępniana.

Pojęcie elektronicznej dokumentacji medycznej wprowadza ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Ustawa ta w art. 2 pkt 6 wskazuje, że elektroniczną dokumentacją medyczną są dokumenty wytworzone w postaci elektronicznej, opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym lub podpisane z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych:

- 1) recepty,
- 2) określone w przepisach wydanych na podstawie art. 13a,
- 3) skierowania określone w przepisach wydanych na podstawie art. 59aa ust. 2 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

Jednocześnie na mocy art. 13a wydano rozporządzenie Ministra Zdrowia z dnia 8 maja 2018 r. w sprawie rodzajów elektronicznej dokumentacji medycznej. Na mocy tego rozporządzenia wskazano, że Elektroniczną dokumentacją medyczną (oprócz e-Recepty i e-Skierowania) stanowią:

- 1) informacja o rozpoznaniu choroby, problemu zdrowotnego lub urazu, wynikach przeprowadzonych badań, przyczynie odmowy przyjęcia do szpitala, udzielonych świadczeniach zdrowotnych oraz ewentualnych zaleceniach - w przypadku odmowy przyjęcia



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



pacjenta do szpitala, o której mowa w przepisach wydanych na podstawie art. 30 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,

- 2) informacja dla lekarza kierującego świadczeniobiorcę do poradni specjalistycznej lub leczenia szpitalnego o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach spożywczych specjalnego przeznaczenia żywieniowego i wyrobach medycznych, w tym okresie ich stosowania i sposobie dawkowania oraz wyznaczonych wizytach kontrolnych, o której mowa w przepisach wydanych na podstawie art. 137 ust. 2 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych,
- 3) karta informacyjna z leczenia szpitalnego, o której mowa w przepisach wydanych na podstawie art. 30 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta,
- 4) wyniki badań laboratoryjnych wraz z opisem
- 5) opis badań diagnostycznych, innych niż wskazane w pkt 4.

Reguły biznesowe i walidacyjne dla wymienionych powyżej typów elektronicznych dokumentów medycznych zawiera udostępniona przez Centrum e-Zdrowia *Polska Implementacja Krajowa HL7 CDA*, która jest polską implementacją standardu HL7 CDA na potrzeby elektronicznych dokumentów medycznych przetwarzanych na Platformie P1. Są to:

Grupa pierwsza - Dokumenty przetwarzane na platformie P1:

- 1) e-Recepta:
 - a) szablon CDA dokumentu recepty,
 - b) szablon CDA dokumentu recepty wystawionej przez farmaceutę w aptecę,
 - c) szablon CDA dokumentu recepty na import docelowy,
 - d) szablon CDA dokumentu recepty spełniającej wymagania związane z refundacją.
- 2) e-Skierowanie:
 - a) szablon CDA dokumentu skierowania,
 - b) szablon CDA dokumentu skierowania do szpitala psychiatrycznego,
 - c) szablon CDA dokumentu skierowania do uzdrowiska,
 - d) szablon CDA dokumentu skierowania do zakładu opiekuńczego,
 - e) szablon CDA dokumentu skierowania na pielęgniarską opiekę długoterminową,
 - f) szablon CDA dokumentu skierowania na badania w związku z podejrzeniem choroby zawodowej.

Grupa druga – dokumenty indeksowane na platformie P1, wytwarzane na podstawie jednostkowych danych medycznych przetwarzanych w systemach informatycznych Podmiotów Wykonujących Działalność Leczniczą:

- 1) karta informacyjna leczenia szpitalnego - szablon CDA dla karty informacyjnej leczenia szpitalnego,
- 2) karta odmowy przyjęcia do szpitala - szablon CDA karty odmowy przyjęcia do szpitala,
- 3) konsultacja lekarska - szablon CDA dokumentu konsultacji lekarskiej,

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 4) karta indywidualnej opieki pielęgniarskiej - zawiera szablony dokumentów:
 - a) kartę oceny stanu pacjenta - szablon CDA dokumentu karty pielęgniarskiej oceny stanu pacjenta,
 - b) kartę wywiadu pielęgniarskiego - szablon CDA karty wywiadu pielęgniarskiego,
 - c) raport pielęgniarski - szablon CDA wpisu do raport pielęgniarskiego,
 - d) zalecenia pielęgniarskie przy wypisie ze szpitala - szablon CDA dokumentu karty pielęgniarskiej oceny stanu pacjenta,
- 5) opis badania diagnostycznego- szablon CDA dla dokumentu opisu badania,
- 6) szablon CDA dokumentu Historia choroby
- 7) szablon CDA dokumentu Historia zdrowia i choroby,
- 8) sprawozdanie z badania laboratoryjnego - szablon CDA sprawozdania z badania laboratoryjnego,
- 9) protokół operacyjny -szablon CDA dla protokołu operacyjnego,
- 10) wpis do karty uodpornienia - szablon CDA dokumentu wpisu do karty uodpornienia,
- 11) szablon bazowy -szablon CDA dokumentu bazowego.

Wdrożone w ramach Projektu systemy oprogramowania będą w pełni stosowały w zakresie dokumentacji medycznej omówione powyżej kwestie, w tym reguły ujęte w dokumencie pn. *Polska Implementacja Krajowa HL7 CDA*. Podręcznik implementatora PIK oraz rejestr OID dostępne są na stronie PIK HL7 CDA⁷

4.1 Metody uwierzytelniania dokumentów medycznych

W ramach Projektu ZeZ, zgodnie z ustawą z dnia 20 lipca 2018 roku o zmianie ustawy o systemie informacji w ochronie zdrowia, dopuszczone są następujące metody uwierzytelniania dokumentów medycznych:

- 1) Podpis elektroniczny weryfikowany certyfikatem kwalifikowanym,
- 2) Podpis zaufany,
- 3) Podpis osobisty - zaawansowany podpis elektroniczny z wykorzystaniem certyfikatu podpisu osobistego,
- 4) Certyfikat ZUS - z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez Zakład Ubezpieczeń Społecznych.

Podpis osobisty jest podpisem wprowadzonym przez ustawę z dnia 6 grudnia 2018 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz.U. 2019 poz. 60). Zgodnie z zapisami ustawy jest to w rozumieniu art. 3 pkt 11 rozporządzenia 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 uchylającego dyrektywę 1999/93/WE, weryfikowany za pomocą certyfikatu podpisu osobistego. Z kolei certyfikat podpisu osobistego to poświadczenie elektroniczne, które przyporządkowuje dane

⁷ <https://www.cez.gov.pl/HL7POL-1.3.2/plcda-html-1.3.2/plcda-html/>

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

służące do walidacji podpisu osobistego do posiadacza dowodu osobistego, potwierdzające dane tego posiadacza. Metoda zawierania podpisu elektronicznego w dokumencie medycznym określona jest w specyfikacji oraz instrukcji dla implementatorów w ramach Polskiej Implementacji Krajowej HL7 CDA.

5. Zdarzenia Medyczne w Projekcie

Podmioty lecznicze mają obowiązek przekazywać do platformy P1 dane zdarzeń medycznych, które będą przetwarzane w Systemie Informacji Medycznej (SIM).

5.1 Informacje ogólne

Zdarzenie Medyczne jest to świadczenie zdrowotne, czyli działanie służące profilaktyce, zachowaniu, ratowaniu, przywracaniu lub poprawie zdrowia oraz inne działanie medyczne wynikające z procesu leczenia. Obowiązek przekazywania do SIM danych dotyczących zdarzenia medycznego dotyczy wszystkich usługodawców niezależnie od źródła finansowania udzielanych świadczeń zdrowotnych, jak również niezależnie od rodzaju udzielanych świadczeń oraz formy organizacyjnej usługodawcy

Założenia - podstawy prawne

Głównym celem stworzenia Elektronicznej Platformy Gromadzenia, Analizy i Udostępniania Zasobów Cyfrowych o Zdarzeniach Medycznych (P1) jest budowa elektronicznej platformy usług publicznych w zakresie ochrony zdrowia, która umożliwi organom administracji publicznej i obywatelom gromadzenie, analizę i udostępnianie zasobów cyfrowych o zdarzeniach medycznych w zakresie zgodnym z ustawą z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Jej zadaniem będzie usprawnienie procesów związanych z planowaniem i realizacją świadczeń zdrowotnych, monitorowaniem i sprawozdawczością z ich realizacji, dostępem do informacji o udzielanych świadczeniach oraz publikowaniem informacji w obszarze ochrony zdrowia.

W systemie P1 znajdują się informacje o zdarzeniach medycznych wszystkich obywateli Polski – niezależnie od płatnika – oraz obywateli Unii Europejskiej i innych krajów, którzy skorzystają ze świadczeń zdrowotnych w Polsce.

Obowiązek przekazywania danych do platformy P1 spoczywa na wszystkich podmiotach leczniczych, także na praktykach lekarskich, prywatnych gabinetach i przychodniach, gdyż ustawa z 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia definiuje usługodawcę jako „świadczeniodawcę, o którym mowa w art. 5 pkt 41 ustawy z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, oraz aptekę”. Świadczeniodawcą z kolei jest podmiot wykonujący działalność leczniczą w rozumieniu przepisów o działalności leczniczej, a także osoba fizyczna, która uzyskała fachowe uprawnienia do udzielania świadczeń zdrowotnych i udziela ich w ramach wykonywanej działalności gospodarczej, oraz podmiot realizujący czynności z zakresu zaopatrzenia w wyroby medyczne.

Zmiana definicji zdarzenia medycznego



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Dotychczasowe pojęcie zdarzenia medycznego definiowała ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Rozumiane było jako czynność w ramach świadczenia zdrowotnego lub świadczenia zdrowotnego rzeczowego i odnosiło się do:

„zakażenia pacjenta biologicznym czynnikiem chorobotwórczym, uszkodzenia ciała lub rozstroju zdrowia pacjenta albo śmierci pacjenta będącego następstwem niezgodnych z aktualną wiedzą medyczną:

1. diagnozy, jeżeli spowodowała ona niewłaściwe leczenie albo opóźniła właściwe leczenie, przyczyniając się do rozwoju choroby,
2. leczenia, w tym wykonania zabiegu operacyjnego,
3. zastosowania produktu leczniczego lub wyrobu medycznego.”

Ustawa z dnia 19 lipca 2019 r. o zmianie niektórych ustaw w związku z wdrażaniem rozwiązań w obszarze e-zdrowia, wprowadzała szereg zmian w obowiązującym prawodawstwie.

Obecnie zdarzenie medyczne jest definiowane jako świadczenie zdrowotne, o którym mowa w ustawie z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych.

W wyniku tej zmiany konieczne stało się dostosowanie do nowego brzmienia definicji zdarzenia medycznego, również zakresu danych, które usługodawcy mają obowiązek przekazywać do Systemu Informacji Medycznej.

Terminy przekazywania danych do SIM:

Usługodawcy muszą przekazać dane niezwłocznie, jednak nie później niż w terminie 2 dni od zakończenia zdarzenia medycznego z wyjątkiem szpitalnictwa.

Sposób przekazywania danych do SIM:

Usługodawcy przekazują dane do SIM w postaci elektronicznej. Dane są przekazywane do SIM w formie komunikatów elektronicznych zgodnie z wzorami dokumentów stanowiącymi opis komunikatów elektronicznych stosowanych do przekazywania danych określonymi przez jednostkę podległą ministrowi właściwemu do spraw zdrowia właściwą w zakresie systemów informacyjnych ochrony zdrowia i zamieszczonymi w Biuletynie Informacji Publicznej ministra właściwego do spraw zdrowia.

5.2 Zakres danych zdarzenia medycznego przetwarzanego w systemie informacji

Określa to Rozporządzenie Ministra Zdrowia z dnia 26 czerwca 2020 r. w sprawie szczegółowego zakresu danych zdarzenia medycznego przetwarzanego w systemie informacji oraz sposobu i terminów przekazywania tych danych do Systemu Informacji Medycznej (Dz.U. z 2020 r. poz. 1253). Rozporządzenie opisuje szczegółowy zakres danych zdarzenia medycznego przetwarzanego w systemie informacji w ochronie zdrowia, o którym mowa w art. 1 ust. 1 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia.

Obejmują one następujące dane:

- 1) dane usługodawcy,
- 2) dane usługobiorcy,
- 3) dane identyfikujące świadczenie zdrowotne,

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 4) dane miejsca udzielenia świadczenia zdrowotnego,
- 5) dane pracownika medycznego udzielającego świadczenia zdrowotnego lub odpowiedzialnego za jego udzielenie, a w przypadku wykonania operacji lub zabiegu w oddziale szpitalnym – dane pracownika medycznego kierującego wykonaniem tej operacji albo zabiegu (operatora),
- 6) dane dotyczące dokumentacji medycznej prowadzonej w postaci elektronicznej zgodnie ze standardem HL7 oraz – w odniesieniu do dokumentacji obrazowej – w formacie DICOM, wytworzonej w związku z udzielonym świadczeniem zdrowotnym,
- 7) inne dane pozwalające na identyfikację zdarzenia medycznego.

5.3 Dane usługodawcy

Pierwsza grupa informacji zamieszczanych w SIM obejmuje dane dotyczące usługodawcy. Podmioty lecznicze raportują do SIM część I kodu resortowego z systemu resortowych kodów identyfikacyjnych oraz 14-znakowy numer REGON zakładu leczniczego, w którym udzielono świadczenia zdrowotnego. Dostarczą one informacji o tym, w jakim podmiocie leczniczym, oraz w którym z jego zakładów leczniczych zaistniało dane zdarzenie medyczne.

Podmioty działające na podstawie wpisu do rejestru prowadzonego przez okręgową radę lekarską, okręgową radę pielęgniarek i położnych albo Krajową Radę Fizjoterapeutów mają obowiązek przekazywania do SIM informacji o identyfikatorze usługodawcy składającym się z numeru wpisu tego podmiotu do rejestru podmiotów wykonujących działalność leczniczą oraz z kodu właściwego organu.

5.4 Dane usługobiorcy

Drugą kategorię informacji zamieszczanych w SIM stanowią dane dotyczące usługobiorcy (pacjenta). Podstawową daną identyfikującą usługobiorcę jest numer PESEL. W sytuacji gdy komuś nie nadano tego numeru – jest to seria i numer paszportu albo innego dokumentu stwierdzającego tożsamość, bądź niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej do celów transgranicznej identyfikacji.

Przewidziano też rozwiązania znajdujące zastosowanie do osób nielegitymujących się żadnym z tych dokumentów. Jeśli pacjentowi nie nadano numeru PESEL, placówka będzie mogła przekazać również datę urodzenia i płeć usługobiorcy.

Ponadto usługodawca będzie zamieszczał w SIM imię (imiona) i nazwisko usługobiorcy, numer telefonu kontaktowego oraz adres poczty elektronicznej, a w przypadku gdy usługobiorca jest osobą małoletnią, całkowicie ubezwłasnowolnioną lub niezdolną do świadomego wyrażenia zgody – numer telefonu kontaktowego oraz adres poczty elektronicznej przedstawiciela ustawowego usługobiorcy albo jego opiekuna faktycznego.

5.5 Dane dotyczące świadczenia zdrowotnego

Trzecia grupa informacji przekazywanych do SIM obejmuje dane identyfikujące świadczenie zdrowotne. Placówka będzie musiała raportować ogólne dane charakteryzujące od strony medycznej udzielone świadczenie zdrowotne. Dane te obejmują:

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 1) kod świadczenia, który stanowi kod jednostki statystycznej określonej zgodnie z załącznikiem nr 1 do rozporządzenia,
- 2) datę rozpoczęcia udzielania świadczenia zdrowotnego,
- 3) datę zakończenia udzielania świadczenia zdrowotnego,
- 4) datę i godzinę rozpoczęcia oraz zakończenia przebywania usługobiorcy na przepustce, w przypadku gdy jednostką statystyczną, o której mowa w załączniku nr 1 do Rozporządzenia w sprawie zakresu niezbędnych informacji, jest pobyt w oddziale szpitalnym lub pobyt,
- 5) kod przyczyny głównej według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta,
- 6) kod przyczyny głównej hospitalizacji, o ile dane te dotyczą przedmiotowego zdarzenia medycznego,
- 7) kody przyczyn współistniejących według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta (istotna jest kolejność ich raportowania do SIM, ponieważ pierwsze trzy z nich będą udostępnione NFZ w celu rozliczania świadczeń opieki zdrowotnej),
- 8) kody przyczyn współistniejących istotnych w przypadku hospitalizacji według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta (podobnie jak wyżej ich kolejność jest ważna, ponieważ pierwsze pięć z nich zostanie udostępnionych NFZ w celu rozliczania świadczeń opieki zdrowotnej) oraz kody zrealizowanych istotnych procedur medycznych.
- 9) identyfikator skierowania na podstawie którego nastąpiło dane zdarzenie medyczne.

Celem raportowania tych danych jest zamieszczenie w SIM syntetycznego opisu udzielonego świadczenia zdrowotnego, aby stanowił on wartościową, a zarazem zwięzłą informację dla innych pracowników medycznych, którzy będą zapoznawali się z tymi danymi np. w ramach zapewniania ciągłości udzielania świadczeń zdrowotnych usługobiorcy.

5.6 Dane miejsca udzielenia świadczenia zdrowotnego

Czwarta grupa informacji przekazywanych do SIM obejmuje dane miejsca udzielenia świadczenia zdrowotnego, które obejmują:

- 1) identyfikator miejsca udzielania świadczenia opieki zdrowotnej,
- 2) niepowtarzalny kod identyfikujący jednostkę organizacyjną zakładu leczniczego w strukturze organizacyjnej podmiotu leczniczego stanowiący część V systemu resortowych kodów identyfikacyjnych, o którym mowa w przepisach wydanych na podstawie art. 105 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej – w przypadku podmiotu leczniczego, w którego strukturze organizacyjnej wyodrębniono jednostki organizacyjne,
- 3) niepowtarzalny kod identyfikujący komórkę organizacyjną zakładu leczniczego podmiotu leczniczego w strukturze organizacyjnej podmiotu leczniczego stanowiący część VII systemu resortowych kodów identyfikacyjnych, o którym mowa w przepisach wydanych na podstawie art. 105 ust. 5 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej – w przypadku

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

podmiotu leczniczego, w którego strukturze organizacyjnej wyodrębniono komórki organizacyjne.

5.7 Dane pracownika medycznego udzielającego świadczenia zdrowotnego

Kolejną grupę danych stanowią dane pracownika medycznego udzielającego świadczenia zdrowotnego lub odpowiedzialnego za jego udzielenie, a w przypadku wykonania operacji lub zabiegu w oddziale szpitalnym – dane pracownika medycznego kierującego wykonaniem tej operacji albo zabiegu (operatora), które obejmują:

- 1) identyfikator pracownika medycznego, o którym mowa w art. 17c ust. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia,
- 2) serię i numer paszportu albo innego dokumentu stwierdzającego tożsamość albo niepowtarzalny identyfikator nadany przez państwo członkowskie Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 1, z późn. zm.3)) – w przypadku pracownika medycznego, który nie posiada identyfikatora pracownika medycznego, o którym mowa w art. 17c ust. 5 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia,
- 3) imię (imiona) i nazwisko,
- 4) kod przynależności do danej grupy zawodowej określony zgodnie z tabelą nr 1 załącznika nr 3 do rozporządzenia w sprawie zakresu niezbędnych informacji.

5.8 Dane dotyczące dokumentacji medycznej

Kolejną grupę danych stanowią dane dotyczące dokumentacji medycznej prowadzonej w postaci elektronicznej zgodnie ze standardem HL7 oraz – w odniesieniu do dokumentacji obrazowej – w formacie DICOM, wytworzonej w związku z udzielonym świadczeniem zdrowotnym, które obejmują:

- 1) identyfikator nadawany przez system usługodawcy,
- 2) rodzaj,
- 3) datę wytworzenia,
- 4) tryb udostępniania,
- 5) adres repozytorium, w którym jest przechowywana dokumentacja medyczna.

5.9 Inne dane pozwalające na identyfikację zdarzenia medycznego

Inne dane pozwalające na identyfikację zdarzenia medycznego obejmują:

- 1) identyfikator zdarzenia medycznego nadawany przez system usługodawcy,
- 2) dane dotyczące płatnika:

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- informację o rodzaju płatnika w rozumieniu art. 2 pkt 9 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia,
 - identyfikator podmiotu zobowiązanego do finansowania świadczeń zdrowotnych ze środków publicznych,
- 3) osobisty numer identyfikacyjny w przypadku usługobiorcy uprawnionego do świadczeń opieki zdrowotnej na podstawie przepisów o koordynacji,
 - 4) informacje charakteryzujące uprawnienie do świadczeń opieki zdrowotnej:
 - kod tytułu uprawnienia do świadczeń opieki zdrowotnej finansowanych ze środków publicznych,
 - dane identyfikujące dokument,
 - 5) identyfikator umowy zawartej między Narodowym Funduszem Zdrowia a usługodawcą, zwanej dalej „umową”,
 - 6) kod gminy krajowego rejestru urzędowego podziału terytorialnego kraju miejsca zamieszkania usługobiorcy,
 - 7) unikalny numer identyfikacyjny karty onkologicznej – w przypadku gdy świadczenie zdrowotne zostało udzielone w związku z wydaniem karty onkologicznej lub na podstawie karty onkologicznej,
 - 8) informację o masie ciała i wzroście usługobiorcy,
 - 9) informację dotyczącą używania przez usługobiorcę, który ukończył 15 rok życia, wyrobów tytoniowych.

W przypadku gdy jednostką statystyczną jest pobyt w oddziale szpitalnym, wszystkie pobyty usługobiorcy, któremu udzielono świadczenia zdrowotnego, pomiędzy wpisem do wykazu głównego przyjęć i wypisów a wypisem z niego, stanowią jedną hospitalizację. W tym przypadku dane charakteryzujące poszczególne pobyty w oddziale usługodawca grupuje i przyporządkowuje do komórki organizacyjnej lub jednostki organizacyjnej, w której udzielono usługobiorcy świadczenia zdrowotnego, jeżeli w strukturze organizacyjnej podmiotu leczniczego nie wyodrębniono komórek organizacyjnych, oraz usługodawca przekazuje dodatkowo do SIM:

- 1) datę przyjęcia usługobiorcy na oddział szpitalny,
- 2) kod trybu przyjęcia usługobiorcy do szpitala w rozumieniu art. 2 ust. 1 pkt 9 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej określony zgodnie z załącznikiem nr 4 do rozporządzenia w sprawie zakresu niezbędnych informacji,
- 3) datę wypisu usługobiorcy z oddziału szpitalnego,
- 4) kod trybu wypisu usługobiorcy ze szpitala w rozumieniu art. 2 ust. 1 pkt 9 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej określony zgodnie z załącznikiem nr 4 do rozporządzenia w sprawie zakresu niezbędnych informacji,
- 5) kod przyczyny głównej hospitalizacji według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja Dziesiąta zgodny z chorobą zasadniczą wpisaną do historii choroby, w części dotyczącej wypisu pacjenta ze szpitala, prowadzonej zgodnie z przepisami w sprawie rodzajów i zakresu dokumentacji medycznej w podmiotach leczniczych oraz sposobu jej przetwarzania,
- 6) kody przyczyn współistniejących istotnych w przypadku tej hospitalizacji według Międzynarodowej Statystycznej Klasyfikacji Chorób i Problemów Zdrowotnych Rewizja



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Dziesiąta – w przypadku świadczeń zdrowotnych finansowanych ze środków publicznych pierwszych pięć kodów przekazanych przez usługodawcę do SIM udostępnia się Narodowemu Funduszowi Zdrowia w celu rozliczania świadczeń opieki zdrowotnej.

5.10 Wymiana informacji o zdarzeniach medycznych

Rozwiązanie zakłada użycie FHIR R4, standardu modelu danych w dziedzinie służby zdrowia i ich wymiany w wersji 4.0.0, opublikowanego przez HL7®.

Rozwiązanie FHIR udostępnia zestaw komponentów modułowych nazwanych „Zasobami”. Z założenia zasoby te można łatwo połączyć w działające systemy, do rozwiązywania różnorodnych problemów klinicznych i administracyjnych ograniczając koszty budowy i dostosowania systemów.

FHIR nadaje się do użytku w wielu różnych kontekstach - aplikacje mobilne, komunikacja w chmurze, współdzielenie zasobów informacyjnych, komunikacja serwerowa pomiędzy podmiotami realizującymi usługi opieki zdrowotnej i wiele innych.

Rozwiązanie FHIR, oprócz istniejących zasobów definiuje proste ramy ich rozszerzania i opisywania ich wykorzystania w profilach, co czyni rozwiązanie mocno elastycznym i prostym w adaptacji w kontekście dużej zmienności potrzeb powodowanej różnorodnymi procesami realizowanymi w ramach usług ochrony zdrowia.

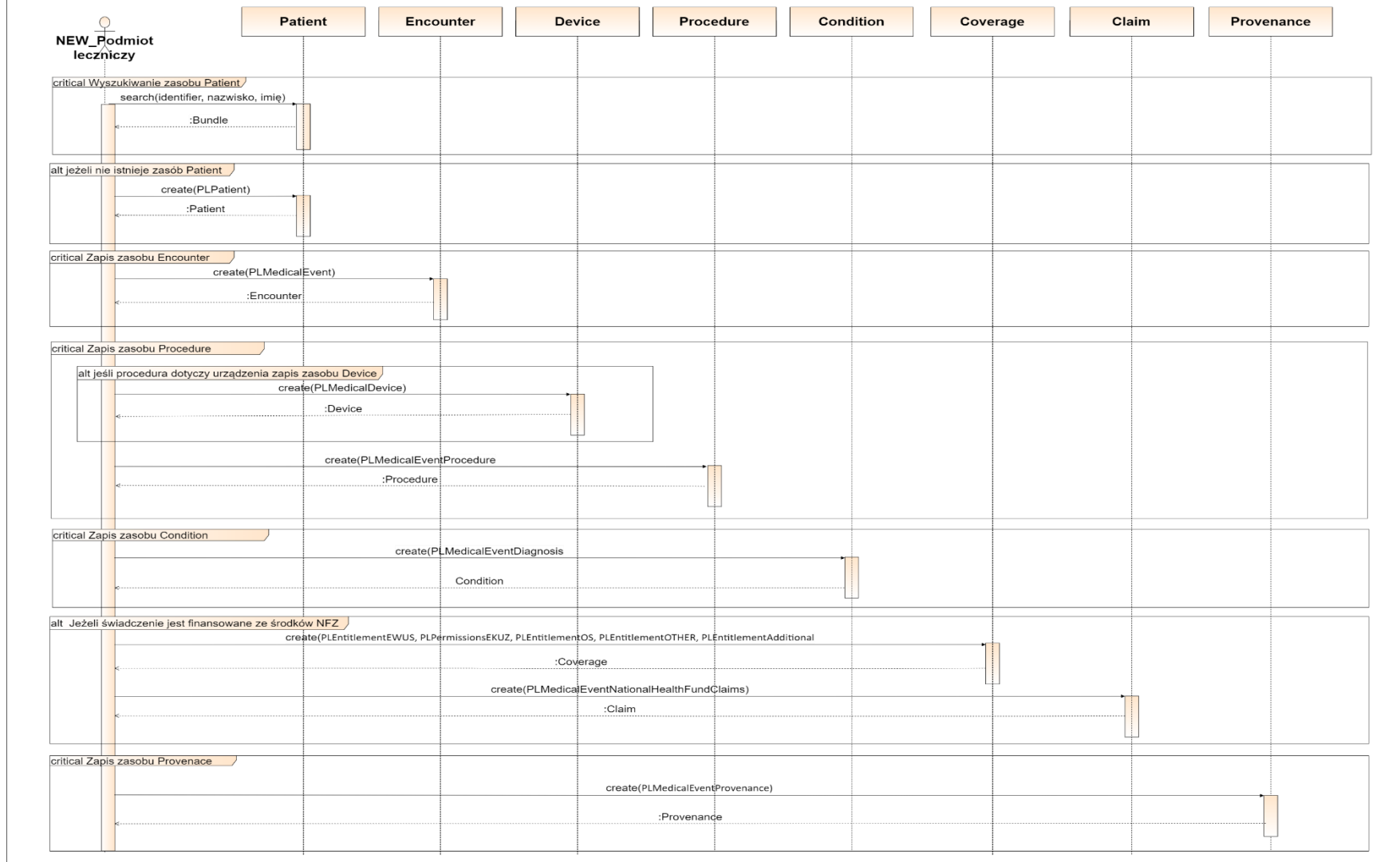
Zasób FHIR może być automatycznie interpretowany przez system, przy czym zawiera również czytelną reprezentację danych zwiększając tym samym bezpieczeństwo w kontekście poprawnej interpretacji danych i zwiększając bezpieczeństwo świadczonych usług medycznych.

Rozwiązanie FHIR zostało wybrane dla obsługi Zdarzeń Medycznych jako alternatywa dla niestandardowych rozwiązań. Daje to warunki dla szybkiego wdrożenia i przyszłych zmian w kontekście wymaganej ustawowo obsługi Zdarzeń Medycznych.

Informacje na temat standardu FHIR znajdują się na stronie <https://www.hl7.org/fhir/>.



ad. Rejestracja Zdarzenia Medycznego



Rys. 2. Diagram rejestracja Zdarzenia Medycznego (źródło: opracowanie własne)



Fundusze Europejskie
Program Regionalny

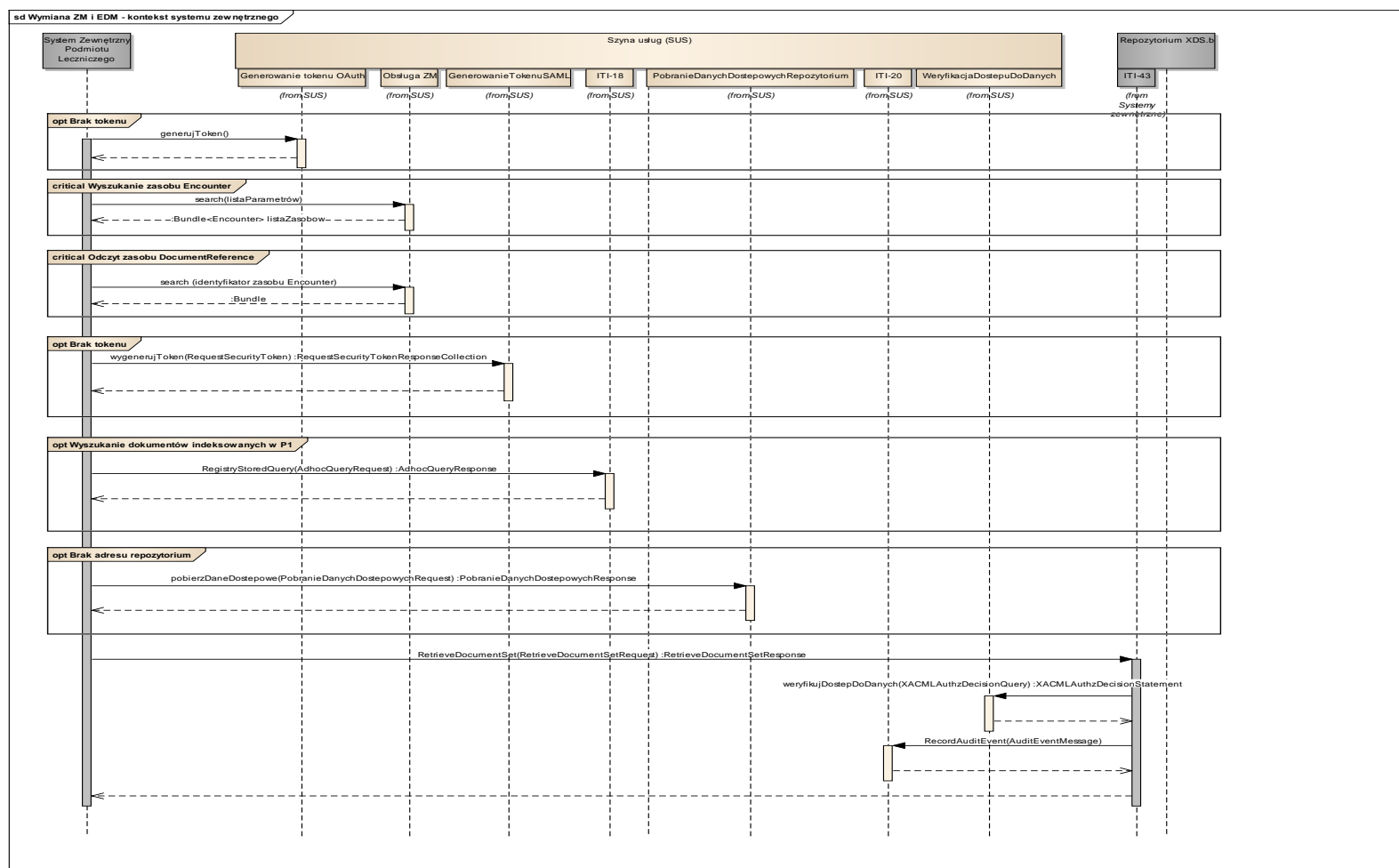


Rzeczpospolita
Polska



Pomorze
Zachodnie

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Rys. 3. Diagram Wymiana Zdarzenia Medycznego i Elektronicznej Dokumentacji Medycznej (źródło: Centrum e-Zdrowia)

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Komunikacja z podsystemem obsługującym EDM:

- 1) System podmiotu A łączy się z systemem P1 w celu uzyskania tokenu SAML. Podczas połączenia system uwierzytelnia się certyfikatem wystawionym przez P1.
- 2) System P1 zwraca token SAML (będzie on wykorzystywany do komunikacji z P1, jak i z repozytorium w którym jest przechowywana dokumentacja elektroniczna)
- 3) System podmiotu A łączy się z systemem P1 z podsystemem realizującym funkcjonalność Rejestru XDS dla Krajowej domeny XDS.b i wyszukuje indeks 8 EDM na podstawie identyfikatora dokumentu ustalonego w pkt.4. System podmiotu A przekazuje pozyskany token SAML.
- 4) System podmiotu A odczytuje z indeksu EDM identyfikator repozytorium, w którym przechowywana jest elektroniczna dokumentacja medyczna dotycząca danego indeksu.
- 5) System podmiotu A łączy się systemem P1 z podsystemem SZAR i pobiera dane dostępne repozytorium, którego identyfikator otrzymano w pkt 8.
- 6) System P1 zwraca dane dostępne (m.in. adres URL repozytorium).
- 7) System podmiotu A łączy się z repozytorium, przekazuje token SAML otrzymany z systemu P1 oraz przekazuje identyfikator dokumentu, który chce pobrać. Połączenie jest zabezpieczone z użyciem TLS, a w trakcie jego zestawiania musi nastąpić dwustronne uwierzytelnienie (zarówno system podmiotu A jak i repozytorium z którym się połączył powinny akceptować certyfikaty wystawione przez P1).
- 8) Repozytorium sprawdza certyfikat wykorzystany do uwierzytelniania (sprawdza wystawcę, okres ważności, czy dotyczy systemu podmiotu A. Następnie weryfikuje token SAML przekazany przez system podmiotu A (integralność, ważność, wystawcę - system P1). Łączy się z systemem P1, aby sprawdzić, czy system podmiotu A ma dostęp do dokumentu, którego żąda.
- 9) System P1 na podstawie polityk globalnych i zarejestrowanych deklaracji zgód określa, czy system podmiotu A ma dostęp do dokumentu i przekazuje decyzję do repozytorium.
- 10) Repozytorium udostępnia dokument do systemu podmiotu A oraz przekazuje do systemu P1 informację do odłożenia w logu ATNA dotyczącą udostępnienia dokumentu.

⁸ System podmiotu może jednocześnie wyszukać wiele indeksów, ale dla uproszczenia w opisie przedstawiono scenariusz dot. pojedynczego indeksu EDM.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



6. Architektura funkcjonalna Systemu ZeZ

Rozdział zawiera omówienie architektury rozwiązań dla Projektu „Zachodniopomorskie e-Zdrowie”.

6.1 Kluczowe założenia i pryncypia

Dla e-usług i kluczowych funkcjonalności dla Projektu ZeZ założono i przyjęto udział obecnych i planowanych rozwiązań zarówno na poziomie centralnym, warstwy regionalnej na poziomie Województwa Zachodniopomorskiego oraz warstwy lokalnej na poziomie Partnerów Projektu / podmiotów leczniczych:

- 1) Poziom centralny, w tym w szczególności P1 w zakresie:
 - a) Internetowe Konto Pacjenta (IKP),
 - b) rejestr Elektroniczna Dokumentacja Medyczna (EDM) w obecnym i dalszych rozszerzeniach zakresu stosowania dla kolejnych dokumentów medycznych (od 25 kwietnia 2020 r. EDM stanowią również opisy badań diagnostycznych innych niż laboratoryjne, a od 25 kwietnia 2021 r. są to także wyniki badań laboratoryjnych wraz z opisem),
 - c) zdarzenia medyczne,
 - d) zgody Pacjenta,
 - e) System Elektronicznej Rejestracji,
 - f) kolejne e-usługi planowane do uruchomienia w przyszłości, recepta transgraniczna
 - g) uwierzytelnianie z wykorzystaniem Węzła Krajowego Identyfikacji Elektronicznej poprzez: Profil zaufany (PZ), e-dowód oraz mojeID - przy pomocy banku lub innego dostawcy tożsamości.

Poziom centralny udostępnia zasoby do świadczenia usług dla pacjentów w ramach ZeZ.

- 2) Warstwa regionalna w zakresie:

Platforma regionalna o następującym zakresie funkcjonalnym:

- a) Regionalne Repozytorium EDM,
- b) Portal Projektu ZeZ,
- c) Systemy analityczne:
 1. System Analiz Zarządczych
 2. System Analiz Sprawozdawczych
 3. Platforma zakupowa SPZOZ/Grupowe zamówienia

Warstwa regionalna wspiera i uczestniczy w świadczeniu usług oraz zapewnia udostępnianie EDM innym podmiotom leczniczym.

- 3) Warstwa lokalna na poziomie Partnerów Projektu – podmiotów leczniczych:

- a) integracja z krajowym Systemem Elektronicznej Rejestracji na Platformie P1,
- b) e-Rejestracja lokalna przez stronę www u wybranych Partnerów Projektu,
- c) lokalne repozytorium EDM,
- d) integracja z Regionalnym Repozytorium EDM,
- e) e-Dzienniczek dla wybranych Partnerów,
- f) przesyłanie indeksów EDM oraz danych o zdarzeniach medycznych do P1,

Fundusze Europejskie
Program RegionalnyRzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

g) integracja z P1 w zakresie odczytu i zapisu zgód pacjenta

Warstwa lokalna świadczy usługi dla pacjentów z zastosowaniem poziomu centralnego oraz warstwy regionalnej.

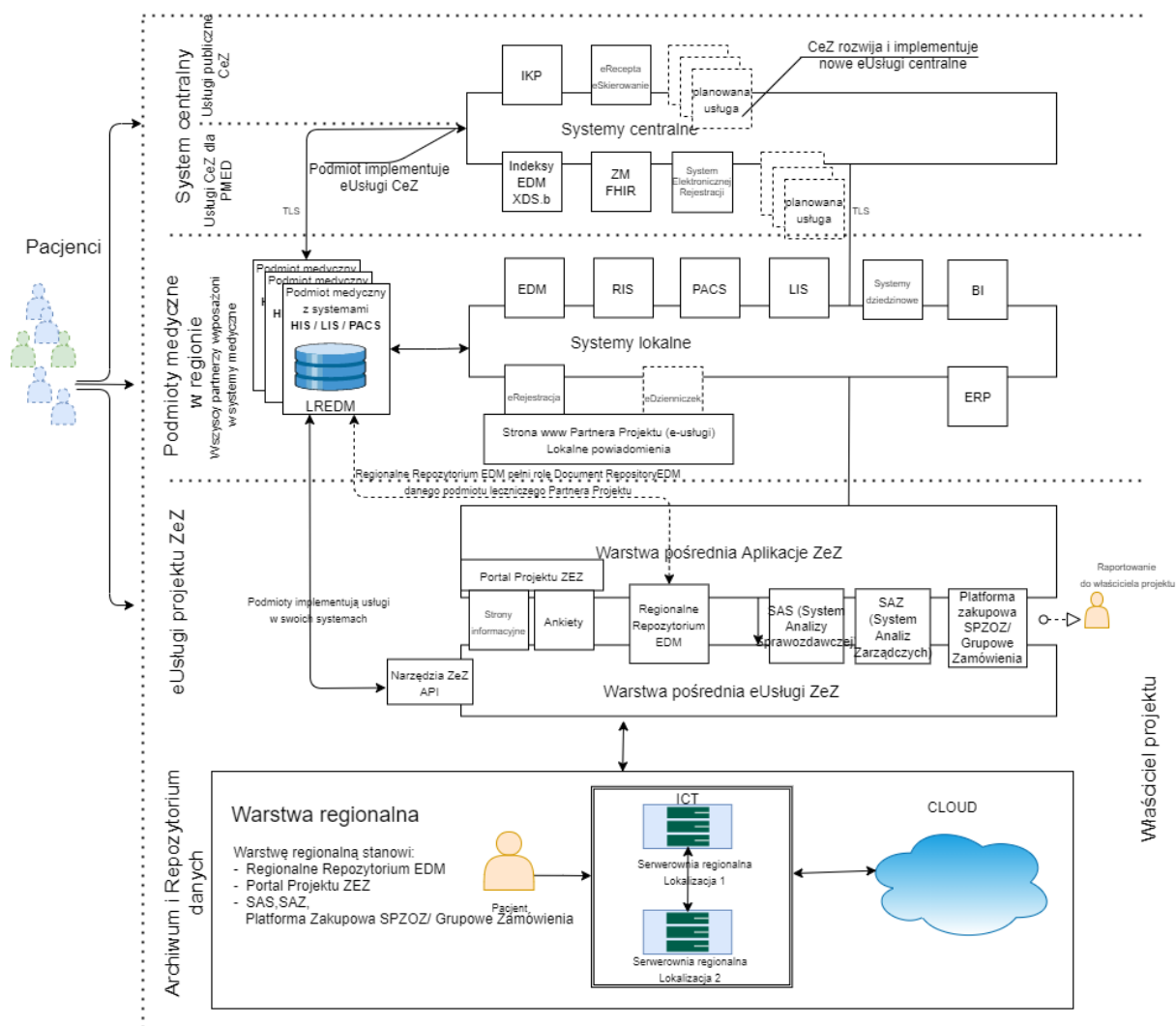
Rejestr oraz repozytorium EDM wskazane na poziomie centralnym i w warstwach regionalnej i lokalnej, rozumiane są następująco:

- źródłem danych dla dokumentacji EDM (Document Source) jest system części białej (HIS, LIS, RIS) w podmiocie leczniczym,
- dokumenty EDM są składowane i archiwizowane w repozytorium lokalnym podmiotu leczniczego;
- informacje opisujące dokumentację medyczną (metadane, indeksy) oraz wskazujące gdzie przechowywana jest właściwa dokumentacja zawarte są w Rejestrze EDM w P1 w ramach Krajowej Domeny (IHE XDS.b),
- informacje do Rejestru EDM są przekazywane bezpośrednio przez podmiot leczniczy,
- Regionalne Repozytorium EDM jest zasilane dokumentami EDM z lokalnych repozytoriów EDM Partnerów Projektu ZeZ;
- Regionalne Repozytorium pełni rolę Document Repository EDM danego podmiotu leczniczego Partnera Projektu;
- kierowanie zapytań o dokumentację EDM z wykorzystaniem rejestru EDM w P1 od innych świadczeniodawców odbywa się do Regionalnego Repozytorium EDM,
- udostępnianie EDM dla zewnętrznych użytkowników (pacjentów i pracowników medycznych) odbywa się przez Regionalne Repozytorium EDM wykorzystując Internetowe Konto Pacjenta w systemie P1 (dla pacjentów) lub poprzez systemy dziedziczne, w tym HIS (dla pracowników medycznych). Stosowne opisy zastosowań znajdują się w poniższych rozdziałach.

Uwagi:

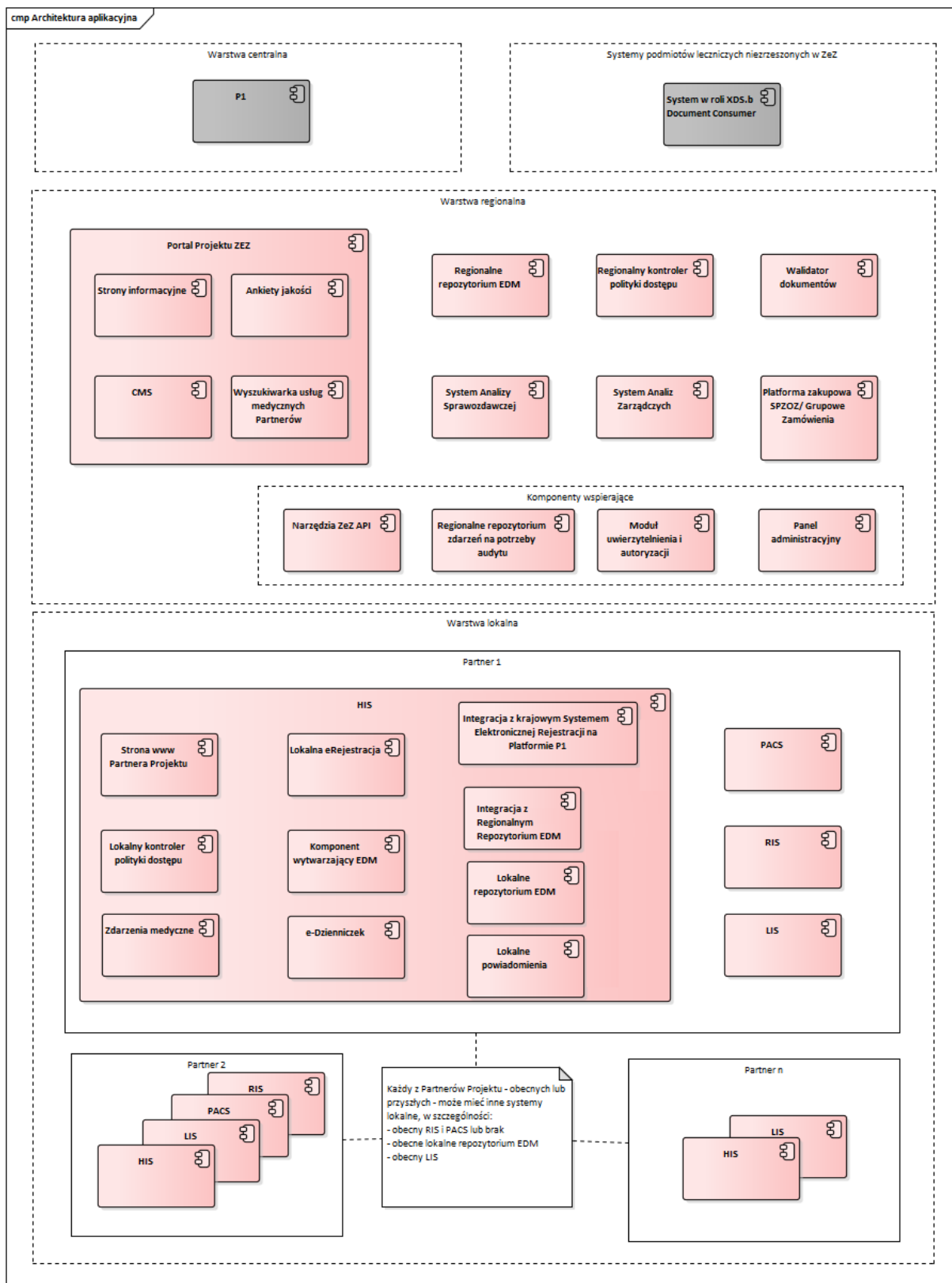
- warstwa regionalna nie prowadzi rejestru (indeksów) EDM. Indeksowanie EDM w P1 prowadzone jest przez Partnera Projektu ZeZ;
- Indeks Pacjenta nie jest wymagany na poziomie regionalnym;
- raportowanie/przekazywanie informacji o Zdarzeniach Medycznych będzie realizowane przez podmiot leczniczy lokalnie ze wskazaniem Regionalnego Repozytorium jako Document Repository EDM;
- wdrożenie Regionalnego Repozytorium EDM jako repozytorium uczestniczącego w wymianie i udostępnianiu dokumentacji EDM nie wyklucza możliwości przetłoczenia i wskazania jako Document Repository w rejestrze EDM P1 Repozytorium Lokalnego Partnera Projektu. Zapewnia redundantność zapisu danych EDM oraz jedno miejsce w Systemie udostępniania danych;
- Partnerzy Projektu wdrażają e-Rejestrację lokalną, do której dostęp zapewniony będzie poprzez stronę www danego Partnera Projektu;
- Partnerzy Projektu wdrażają e-Rejestrację lokalną z uwzględnieniem planowanego Systemu Elektronicznej Rejestracji (e-Rejestracji centralnej) świadczeń wskazanych przez Ministerstwo Zdrowia;

- systemy oprogramowania danego podmiotu zostaną zintegrowane z Systemem Elektronicznej Rejestracji na Platformie P1.



Rys. 4. Model pogładowy architektury systemu

6.2 Model architektury aplikacyjnej



Rys. 5. Architektura aplikacyjna ZeZ



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



6.3 Portal Projektu ZeZ

W ramach Portalu występować będą obszary funkcjonalne, pogrupowane tematycznie jak poniżej:

I. Strefa dla pacjenta:

- 1) Aktualności (tzw. news room) – bieżące informacje z zakresu funkcjonowania systemu ochrony zdrowia w regionie z możliwością bezpośredniego dodawania aktualności przez podmioty lecznicze, po wstępnej weryfikacji treści przez administratora,
- 2) Badanie jakości poprzez ankiety i wnioski – aktywne formularze umożliwiające pacjentom przekazywanie uwag i wniosków odnoszących się do funkcjonowania podmiotów leczniczych, udzielanych przez nie świadczeń oraz prowadzenie regularnych badań ankietowych związanych z badaniami poziomu satysfakcji pacjentów,
- 3) Świadczenia zdrowotne podmiotów leczniczych (wydzielona przestrzeń dla każdego Partnera Projektu). Powinna zawierać informacje bieżące z poszczególnych podmiotów leczniczych oraz informacje o zakresie funkcjonowania, oddziałach, poradniach, miejscach udzielania świadczeń oraz przekierowania (link) do modułu e-Rejestracja danego podmiotu leczniczego,
- 4) Użyteczne adresy www: inne podmioty lecznicze w regionie nie będące Partnerem Projektu, apteki, dostęp do IKP, PUE ZUS i inne,
- 5) Informacje o Projekcie „Zachodniopomorskie e-Zdrowie”: założenia, cele, korzyści dla pacjentów, kalendarium prac, serwis fotograficzny itp.

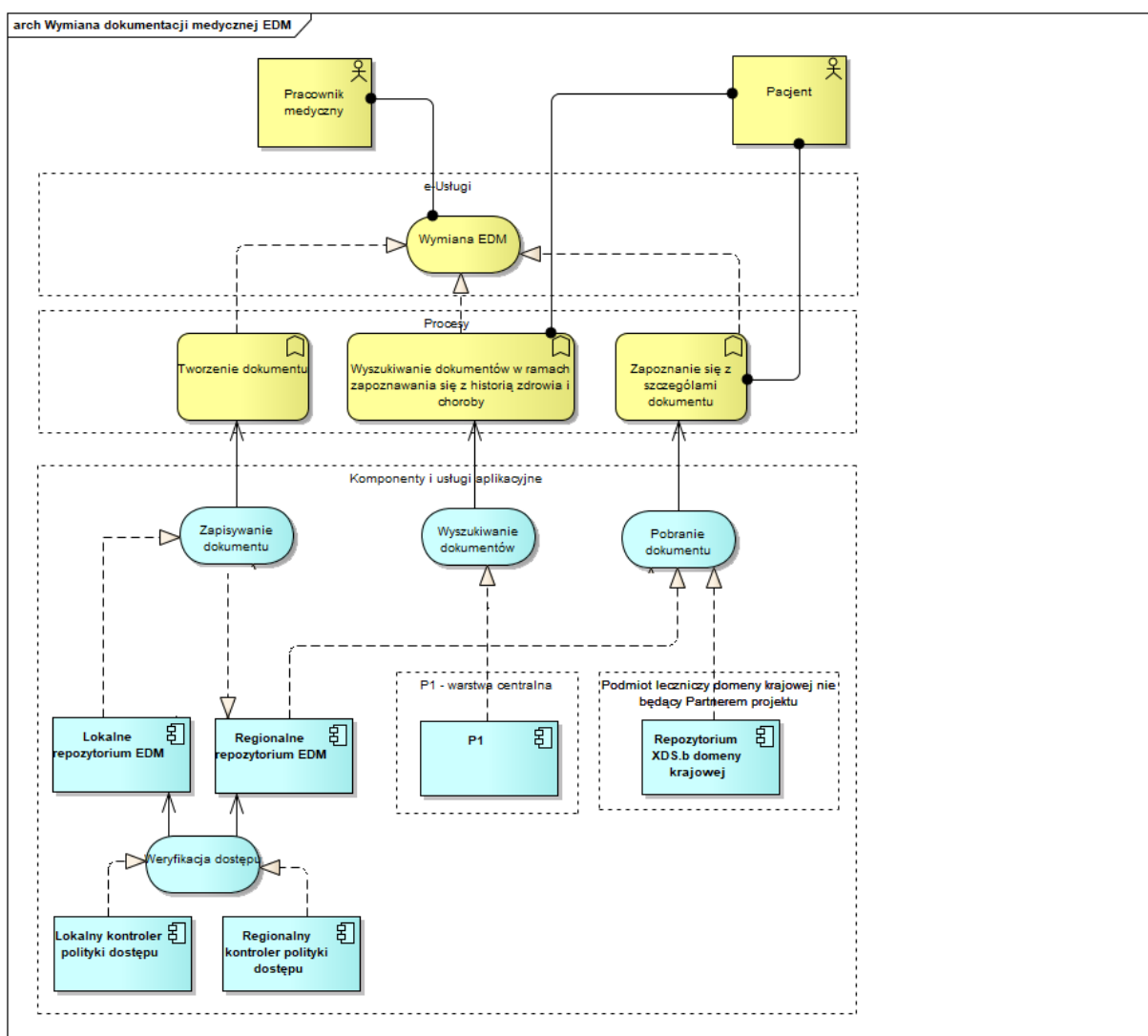
II. Strefa dla Partnera Projektu:

- 1) Platforma Zakupowa SPZOZ,
- 2) Informacje, zestawienia analityczne publikowane przez organ tworzący (Urząd Marszałkowski) z zakresu świadczonych usług: wyniki, benchmarki itp.,
- 3) Wyniki z badania jakości.

Redagowanie i formatowanie treści opisanych w pkt I.1, 2, 4, 5 oraz II.2 będzie możliwe za pośrednictwem modułu CMS (ang. content management system), bez konieczności edycji źródeł strony w HTML ani w innych językach.

6.4 Wymiana dokumentacji medycznej EDM

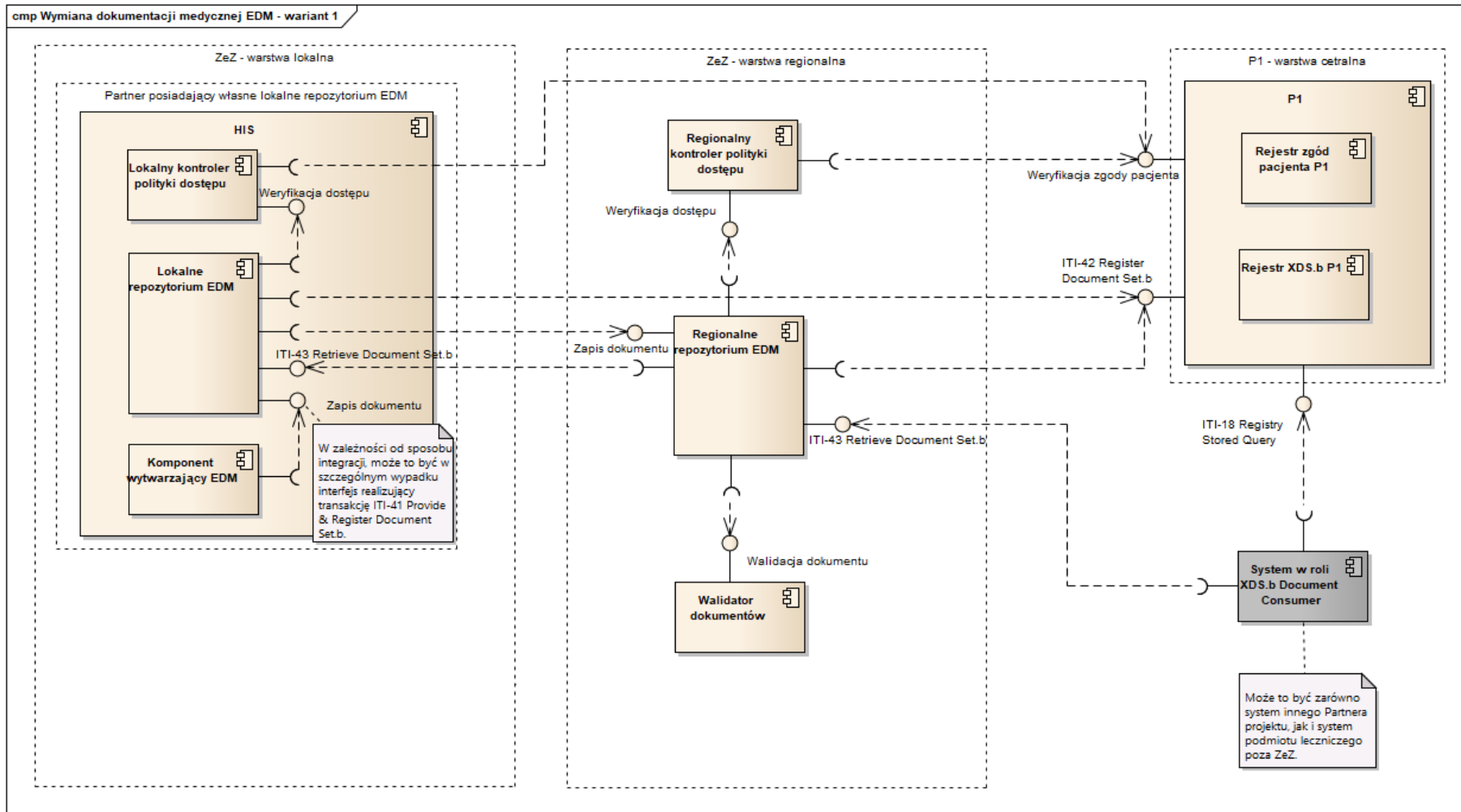
W rozdziale zawarte są informacje na temat przyjętego do realizacji - zgodnie z rekomendacją - modelu wymiany elektronicznej dokumentacji medycznej EDM.



Rys. 6. Realizacja e-Usługi Wymiana EDM

6.5 Architektura aplikacyjna obszaru wymiany dokumentacji medycznej EDM

Poniższy diagram obrazuje komponenty aplikacyjne zaangażowane w realizację obszaru wraz z wykorzystywanymi w tym celu operacjami.



Rys. 7. Architektura aplikacyjna obszaru wymiany dokumentacji medycznej EDM

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

6.6 Domenowość

Partnerzy Projektu wytwarzający dokumentację EDM podlegającą indeksowaniu w Systemie P1 będą należeć jedynie do Krajowej Domeny XDS. Nie zakłada się wdrożenia domeny regionalnej XDS.b.

6.7 Rejestr indeksów (metadanych) EDM

Rejestr Elektroniczna Dokumentacja Medyczna (EDM) w obecnym i dalszych rozszerzeniach zakresu stosowania dla kolejnych dokumentów medycznych zawiera indeksy (metadane) dokumentów EDM.

Dokumenty EDM tworzone przez Partnerów Projektu będą podlegały indeksowaniu w Systemie P1 dla umożliwienia ich dalszego udostępniania.

Indeksowaniu podlegają wszystkie elektroniczne dokumenty medyczne o ile zostały wytworzone w zgodności z HL7 CDA.

6.8 Dostęp do dokumentów i elektroniczne zgody pacjenta

Przyjęte rozwiązanie dostępu do informacji o stanie zdrowia, dokumentów medycznych, na świadczenie medyczne oraz udzielania zgód dla pracownika medycznego lub podmiotu leczniczego spełnia wymóg pełnej implementacji wytycznych CeZ.

Wymiana informacji medycznej w ZeZ bazuje na trybie dostępu do dokumentów zadeklarowanym przez system lub komponent wnioskujący o dostęp, oraz na zgodzie pacjenta. Obsługiwane są następujące tryby dostępu:

- a) Dostęp dla autora dokumentu,
- b) Dostęp dla pacjenta, którego dokument dotyczy,
- c) Dostęp w ramach kontynuacji leczenia (w obrębie podmiotu, w którym wytworzono dokument),
- d) Dostęp w trybie ratowania życia,
- e) Dostęp za zgodą pacjenta – wymaga weryfikacji zgody w systemie P1.

Weryfikacja zgód w trybie e) może następować tylko i wyłącznie na poziomie Systemu P1. Pacjent ma możliwość nadawania zgód z poziomu IKP lub z wykorzystaniem autoryzacji SMS (Dokumentacja integracyjna systemu P1 w zakresie nadawania dostępu do danych medycznych pacjenta (autoryzacja)) w ramach preautoryzacji. Nie przewiduje się wdrożenia do użytkowania Regionalnego Rejestru Zgód.

Za realizację kontroli trybu dostępu są odpowiedzialne dedykowane komponenty:

- 1) Lokalny kontroler polityki dostępu – działający przy każdym Lokalnym repozytorium dokumentów EDM,
- 2) Regionalny kontroler polityki dostępu – działający przy Regionalnym repozytorium dokumentów EDM.

Uwaga:

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Systemy lokalne podmiotów leczniczych muszą zapewniać usługi odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia i odczytu zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1 (w tym autoryzacji przez SMS) oraz usługi zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne.

6.9 Lokalne Repozytoria EDM

Przyjęto założenie, że Partnerzy Projektu wdrażają, a następnie użytkują Lokalne Repozytoria EDM.

Lokalne Repozytorium EDM (LREDM) jest elementem architektury rozwiązania informatycznego zapewniającego obsługę informatyczną części medycznej podmiotu leczniczego w zakresie gromadzenia i udostępniania dokumentacji medycznej wytworzonej w postaci elektronicznej. LREDM odpowiada za gromadzenie i indeksowanie EDM w Domenie Krajowej XDS.b (zgodnej z HL7 CDA) zgodnie z prawem. Repozytorium gromadzi całą elektroniczną dokumentację pacjenta (EDM) wytwarzaną w podmiocie leczniczym, we wszystkich jej wytworzonych wersjach.

W repozytorium przechowywane mogą być wszystkie elektroniczne dokumenty medyczne, o ile zostały wytworzone w zgodności ze standardem HL7 CDA.

Lokalne repozytorium może uczestniczyć w wymianie i udostępnianiu dokumentów EDM, w zależności od przyjętego rozwiązania. Zasila regionalne repozytorium EDM danymi – dokumentami EDM Partnerów Projektu ZeZ.

6.10 Regionalne Repozytorium EDM

Regionalne Repozytorium EDM będzie pełniło funkcję Document Repository (jako repozytorium XDS dla domeny krajowej) przechowując dokumenty medyczne, które są zaindeksowane i przeznaczone do udostępniania na platformie P1. Zainteresowany podmiot leczniczy uczestniczący w Projekcie ZeZ (który będzie chciał przechowywać udostępniać EDM przez Regionalne Repozytorium) będzie dysponował swoją, niezależną przestrzenią w Regionalnym Repozytorium EDM. Repozytorium ma być technologicznie gotowe na przyłączenie innych podmiotów.

Kopia przechowywana w Repozytorium Regionalnym powinna mieć możliwość posłużenia do odtworzenia Lokalnego Repozytorium po awarii.

6.11 Wytwarzanie EDM w systemach Partnerów

Każdy z systemów HIS Partnerów musi być przystosowany do wytwarzania dokumentów EDM w postaci elektronicznej, zgodnych z Polską Implementacją Krajową (PIK) HL7 CDA, oraz ich podpisywania z użyciem prawnie dopuszczonych rodzajów podpisu. Sposób realizacji tej funkcjonalności może być różny w każdym z systemów HIS: może ona być zrealizowana dedykowanym komponentem systemu HIS, osobną aplikacją zintegrowaną z systemem, bądź stanowić integralną część tego systemu (np. systemy o architekturze monolitycznej). Dla uproszczenia, na diagramach architektury aplikacyjnej obszaru wymiany dokumentacji medycznej EDM systemu ZeZ przyjęto, że odbywa się to w przykładowym Komponentie wytwarzającym EDM stanowiącym komponent systemu HIS.

6.12 Systemy Analityczne

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Wdrożenie systemów analitycznych oraz wspomagających zarządzanie podmiotami leczniczymi uczestniczącymi w ZeZ:

- 1) System Analizy Sprawozdawczej SAS - system klasy Business Intelligence w zakresie: dostarczanie raportów, monitorowanie i analiza stanu wykorzystania usług i portalu przez użytkowników w zakresie:
 - poziomu realizacji wskaźników,
 - efektywności wykorzystywania e-usług,
 - zasobów medycznych i ich wykorzystania.
- 2) System Analiz Zarządczych SAZ – system klasy Business Intelligence w zakresie:
 - przetwarzania danych, rozproszonych w różnych systemach i aplikacjach, monitorowania wskaźników efektywności organizacyjnej i ekonomicznej,
 - raportowania wspomagającego zarządzanie w poszczególnych placówkach ochrony zdrowia Partnerów Projektu.
 - wspierania decyzji z zakresu kreowania polityki zdrowotnej regionu z poziomu organu właścicielskiego.
- 3) Platforma Zakupowa SPZOZ/Grupowe Zamówienia – zbieranie danych o potrzebach zakupowych od Partnerów w celu przeprowadzania zakupów wspólnych.

6.13 Zdarzenia medyczne

Każdy z systemów HIS Partnerów musi mieć komponent odpowiedzialny za zapewnienie wymiany informacji na potrzeby kontynuacji procesu leczenia. Podmioty lecznicze zobowiązane są przekazywać do P1 informacje o udzielonych pacjentom świadczeniach oraz wytworzonej elektronicznej dokumentacji medycznej (EDM).

Moduł systemu HIS znajduje się w warstwie lokalnej i odpowiada za komunikację z platformą P1. Usługodawcy przekazują dane do P1 w postaci elektronicznej. Dane są przekazywane do P1 w formie komunikatów elektronicznych zgodnie z wzorami dokumentów stanowiącymi opis komunikatów elektronicznych stosowanych do przekazywania danych określonymi przez CeZ.

Moduł komunikuje się z serwerem FHIR CSIOZ, który implementuje FHIR R4, jako standard modelu danych w dziedzinie ochrony zdrowia i ich wymiany w wersji 4.0.0, opublikowanego przez HL7®. Zasób FHIR może być automatycznie interpretowany przez moduł zdarzeń medycznych przy czym zawiera również czytelną reprezentację danych zwiększając tym samym bezpieczeństwo w kontekście poprawnej interpretacji danych i zwiększając bezpieczeństwo świadczonych usług medycznych.

Moduł musi być zgodny z najnowszą wersją dokumentacji integracyjnej oraz jej przyszłymi zmianami.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



6.14 e-Rejestracja

W odniesieniu do usługi e-Rejestracja w projekcie ZeZ powstaną dwa produkty:

- 1) moduł e-Rejestracja poprzez stronę www wybranego Partnera Projektu – odrębny/osobny/niezależny kanał dostępu do rejestracji przez stronę www Partnera Projektu (według zgłoszonej potrzeby poszczególnych PP).
- 2) integracja modułów rejestracji w systemach HIS z krajowym Systemem Elektronicznej Rejestracji w P1 – pozwoli na rejestrację poprzez IKP.

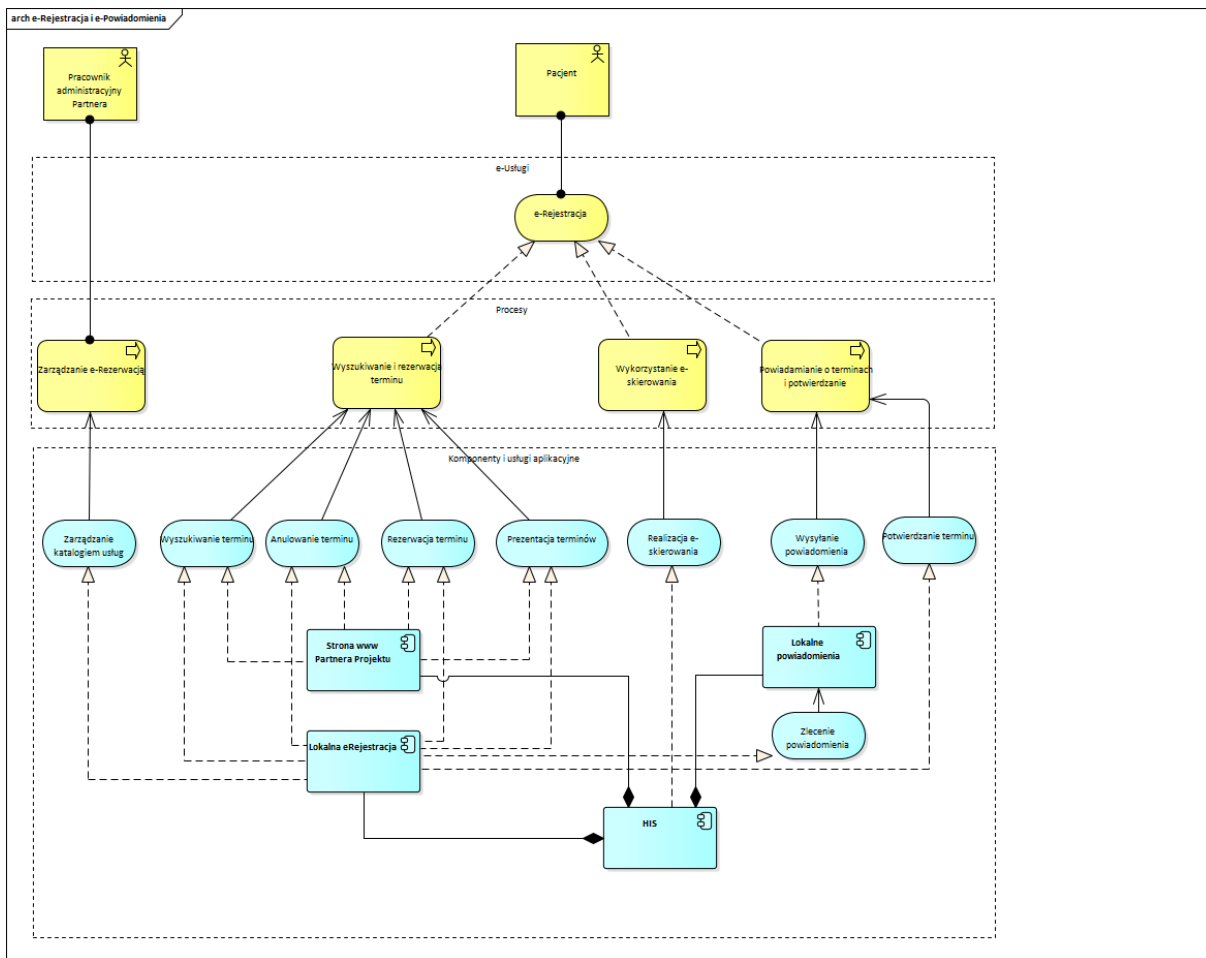
Moduł e-Rejestracja należy do warstwy lokalnej i jest komponentem systemu HIS lub innego systemu gabinetowego Partnera odpowiedzialnym za zadania związane z:

- 3) utrzymywaniem katalogu usług świadczonych przez podmioty lecznicze i jednostki organizacyjne Partnera,
- 4) wyszukiwaniem wolnych terminów, zakładaniem rezerwacji, potwierdzaniem, modyfikacją i anulowaniem rezerwacji,
- 5) definiowaniem protokołów przygotowania do wizyty,
- 6) przekazywanie zdarzeń do komponentu Lokalne powiadomienia celem wysyłki powiadomień do pacjentów.

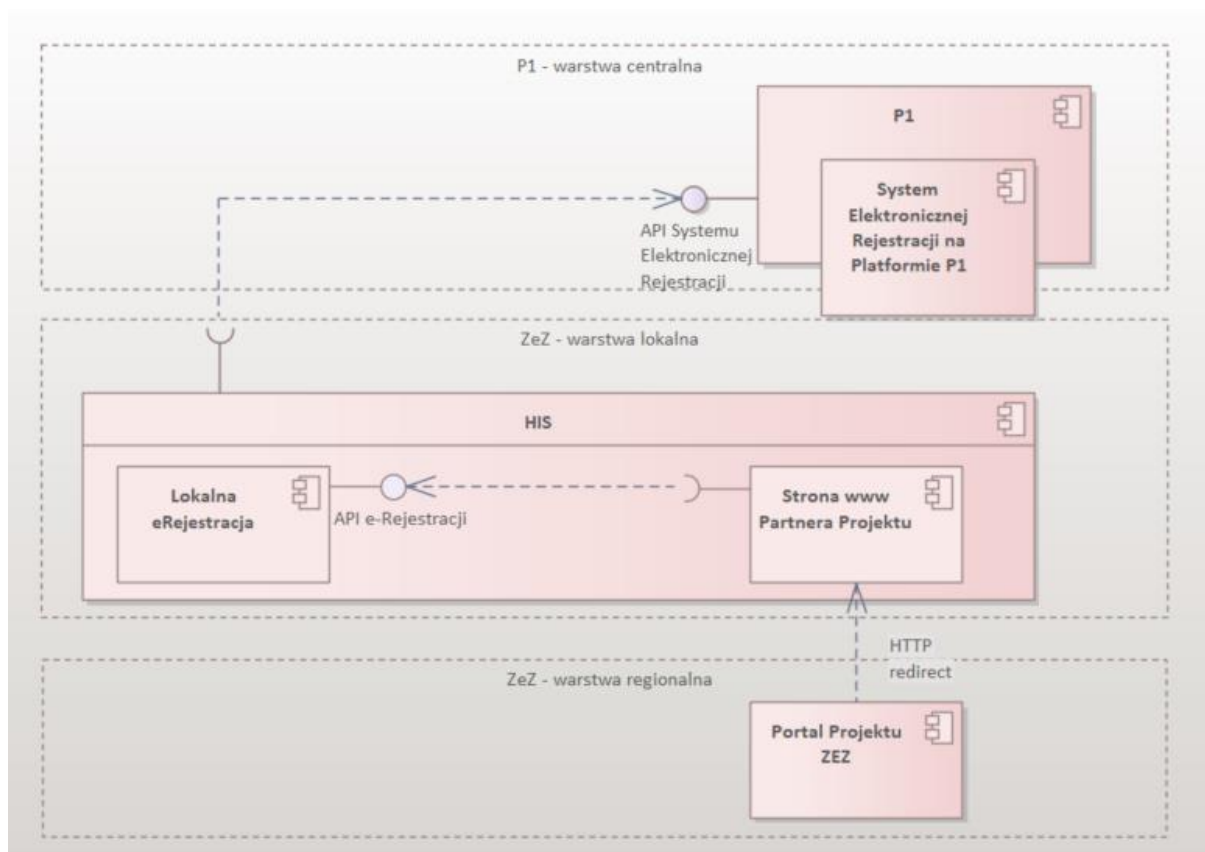
Funkcjonalności e-Rejestracji przeznaczone dla pacjentów są udostępniane poprzez stronę www, funkcjonalności dla pracowników medycznych i administracyjnych są dostępne w systemie HIS lub systemie gabinetowym Partnera.

Ponieważ każdy Partner posiada własną, odrębną e-Rejestrację, pacjent będzie miał dostęp do rezerwacji tylko w obrębie tego Partnera.

Moduł integrujący rejestrację w systemach HIS z krajowym Systemem Elektronicznej Rejestracji musi być zgodny z najnowszą wersją dokumentacji integracyjnej oraz jej przyszłymi zmianami.



Rys. 8. Realizacja usługi e-Rejestracja



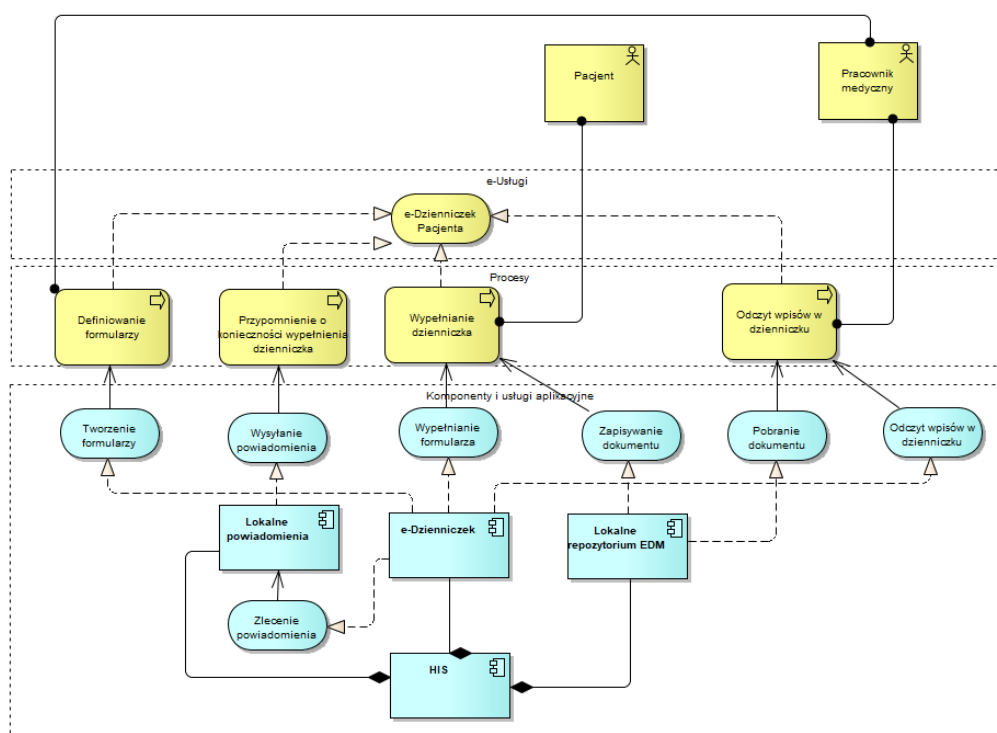
Rys. 9. Integracje modułu e-Rejestracja

6.15 Powiadomienia

Z uwagi na ściśle powiązanie mechanizmów powiadomień z logiką modułu rejestracji, powiadomienia dotyczące usługi e-Rejestracja są zarządzane i wysyłane za pośrednictwem komponentów Lokalne Powiadomienia dedykowanych dla każdego komponentu Lokalna e-Rejestracja.

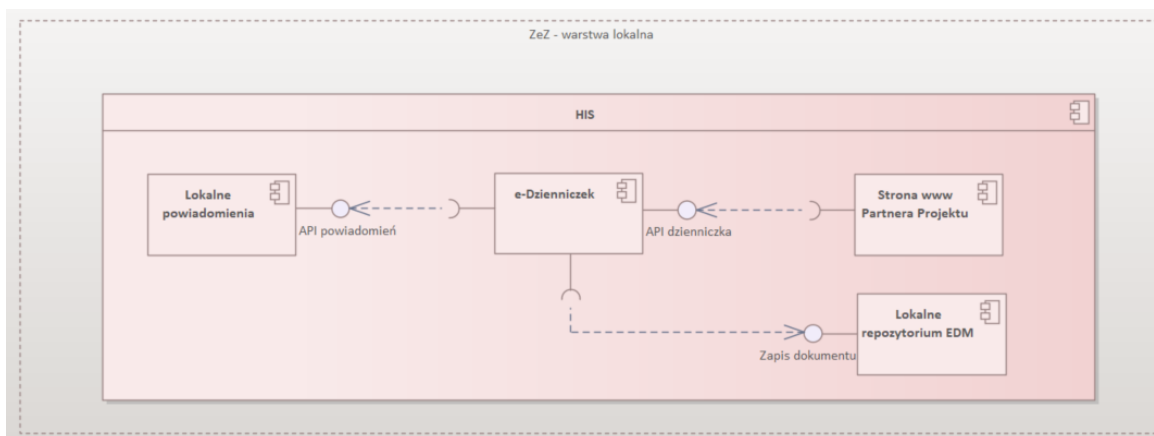
Lokalne powiadomienia odpowiadają za realizację procesu wysyłania powiadomień do pacjenta oraz pozwalają na konfigurację kanałów powiadamiania pacjentów (mail, sms, portal,) dla poszczególnych typów powiadomień.

6.16 e-Dzienniczek Pacjenta



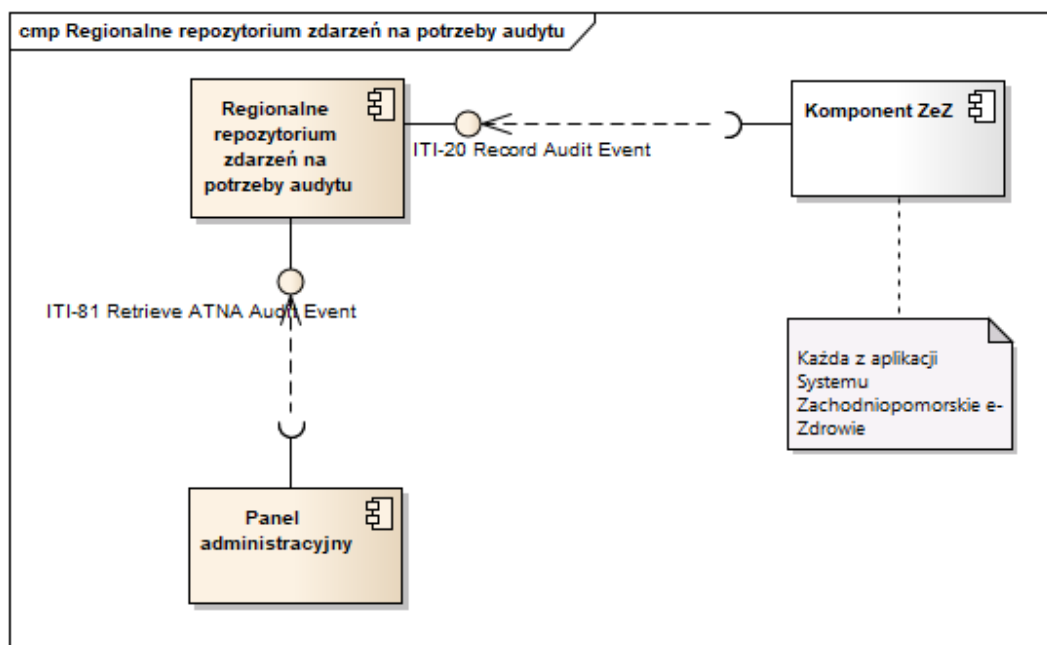
Rys. 10. Realizacja usługi e-Dzienniczek Pacjenta

Lokalny komponent działający w podmiotach leczniczych, które prowadzą okresowy kontakt lub stałą opiekę nad pacjentem nieprzebywającym w sposób ciągły w podmiocie leczniczym, np. terapeutyczne, alergiczne, zabiegi rehabilitacyjne, położnictwo oraz choroby przewlekłe. Usługa pozwala na okresowe lub stałe wprowadzanie indywidualnych danych medycznych pacjenta bezpośrednio przez samego pacjenta lub jego opiekuna, a pracownikowi medycznemu pozwala na utrzymywanie kontaktu z pacjentem, obserwowanie i analizowanie danych oraz udzielanie teleporad jako element telemedycyny.



Rys. 11. Interakcje obszaru e-Dzienniczek Pacjenta

6.17 Zapisywanie zdarzeń na potrzeby audytu



Rys. 12. Interakcje obszaru Regionalnego repozytorium zdarzeń na potrzeby audytu

Moduł Regionalne repozytorium zdarzeń na potrzeby audytu funkcjonuje jako centralny punkt zapisywania (logowania) zdarzeń audytowych zgodnie z profilem IHE ATNA, stanowiącym obowiązkowy profil towarzyszący do profilu XDS.b.

Komunikaty zdarzeń audytowych wysyłane są przez komponenty ZeZ w odpowiedzi na błędy w działaniu aplikacji, naruszenia bezpieczeństwa oraz we wszystkich przypadkach komunikacji z innymi komponentami przewidzianych przez implementowane profile IHE. Komponent posiada również interfejs do wyszukiwania komunikatów zdarzeń, który może być wykorzystany np. do przygotowywania raportów dla pacjentów z udostępniania ich danych.

Komponent oparty jest o otwarty model danych, co umożliwia jego wykorzystanie w innych e-usługach w przyszłości.

Należy zauważyć, że zapis zdarzeń do Regionalnego repozytorium zdarzeń na potrzeby audytu działa równoległe do zapisywania zdarzeń do podsystemu audytu P1, które to dotyczy wyłącznie transakcji z systemem P1.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

6.18 Panel administracyjny

Moduł służy do zarządzania konfiguracją poszczególnych komponentów składających się na warstwę regionalną Systemu ZeZ. Dodatkowo, umożliwia eksport raportów z logów zapisanych w Regionalnym repozytorium zdarzeń na potrzeby audytu, w tym przygotowywanie raportów z udostępnienia danych osobowych w odpowiedzi na zapytania osób fizycznych.

6.19 Moduł uwierzytelniania i autoryzacji

Moduł służy do gwarantowania bezpieczeństwa danych Systemu ZeZ poprzez udostępnianie mechanizmów uwierzytelniania i autoryzacji system - system obligatoryjnych do użycia przez systemy Partnerów łączące się z warstwą regionalną.

Należy zaznaczyć, że moduł ten nie służy do uwierzytelniania, autoryzacji, ani kontroli dostępu do dokumentów dla użytkowników, w tym pacjentów.

6.20 Narzędzia ZEZ API

Moduł odpowiedzialny za udostępnianie i zarządzanie usługami sieciowymi wystawianymi przez komponenty warstwy regionalnej do użycia przez integrujące się z nimi systemami używanymi w komunikacji.

6.21 Integracja z systemem HIS w zakresie interfejsu użytkownika

Interfejs HIS powinien być podstawowym sposobem korzystania z e-Usług systemu przez pracowników medycznych. W związku z powyższym w ramach interfejsu użytkownika systemu HIS pracownik medyczny powinien co najmniej mieć możliwość realizacji następujących zadań:

- 1) zapoznanie się z listą dokumentów pacjenta zaindeksowanych w systemie P1, z uwzględnieniem zadeklarowania trybu dostępu,
- 2) pobranie i wyświetlenie dokumentu medycznego pacjenta z uwzględnieniem zadeklarowania trybu dostępu,
- 3) utworzenie i zapisanie dokumentu medycznego w repozytorium EDM,
- 4) przeglądanie Zdarzeń Medycznych zarejestrowanych w systemie P1,
- 5) zlecenie wykonania badania/świadczenia w ramach e-Skierowania,
- 6) przyjęcie do realizacji lub odrzucenie realizacji badania/świadczenia w ramach e-skierowania,
- 7) zakończenie realizacji badania w ramach e-Skierowania wraz z przesłaniem wyników do wystawcy skierowania,
- 8) obsługa zgód w zakresie:
 - usługi odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia
 - usługi odczytu zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1 (w tym autoryzacji przez SMS)
 - usługi zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne pacjenta
- 9) obsługa procesu związanego z Systemem Elektronicznej Rejestracji w P1:

- pobranie informacji o zapisanych na wizyty pacjentach,
- zsynchronizowanie w systemie pobranych danych z danymi pochodzącymi w innych kanałach rejestracji (np. telefon, osobista wizyta w rejestracji poradni);
- uzyskanie danych osobowych pacjentów;
- komunikacja między Podmiotem a pacjentem realizowana bez udziału Systemu Elektronicznej Rejestracji.

7. Specyfikacja e-usług w Projekcie, analiza procesów biznesowych, wskazanie profili IHE

W rozdziale omówiono planowane do wdrożenia e-usługi, zgodnie z przyjętymi przez Komitet Sterujący rekomendacjami. Opisy w kolejnych podrozdziałach zawierają specyfikacje wymagań funkcjonalnych i нефункциональных dla poszczególnych e-usług.

Omówienie zaimplementowanych profili integracyjnych IHE zamieszczono w rozdziale 3 *Profile oraz transakcje IHE w Projekcie*.

7.1 Specyfikacja e-usług

7.1.1 e-Uслуги - Wymagania нефункциональные

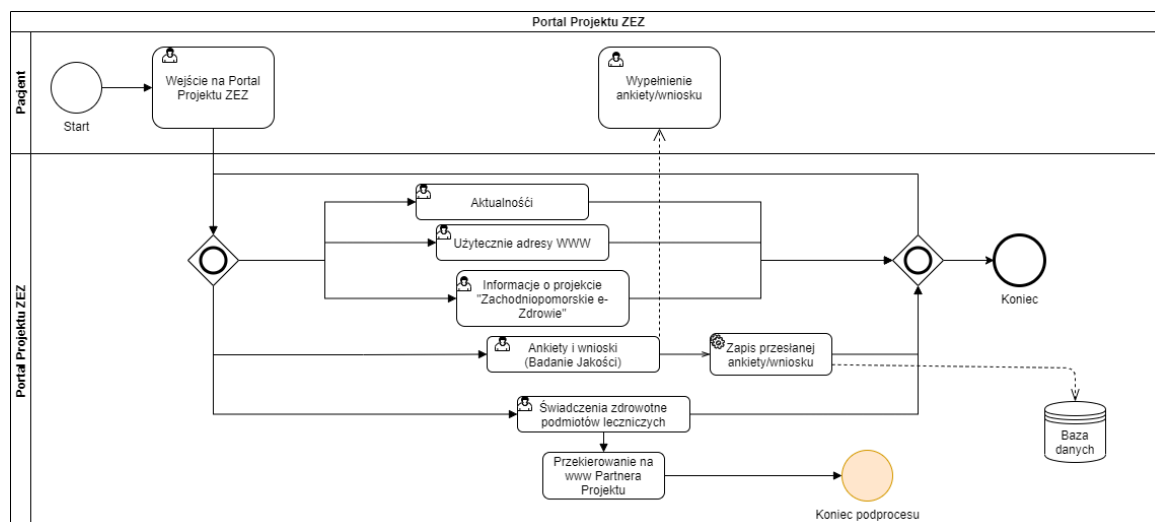
Lp.	Wymaganie
1.	<p>Bezpieczeństwo:</p> <p>1) system zapewni przesyłanie danych z wykorzystaniem bezpiecznego kanału komunikacji - powinien umożliwiać szyfrowanie transmisji danych co najmniej pomiędzy urządzeniami/systemami klienta: komputerami, urządzeniami mobilnymi itp. a pierwszym komponentem systemu, na którym są one przetwarzane;</p> <p>2) system posiada dedykowane mechanizmy obsługi uprawnień, pozwalające na tworzenie i przydzielanie uprawnień użytkownikom osobowym (w ramach Panelu administracyjnego) jak i innym systemom informatycznym w ramach Modułu Uwierzytelnienia i Administracji.</p> <p>3) funkcjonalności związane z udostępnianiem danych są dostępne tylko dla uwierzytelnionych użytkowników;</p>
2.	<p>Graficzny interfejs użytkownika:</p> <p>1) wymagana jest zgodność interfejsu użytkownika z WCAG 2.1 (ang. Web Content Accessibility Guidelines),</p> <p>2) system udostępnia graficzny interfejs użytkownika dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany. Wymagana jest możliwość użytkowania elementów systemu przeznaczonych dla pacjentów w przeglądarkach smartfonów, tabletów i komputerów osobistych,</p> <p>3) wymagana jest możliwość użytkowania systemu na najnowszych wersjach popularnych przeglądarek internetowych: Google Chrome, Firefox, Edge bez konieczności instalacji dodatkowych elementów środowiska uruchomieniowego,</p> <p>4) system udostępnia interfejs użytkownika w języku polskim wraz z możliwością prezentacji nazw słownikowych.</p>
3.	<p>Architektura rozwiązania:</p> <p>1) system powinien posiadać modułową budowę - preferowana architektura oparta o mikrouслуги, podsystemy funkcjonalne;</p> <p>2) należy zapewnić możliwość skalowania horyzontalnego wybranych modułów systemu (w zależności od obciążenia),</p> <p>3) system powinien udostępniać interfejs programowy (API) umożliwiający jego integrację z innym</p>

	oprogramowaniem działającym obecnie lub w przyszłości u Zamawiającego,
	4) architektura systemu powinna pozwalać na wdrożenie go w wariantcie wysokiej dostępności (ang. high availability) poprzez równoczesne działanie jego "zapasowej" instancji.
4.	Oprogramowanie Serwera WWW hostującego system eUsług musi być programem międzyplatformowym i musi być dostępne co najmniej w systemach operacyjnych Linux i Windows.
5.	Stosowane technologie:
	1) wykorzystywane technologie muszą być zgodne z wytycznymi konsorcjum W3C wyznaczającym standardy dokumentów www.
	2) Stosowanie najnowszych wersji odmiany języka HTML wersja HTML5.
	3) Stosowane technologie są akceptowane i wspierane przez producentów popularnych przeglądarek www.
	4) Stosowanie popularnych i ogólnie dostępnych bibliotek i frameworków takich jak: JQuery, Angular, JQuery UI, Bootstrap i tym podobne.
6.	Modele wdrożenia:
	1) zakłada się dostarczenie gotowych do uruchomienia komponentów systemu wraz z wszystkimi zależnościami i domyślną konfiguracją - preferowane wykorzystanie technologii konteneryzacji,
	2) system podczas eksploatacji powinien zapisywać logi z działania w postaci umożliwiającej ich dalsze przetwarzanie w dedykowanych ku temu narzędziach (np. Logstash).

7.2 Portal Projektu ZeZ

7.2.1 Opis usługi - Portal Projektu ZeZ

L.p.	Funkcjonalności podstawowe
1.	Dostęp Pacjenta co do Portalu Projektu ZeZ nie wymaga logowania.
2.	Portal pełni funkcje informacyjne oraz przekierowuje pacjenta do stron www podmiotów leczniczych w celu realizacji e-usług.
	Opis usługi
3.	Portal pełni funkcję informacyjną podzieloną na obszary funkcjonalne pogrupowane tematycznie jak poniżej: <ol style="list-style-type: none"> 1) Aktualności (tzw. news room) – bieżące informacje z zakresu funkcjonowania systemu ochrony zdrowia w regionie z możliwością bezpośredniego dodawania aktualności przez podmioty lecznicze, po wstępnej weryfikacji treści przez administratora. 2) Badanie jakości poprzez ankiety i wnioski – aktywne formularze umożliwiające pacjentom przekazywanie uwag i wniosków odnoszących się do funkcjonowania podmiotów leczniczych, udzielanych przez nie świadczeń oraz prowadzenie regularnych badań ankietowych związanych z badaniami poziomu satysfakcji pacjentów. 3) Świadczenia zdrowotne podmiotów leczniczych (wydzielona przestrzeń dla każdego Partnera Projektu). Powinna zawierać informacje bieżące z poszczególnych podmiotów leczniczych oraz informacje o zakresie funkcjonowania, oddziałach, poradniach, miejscach udzielanie świadczeń oraz przekierowania do e-Rejestracji. 4) Użyteczne adresy www: inne podmioty lecznicze w regionie nie będące Partnerem Projektu, apteki, dostęp do IKP, PUE ZUS i inne. 5) Informacje o projekcie „Zachodniopomorskie e-Zdrowie”: założenia, cele, korzyści dla pacjentów, kalendarium prac, serwis fotograficzny itp.
4.	Interesariusze e-usługi: pacjenci w regionie.
5.	Poziom dojrzałości usługi: 1 – informacja.
6.	Typ usługi: A2C.



Rys. 13. Diagram: Portal Projektu ZeZ

7.3 e-Rejestracja

7.3.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

e-Rejestracja				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsyste- my do realizacji e-usługi	Brakujące moduły/systemy/podsyste- my do realizacji e-usługi
1.	ZCO	Partner posiada i użytkuje moduł e- Rejestracji do przychodni	HIS (Ruch chorych), e-Rejestracja	Powiadomienia, Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
2.	SPWSZ Arkońska	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	e-Rejestracja, e-Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
3.	SPSZOZ Zdroje	Partner posiada i użytkuje moduł e- Rejestracji	HIS (Ruch chorych), e- Rejestracja, e-Skierowanie	e-Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
4.	RS Kołobrzeg	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	e-Rejestracja, e-Powiadomienia, e- Skierowanie Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
5.	SW Koszalin	Partner posiada licencje ale nie wykorzystuje ich produkcyjnie	HIS (Ruch chorych), e- Rejestracja, Powiadomienia,	e-Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
6.	SZGiCHP Koszalin	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	e-Rejestracja, Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu

				Rejestracja w HIS
7.	SPZOZ Gryfice	Partner posiada licencje – rejestracja do przychodni	HIS (Ruch chorych), e-Rejestracja	Powiadomienia, e-Rejestracja Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
8.	ZOL Tuczno	brak	brak	e-Rejestracja, e-Powiadomienia, e-Skierowanie Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
9.	WOMP Szczecin	Partner posiada i wykorzystuje licencje – rejestracji internetowej	HIS, e-Rejestracja	e-Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
10.	WOMP Koszalin	brak	HIS	e-Rejestracja, e-Powiadomienia, e-Skierowanie Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
11.	WSPR Szczecin	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ
12.	Willa Fortuna	brak	HIS	e-Rejestracja, e-Powiadomienia Konieczna integracja z SER na P1 Aktualizacja/rozbudowa modułu Rejestracja w HIS
13.	Stanomino	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	e-Rejestracja, Powiadomienia, e-Skierowanie
14.	UMWZ	brak Usługa na poziomie lokalnym	Usługa na poziomie lokalnym	Usługa na poziomie lokalnym

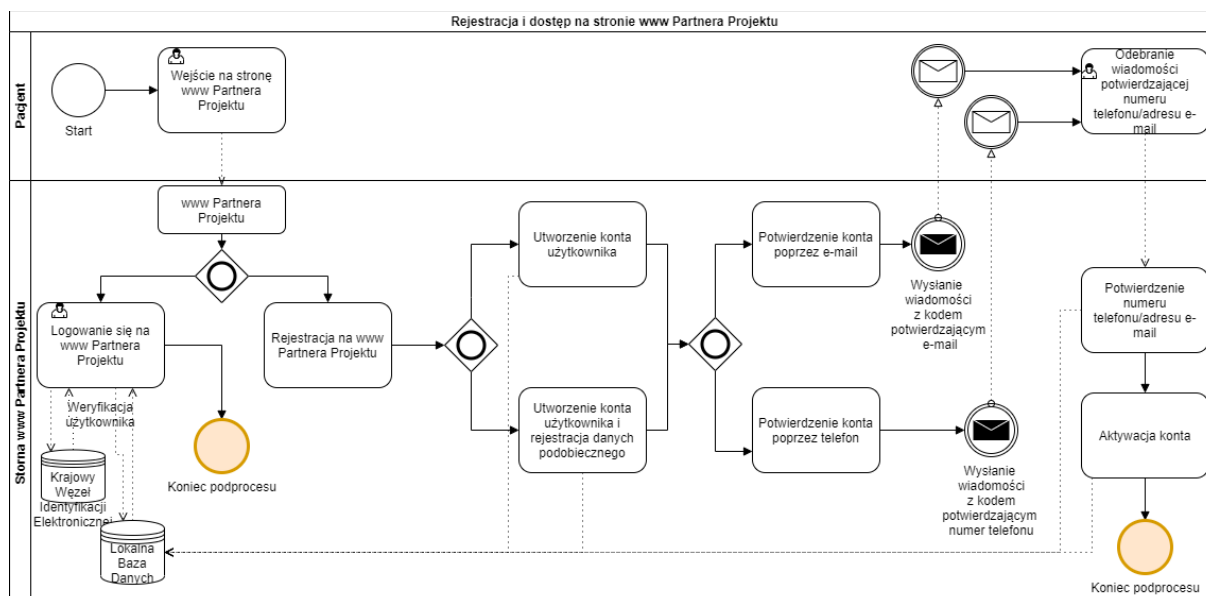
7.3.2 Opis usługi – e-Rejestracja

L.p.	Funkcjonalności podstawowe
1.	Możliwość samodzielnego utworzenia konta w systemie. Dla zagwarantowania właściwego uwierzytelnienia, wymagana aktywacja przy osobistym stawiennictwie w podmiocie leczniczym.
2.	Logowanie z wykorzystaniem Krajowego Węzła Identyfikacji Elektronicznej lub danymi dostępowymi do uprzednio założonego i aktywowanego konta (aktywacja przy osobistym stawiennictwie w podmiocie leczniczym)
3.	Możliwość umówienia wizyty poprzez aplikację webową w podmiocie leczniczym objętym Projektem.
4.	Możliwość rezerwacji terminów wizyt w podmiocie leczniczym oraz anulowania i zmiany terminu wcześniej dokonanych rezerwacji.
5.	e-Rejestracja na wizyty realizowana jest z poziomu strony internetowej www podmiotu leczniczego.
6.	Każdy podmiot leczniczy udostępnia własną aplikację e-Rejestracji.
7.	Integracje: - integracja z P1 w zakresie e-Skierowania, - e-Rejestracja krajowa – integracja z Systemem Elektronicznej Rejestracji SER na platformie P1.

Rejestracja konta użytkownika	
8.	<p>1. Rejestracja konta użytkownika, który jest lub potencjalnie będzie pacjentem jednostki:</p> <ol style="list-style-type: none"> 1) system rejestruje podstawowe dane pacjenta: <ol style="list-style-type: none"> a) imię, nazwisko, b) dane identyfikacyjne pacjenta: nr PESEL albo numer ewidencyjny lub numer dokumentu tożsamości nadane we wskazanym kraju (w przypadku rejestracji obcokrajowców), 2) system rejestruje adres e-mail użytkownika portalu, o ile weryfikowany jest taki kanał komunikacyjny, 3) system rejestruje nr telefonu komórkowego użytkownika portalu, o ile weryfikowany jest taki kanał komunikacyjny, 4) w celu zarejestrowania użytkownika system wymusza akceptację regulaminu świadczenia e-usługi oraz zgody na przetwarzanie danych osobowych, 5) system tworzy konto: <ol style="list-style-type: none"> a) możliwe jest w zależności od ustawień systemu: wymuszenie zgodności nazwy użytkownika (loginu) z podanym adresem e-mail (o ile jest rejestrowany) lub wygenerowanie łatwej do zapamiętania unikalnej nazwy użytkownika (np. pierwsza litera imienia + nazwisko + opcjonalnie nr kolejny użytkownika) lub wprowadzenie przez rejestrującego własnej nazwy użytkownika z kontrolą jej unikalności, b) system umożliwia podanie i powtórzenie hasła do konta oraz weryfikuje poprawność podanego hasła z zadaną polityką. <p>2. Rejestracja konta użytkownika reprezentującego swojego podopiecznego:</p> <ol style="list-style-type: none"> a) system umożliwia rejestrację konta użytkownika poprzez podanie jego imienia, nazwiska, danych kontaktowych (w zależności od przyjętego kanału komunikacji e-mail lub SMS), nazwy użytkownika i hasła spełniając wymagania analogicznie do pkt. 1, b) system umożliwia jednoczesną rejestrację danych podopiecznego użytkownika analogicznie do danych pacjenta w pkt. 1. <p>3. Dostęp do systemu:</p> <ol style="list-style-type: none"> a) system udostępnia funkcję logowania przy użyciu Węzła Krajowego, b) danymi dostępowymi do uprzednio założonego i aktywowanego konta. <p>System udostępnia funkcję zmiany hasła użytkownika – w czasie zmiany hasła weryfikowana jest jego poprawność względem przyjętej polityki – możliwe jest określenie: minimalnej długości hasła, minimalnej liczby wielkich liter, cyfr, znaków specjalnych, liczby niepowtarzających się kolejnych haseł użytkownika.</p>
Opis usługi	
9.	<p>1. Rezerwacja terminu wizyty w podmiocie leczniczym udostępniającym e-Rejestrację na stronie www podmiotu leczniczego:</p> <ol style="list-style-type: none"> 1) system umożliwia wyszukiwanie pacjentom usługi medycznej związanej z planowaną wizytą; usługa może być wyszukiwana z wykorzystaniem następujących kryteriów: <ol style="list-style-type: none"> a) nazwy usługi (poprzez podanie dowolnego ciągu znaków zawierającego się w nazwie usługi), b) nazwy jednostki organizacyjnej szpitala, w której udzielana jest oczekiwana usługa, c) imienia, nazwiska, tytułu naukowego i specjalności lekarza udzielającego oczekiwanej usługi, 2) system umożliwia wybór jednostki organizacyjnej, jeżeli usługa udzielana jest w wielu miejscach, 3) system umożliwia wybór personelu/lekarza udzielającego usługi medycznej, o ile jest dostępny

	<p>dla danej usługi,</p> <ol style="list-style-type: none"> 4) System HIS zwraca listę trzech wolnych terminów odpowiadających kryteriom podanym przez pacjenta oraz pozwala na wybór terminu z listy; po wybraniu terminu system HIS blokuje możliwość wyboru przez innych użytkowników zarówno Portalu Pacjenta jak i HIS, 5) system umożliwia prezentację szczegółowych danych planowanej wizyty: <ol style="list-style-type: none"> a) wybranej usługi medycznej, w tym informacji o warunkach udzielenia usługi, b) danych adresowych miejsca udzielenia usługi, c) danych wybranego personelu/lekarza udzielającego usługi, d) danych na temat miejsca zaplanowanego świadczenia na liście oczekujących do realizacji 6) w przypadku rezerwacji terminu udzielenia świadczeń wymagających skierowania system umożliwia lub wymusza (w zależności od konfiguracji dla danej usługi) rejestrację danych skierowania. <ol style="list-style-type: none"> 2. Przegląd zaplanowanych wizyt pacjenta w podmiocie leczniczym udostępniającym e-Rejestrację: <ol style="list-style-type: none"> 1) system umożliwia przegląd zaplanowanych wizyt pacjenta, 2) system umożliwia prezentację szczegółowych danych zaplanowanej wizyty: informacji o usłudze medycznej wraz z warunkami udzielenia usługi, danych teleadresowych miejsca udzielenia usługi, informacji o personelu udzielającym usługi (o ile jest wybrany na etapie rezerwacji terminu wizyty), planowanego terminu wizyty. 3. Anulowanie zaplanowanych wizyt: <ol style="list-style-type: none"> 1) system umożliwia anulowanie rezerwacji wskazanego terminu wizyty, 2) system automatycznie usuwa rezerwacje terminów wizyt, które nie zostały potwierdzone kodem przesłanym przez SMS po upływie zdefiniowanego przedziału czasu. 4. Zmiana/modyfikacja terminu wizyty w podmiocie leczniczym: <ol style="list-style-type: none"> 1) system umożliwia zmianę/modyfikację wskazanego terminu wizyty na inny dostępny termin, 2) system automatycznie zmienia termin wizyty a następnie przesyła powiadomienie do pacjenta. 5. Integracja z systemem HIS: e-Rejestracja integruje się on-line z systemem HIS w zakresie: <ol style="list-style-type: none"> 1) pobierania dostępnych terminów udzielenia wybranych świadczeń, 2) rezerwacji terminu wybranego świadczenia wraz z rejestracją danych skierowania, o ile są one wprowadzone przez pacjentów, 3) anulowania terminów zaplanowanych wizyt, 4) zmiana/modyfikacje terminu wizyty, 5) zapewnienie spójności słowników między systemami, 6) pobierania informacji o planowanych terminach wizyt. 6. Integracja z P1 w zakresie e-Skierowanie: <ol style="list-style-type: none"> 1) wprowadzenie przez pacjenta kodu autoryzacyjnego skierowania podczas rezerwacji terminu, 2) przekazanie kodu do modułu HIS odpowiedzialnego za przetwarzanie e-Skierowań z P1, 3) informacja dla pacjenta o akceptacji do realizacji lub odrzuceniu skierowania przez pracownika podmiotu leczniczego. 7. Administracja i konfiguracja e-usługi: <ol style="list-style-type: none"> 1) możliwość definiowania ról w systemie z różnymi poziomami dostępu do systemu (uprawnienia), 2) możliwość konfiguracji e-usługi zgodnie z uprawnieniami, 3) definicja słowników z możliwością zachowania spójności z systemem HIS.
10.	Interesariusze e-usługi: pacjenci podmiotu leczniczego, do którego należy dany Lokalny portal pacjenta.
11.	Poziom dojrzałości usługi: 5 – personalizacja.

12. Typ usługi: A2C.



Rys. 14. Diagram: Rejestracja

Prowadzone przez Centrum e-Zdrowia prace, w wyniku których nastąpiło uruchomienie programu pilotażowego w zakresie elektronicznej rejestracji centralnej na wybrane świadczenia. Celem programu pilotażowego jest ocena efektywności elektronicznej rejestracji centralnej, w tym możliwości samodzielnego wyszukiwania przez świadczeniobiorców dostępnych terminów udzielania wybranych świadczeń i dokonywania przez nich zgłoszeń, mechanizmów przydzielania świadczeniobiorcom terminów udzielenia świadczenia, z uwzględnieniem określonych przez nich kryteriów, a także udostępniania przez świadczeniodawców jednostce podległej ministrowi właściwemu do spraw zdrowia właściwej w zakresie systemów informacyjnych ochrony zdrowia harmonogramów przyjęć dla zakresów świadczeń, których dotyczy program pilotażowy, oraz ich prowadzenia w systemie P1 opieki zdrowotnej z zakresu ambulatoryjnej opieki specjalistycznej.

Powyższe działania wymuszają konieczność rozbudowy funkcjonalnej użytkowanych systemów oprogramowania dla zapewnienia integracji systemów HIS podmiotu leczniczego Partnera Projektu (zewnętrzny w stosunku do P1) celem osiągnięcia następujących funkcjonalności:

L.p.	Opis wymagań
1.	System oprogramowania Zamawiającego bezpośrednio zapisuje pacjentów na wizyty dotyczące ww. świadczeń tylko w przypadku, kiedy dla danego świadczenia nie będzie osób oczekujących na wolny termin.
2.	Wykonawca jako dostawca oprogramowania musi zapewnić integrację systemu HIS z systemem P1 w zakresie zarządzania harmonogramami oraz wizytami w Systemie Elektronicznej Rejestracji.
3.	System oprogramowania przesyła do Systemu Elektronicznej Rejestracji (SER) harmonogram zawierający wolne sloty. Wolny slot rozumiany jest jako Obiekt reprezentujący termin (datę i czas) dla danego świadczenia, który Zamawiający zgłasza do Systemu Elektronicznej Rejestracji w celu umożliwienia przypisania do niego pacjenta.
4.	Podmiot może dowolnie modyfikować i usuwać przesłane harmonogramy dopóki do danego wolnego slotu nie

	zostanie przypisany pacjent (zapisana wizyta).
5.	Uruchamiany minimum raz dziennie algorytm w systemie SER dokonuje wyboru pacjentów zgodnie z ich zapisanymi kryteriami dostępności, ustala ich kolejność na podstawie wag a następnie dokonuje przypisania do poszczególnych wolnych slotów zgłoszonych w ramach harmonogramów przez Podmiot.
6.	Po zakończeniu działania algorytmu, SER wysyła powiadomienia do pacjentów, którzy zostali zapisani na wizytę podczas ostatniego uruchomienia algorytmu z informacją, do którego Podmiotu zostali zapisani oraz na jaki dzień i godzinę.
7.	System oprogramowania odpytuje SER w celu pobrania informacji o zapisanych na wizyty pacjentach i zsynchronizowania ich w swoim systemie.
8.	Po uzyskaniu danych osobowych pacjenta przez system oprogramowania Podmiotu dalsza komunikacja między Podmiotem, a pacjentem realizowana jest bez udziału Systemu Elektronicznej Rejestracji.
9.	W komunikacji z systemem P1 wymagane jest użycie rozszerzenia Web Services Security i profilu Web Services Security X.509 Certificate Token Profile.
Uwierzytelnianie Systemu	
10.	Wszystkie usługi sieciowe Systemu Elektronicznej Rejestracji są zabezpieczone z wykorzystaniem mechanizmów WS-Security. System zewnętrzny jest zobowiązany do używania pary certyfikatów wystawionych podmiotowi przez Centrum Certyfikacji P1, tj. certyfikatu do uwierzytelnienia systemu (TLS) i certyfikatu do uwierzytelnienia danych (WS-Security).
11.	Uwierzytelnienie Systemu zewnętrznego wywołującego usługę systemu P1 następuje w warstwie transportowej połączenia za pomocą protokołu TLS z obustronnym uwierzytelnieniem - oprócz uwierzytelnienia serwera przez system zewnętrzny następuje uwierzytelnienie klienta (Systemu zewnętrznego) przez serwer.
12.	Do nawiązania połączenia TLS system zewnętrzny zobowiązany jest użyć certyfikatu do uwierzytelnienia systemu wydanego przez Centrum Certyfikacji P1 (użycie przez klienta P1 klucza prywatnego powiązanego z certyfikatem do uwierzytelnienia systemu przekazanego przez CeZ w wyniku założenia konta).
Uwierzytelnianie danych	
13.	System zewnętrzny zobowiązany jest do podpisania komunikatu SOAP z użyciem certyfikatu do uwierzytelnienia danych służącego do weryfikacji złożonego podpisu cyfrowego.
14.	Po poprawnej weryfikacji podpisu cyfrowego na podstawie certyfikatu do uwierzytelnienia danych identyfikowany i uwierzytelniany jest Usługodawca, w kontekście którego realizowana będzie usługa.
15.	Po uwierzytelnieniu następuje autoryzacja, na którą składa się autoryzacja wykonania usługi oraz autoryzacja dostępu do danych. Autoryzacja wykonania usługi polega na sprawdzeniu przydzielenia do konta Usługodawcy uprawnień związanych z wywoływaniem usługi. Autoryzacja dostępu do danych wykonywana jest w określonych przypadkach i weryfikuje możliwość dostępu do danych na podstawie parametrów wywołania usługi (np. dostęp podmiotu do zarezerwowanej w nim wizyty).
16.	Za uwierzytelnienie użytkownika końcowego Usługodawcy odpowiedzialny jest System zewnętrzny.
17.	System zewnętrzny uwierzytelnia użytkowników końcowych, a następnie przekazuje żądania do systemu P1. Tam gdzie jest to wymagane system zewnętrzny deklaruje informacje o użytkowniku końcowym (np. przez przekazanie identyfikatora pracownika medycznego lub pracownika administracyjnego zgodnie z ustalonym formatem).
18.	System P1 nie realizuje powtórnego uwierzytelnienia użytkownika końcowego, w kontekście którego wykonywana jest usługa sieciowa.
19.	Scenariusz wywołania usług: <ul style="list-style-type: none"> a) pobranie informacji o wizytach; b) zapis pacjenta na listę oczekujących;



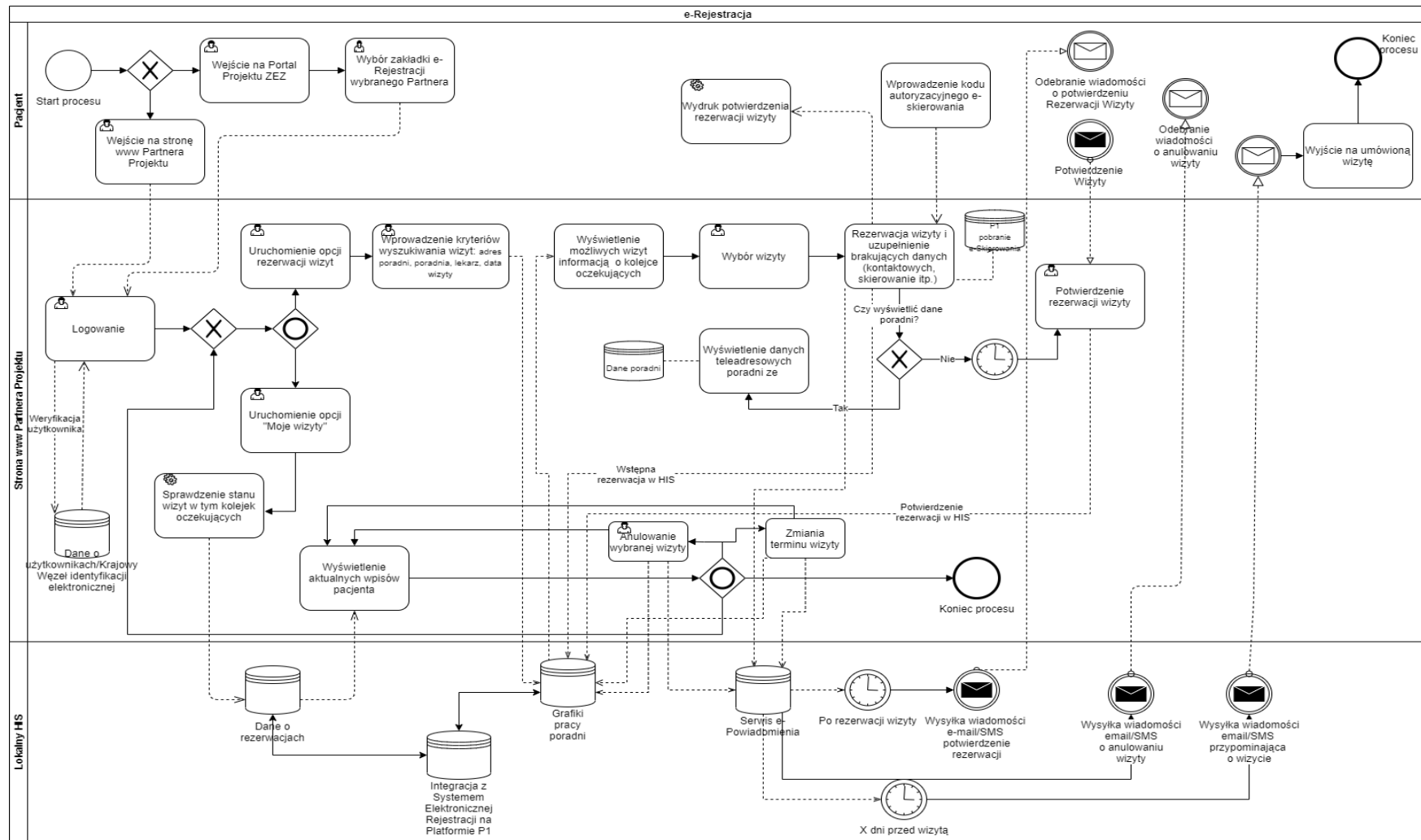
Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



	<ul style="list-style-type: none">c) anulowanie/zmiana zapisu pacjenta na listę oczekujących;d) zapis pacjenta na wizytęe) anulowanie / zmiana zapisu na wizytę
--	---

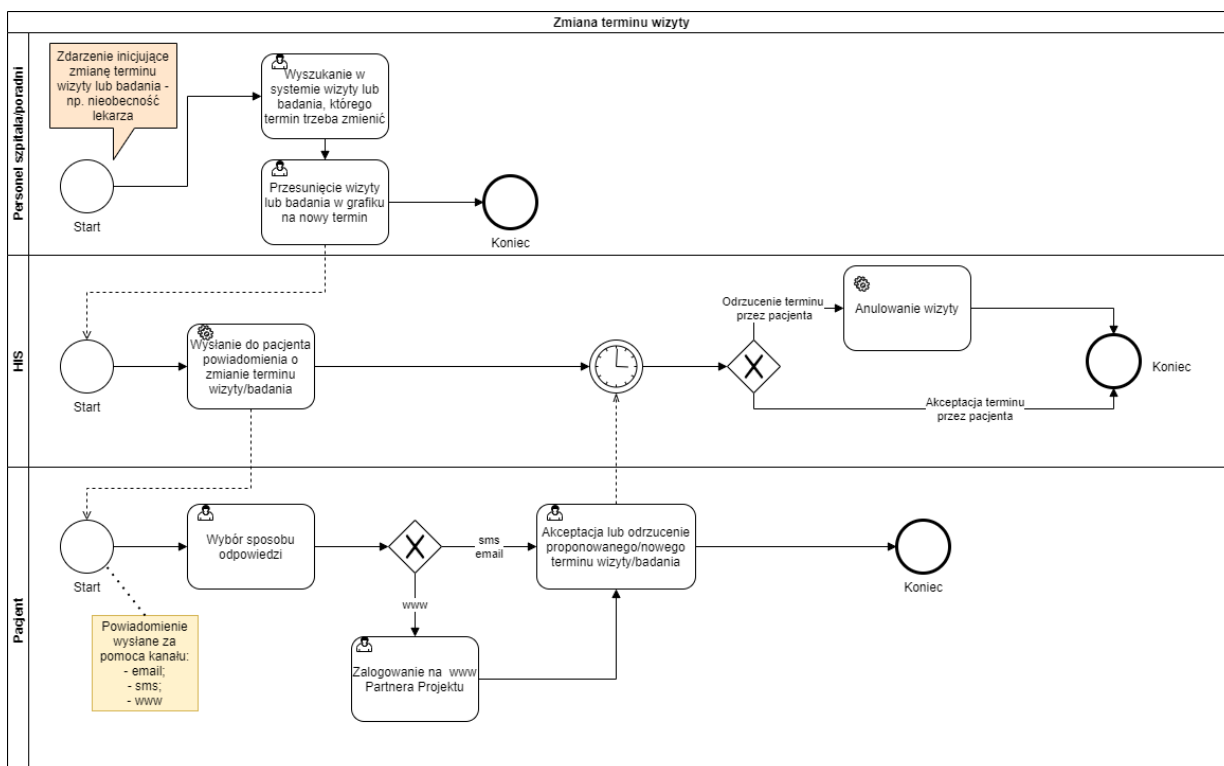


Rys. 15. Diagram: e-Rejestracja

7.3.3 Funkcjonalność e-Powiadomienia w ramach e-Uслуги e-Rejestracja

Lp.	Funkcjonalności minimalne
1.	Możliwość powiadamiania pacjentów o planowanych wizytach w poradniach specjalistycznych za pomocą technologii internetowo-komunikacyjnych (SMS, e-mail).
2.	Możliwość potwierdzania przez pacjentów zaplanowanych wizyt w poradniach specjalistycznych za pomocą technologii internetowo-komunikacyjnych (SMS, e-mail).
	Opis funkcjonalności e-Powiadomienia
3.	<p>Realizacja funkcjonalności w oparciu o następujące procesy:</p> <ol style="list-style-type: none"> 1) na skutek określonego zdarzenia, np. nieobecności lekarza, personel zmienia termin wizyty pacjenta, 2) system wysyła dostępnymi kanałami (email, sms) powiadomienie dla pacjenta o zmianie terminu wizyty/badania i prosi o potwierdzenie proponowanego nowego terminu; następnie oczekuje na odpowiedź pacjenta, 3) Pacjent wysyła zwrotną informację o potwierdzeniu lub odrzuceniu proponowanego terminu za pomocą sms, email lub bezpośrednio poprzez stronę internetową (w tym przypadku wcześniej się do niego loguje). System analizuje otrzymaną informację zwrotną – jeśli pacjent nie potwierdza nowego terminu rezerwacji, system anuluje wizytę/badanie. <p>Funkcjonalności:</p> <ol style="list-style-type: none"> 1) moduł automatycznych powiadomień pacjenta o zbliżających się terminach wizyt oraz innych zdarzeń medycznych (np. termin badania, wizyty, informacje o badaniach profilaktycznych) za pomocą 3 kanałów komunikacji: e-mail, wiadomości systemowe portalu pacjenta dostępne po zalogowaniu do portalu, SMS za pomocą bramki SMS udostępnionej przez właściciela usługi, 2) generowanie wiadomości przypominających pacjentom o wizytach i badaniach, 3) generowanie wiadomości w pakietach, 4) możliwość konfiguracji formatu treści wiadomości do wysyłki, a w tym użycie parametrów: <ol style="list-style-type: none"> a) imię pacjenta, b) nazwisko pacjenta, c) numer pacjenta, d) data wizyty (dd-mm-yyyy), e) dzień wizyty (dd), f) miesiąc wizyty (numer w formacie mm lub słownie), g) rok wizyty (yyyy), - godzina wizyty (HH:mm), h) krótka nazwa usługi. 5) możliwość definicji szablonów wiadomości niezależnych dla każdego typu usług/porad, 6) możliwość definicji domyślnego szablonu wiadomości dla usług/porad/wizyt, 7) możliwość generowania wiadomości tylko dla pacjentów, którzy wyrazili zgodę na otrzymywanie komunikatów SMS, 8) gromadzenie wszystkich wysłanych wiadomości w bazie danych systemu wraz z datą wygenerowania i powiązanie ich z wizytą, usługą, pacjentem, wykorzystanym szablonem wiadomości, 9) zabezpieczenie przed ponowną wysyłką tego samego komunikatu, 10) możliwość konfiguracji godziny oraz cykli w dniach, w jakich pakiety wiadomości będą generowane do wysyłki, 11) moduł komunikacji SMS opcjonalnie zintegrowany z rejestrem wizyt i pacjentów systemu

- Ruchu Chorych,
- 12) możliwość konfiguracji maksymalnej długości wiadomości SMS,
 - 13) automatyczna weryfikacja i generowanie wiadomości tylko do pacjentów posiadających uzupełniony w systemie numer telefonu komórkowego,
 - 14) możliwość wskazania przez pacjenta jakie kanały komunikacji preferuje w przypadku powiadomień o wizytach, badaniach, zbliżającym się terminie przyjęcia do szpitala wg kolejki oczekujących, informacjach o badaniach profilaktycznych.



Rys. 16. Diagram: e-Powiadomienia – zmiana terminu wizyty

7.4 EDM

EDM	
L.p.	Funkcjonalności minimalne
1	Umożliwienie wymiany elektronicznej dokumentacji medycznej EDM w obrębie domeny krajowej z udziałem systemu P1.
2	Umożliwienie pracownikowi medycznemu Partnera Projektu dostępu do elektronicznej dokumentacji medycznej EDM wytworzonej poza podmiotem, w którym pracuje dany pracownik.
3	Umożliwienie dostępu do elektronicznej dokumentacji medycznej EDM wytworzonej przez Partnera projektu, pracownikom medycznym innych podmiotów.
4	Umożliwienie pacjentom dostępu do własnej elektronicznej dokumentacji medycznej EDM, udostępnionej przez Partnera, za pośrednictwem Internetowego Konta Pacjenta.
5	Umożliwienie pracownikom medycznym Partnerów projektu raportowanie, wyszukiwanie i odczyt Zdarzeń Medycznych przechowywanych w systemie P1.
Opis usługi:	
6	Wytworzone w podmiocie leczniczym dokumenty medyczne EDM są zapisywane przez HIS w Lokalnym Repozytorium EDM podmiotu leczniczego.
7	Wytworzone w podmiocie leczniczym dokumenty medyczne EDM objęte obowiązkiem indeksowania EDM są rejestrowane w rejestrze EDM systemu P1. Rejestracji dokonuje repozytorium, w którym został zapisany dokument (lokalne lub regionalne).
8	Wytworzone w podmiocie leczniczym dokumenty medyczne EDM są udostępniane z Regionalnego Repozytorium EDM
9	Systemy HIS Partnerów mogą wyszukiwać dokumenty medyczne EDM zaindeksowane w rejestrze EDM systemu P1.
10	Systemy HIS Partnerów mogą pobierać dokumenty medyczne EDM zaindeksowane w rejestrze EDM systemu P1 z repozytoriów domeny krajowej, w których te dokumenty są przechowywane.
11	Dostęp do dokumentów EDM gromadzonych w repozytoriach ZeZ jest możliwy tylko w ramach trybów przewidzianych ustawowo w ramach globalnych polityk dostępu, w tym w trybie zgody pacjenta.
12	Zarządzanie zgodami na dostęp do EDM realizowane jest z poziomu IKP (P1). Pacjent samodzielnie decyduje o nadaniu zgody na dostęp. System ZeZ nie posiada własnego repozytorium zgód ani własnych mechanizmów ich wyrażania.
13	Systemy HIS Partnerów mogą rejestrować zdarzenia medyczne w systemie P1. Komponenty służące do tego celu znajdują się w warstwie lokalnej.
14	Systemy HIS Partnerów mogą wyszukiwać i pobierać zdarzenia medyczne zarejestrowane w systemie P1. Komponenty służące do tego celu znajdują się w warstwie lokalnej.
15	Systemy HIS Partnerów podczas rejestrowania, wyszukiwania lub pobierania dokumentów indeksowanych w P1 lub zdarzeń medycznych, uwierzytelniają się i autoryzują w P1 z wykorzystaniem metod i procedur określonych przez CeZ.
16	Interesariusze e-usługi: personel medyczny, pacjenci .
17	Poziom dojrzałości usługi: 4 – transakcja.
18	Typ usługi: A2C.

7.4.1 Funkcjonalność EDM dla pacjenta

7.4.1.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

EDM dla Pacjenta				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/pod systemy do realizacji e-usługi	Brakujące moduły/systemy/podsystemy do realizacji e-usługi
1.	ZCO	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
2.	SPWSZ Arkońska	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
3.	SPSZOZ Zdroje	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
4.	RS Kołobrzeg	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
5.	SW Koszalin	brak	HIS (Ruch Chorych, Lecznictwo otwarte), EDM, e-Wyniki	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
6.	SZGiCHP Koszalin	brak	HIS (Ruch Chorych, Lecznictwo otwarte), EDM	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
7.	SPZOZ Gryfice	brak	HIS (Ruch Chorych, Lecznictwo otwarte), EDM	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
8.	ZOL Tuczno	brak	brak	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne HIS (dostawa i wdrożenie)
9.	WOMP Szczecin	brak	HIS, EDM	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
10.	WOMP Koszalin	brak	HIS	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne HIS (dostawa i wdrożenie)
11.	WSPR Szczecin	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ

12.	Willa Fortuna	brak	HIS	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
13.	Stanomino	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	dostosowanie do wymagań projektu: EDM, Zdarzenia Medyczne
14.	UMWZ	Usługa na poziomie lokalnym	Usługa na poziomie lokalnym	Usługa na poziomie lokalnym

7.4.1.2 Opis usługi – EDM dla pacjenta

EDM dla pacjenta	
L.p.	Funkcjonalności minimalne
1.	Zapewnienie pacjentowi możliwości dostępu do własnej dokumentacji medycznej wytworzonej przez Partnera Projektu metodą zdalną, za pośrednictwem Internetu.
2.	Dostęp pacjenta do EDM objętej obowiązkiem indeksowania oraz zdarzeń medycznych, jest realizowany zgodnie z rekomendacjami CeZ poprzez IKP.
Opis usługi:	
3.	Dostęp do elektronicznej dokumentacji medycznej EDM wytworzonych i zaindeksowanych przez Partnera jest realizowany jedynie poprzez Internetowe Konto Pacjenta.
4.	Pacjent poprzez IKP może pobrać całość swojej dokumentacji przechowywanej w Repozytorium Regionalnym EDM lub Repozytorium Lokalnym
5.	Poziom dojrzałości usługi: 4 – transakcja.
6.	Typ usługi: A2C.

7.4.2 Funkcjonalność EDM dla lekarza

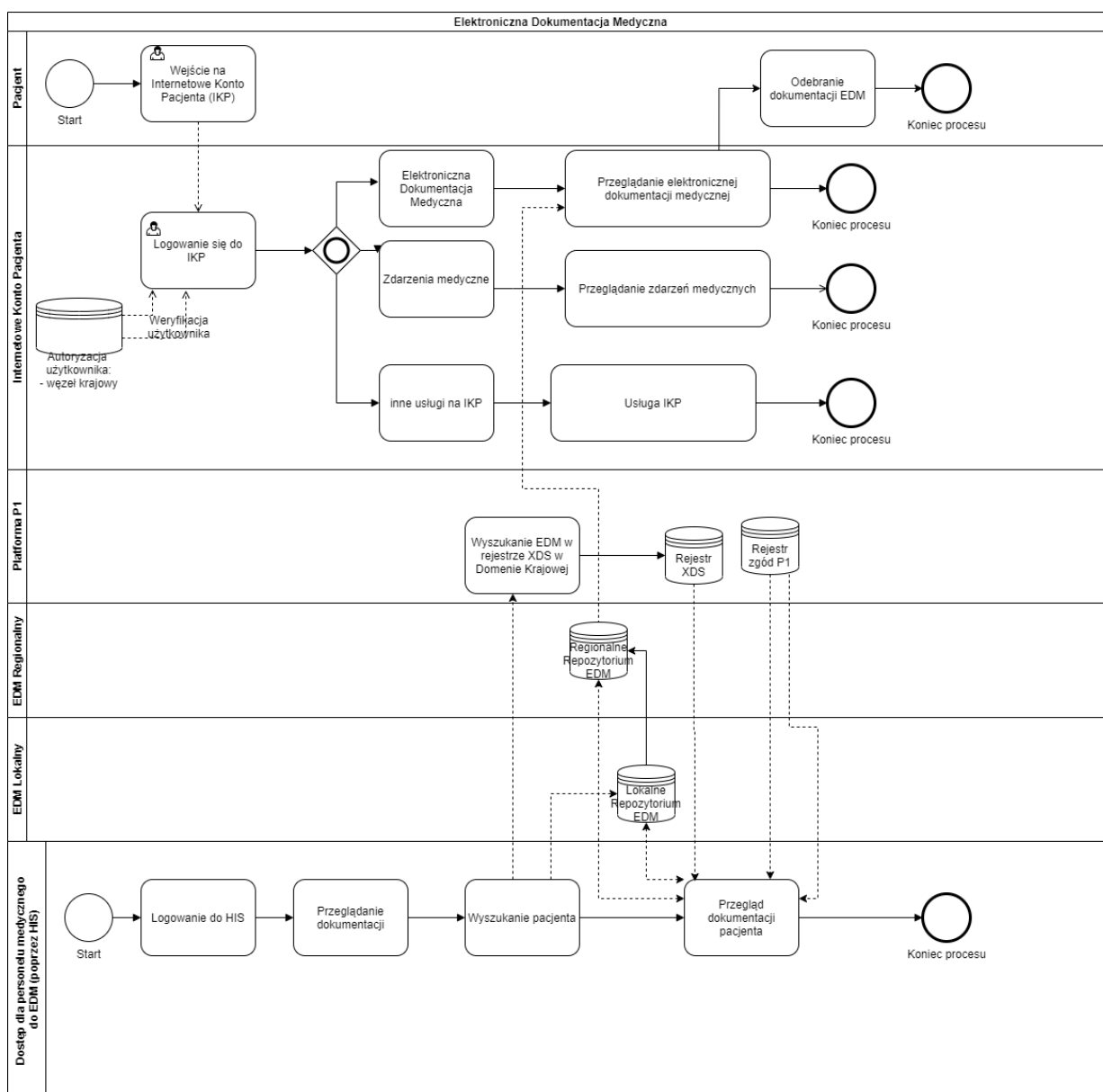
7.4.2.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

EDM dla Lekarza				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsystemy do realizacji e-usługi	Brakujące moduły/systemy/podsystemy do realizacji e-usługi
1.	ZCO	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), e-ZLA, e-ZWM, Panel Lekarski na Oddziale, RIS/PACS, Integracja HIS-RIS/PACS
2.	SPWSZ Arkońska	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne

3.	SPSZOZ Zdroje	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne, Blok Operacyjny, Zakażenia szpitalne, Integracja z LIS, Integracja z RIS/PACS, Blok porodowy, SOR
4.	RS Kołobrzeg	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne, Rehabilitacja, Blok Operacyjny, Zakażenia szpitalne, e-ZLA, e-Skierowanie
5.	SW Koszalin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), e-ZLA, e-ZWM, Pulpit Lekarski, RIS/PACS, Integracja HIS-RIS/PACS
6.	SZGiCHP Koszalin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), HIS (rozszerzenie licencji wybranych modułów), Zakażenia Szpitalne, Pulpit Lekarski i pielęgniarzki
7.	SPZOZ Gryfice	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), HIS (rozszerzenie licencji wybranych modułów), Blok Porodowy, Rehabilitacja, Pulpit Lekarski i Pielęgniarski
8.	ZOL Tuczno	brak	brak	EDM, Zdarzenia Medyczne, HIS (dostawa i wdrożenie)
9.	WOMP Szczecin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), Medycyna Pracy, Integracja HIS-RIS-PACS
10.	WOMP Koszalin	brak	HIS	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu),
11.	WSPR Szczecin	brak	brak	Partner nie realizuje usługi w projekcie ZEZ
12.	Willa Fortuna	brak	HIS	EDM, Zdarzenia Medyczne , HIS (rozszerzenie licencji wybranych modułów), Przychodnia, eZLA, eZWM
13.	Stanomino	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, Zdarzenia Medyczne (dostosowanie do wymogów projektu), Integracja z LIS, Podpis Elektroniczny, e-ZLA, e-Skierowanie
14.	UMWZ	brak	brak	brak

7.4.2.2 Opis usługi – EDM dla lekarza

EDM dla lekarza	
L.p.	Funkcjonalności minimalne
1.	Umożliwienie pracownikowi medycznemu Partnera projektu dostępu do elektronicznej dokumentacji medycznej EDM wytworzonej poza podmiotem, w którym pracuje dany pracownik.
2.	Umożliwienie dostępu do elektronicznej dokumentacji medycznej EDM przechowywanej w Repozytorium Regionalnym EDM wytworzonej przez Partnera projektu, pracownikom medycznym innych podmiotów.
3.	Umożliwienie pracownikom medycznym Partnerów projektu raportowanie, wyszukiwanie i odczyt Zdarzeń Medycznych przechowywanych w systemie P1.
4.	Systemy lokalne podmiotów leczniczych muszą zapewniać możliwość deklaracji trybu dostępu do dokumentacji medycznej, usług odczytu zgody pacjenta na dostęp do informacji o stanie zdrowia i odczytu zgody pacjenta na dostęp do dokumentacji medycznej zarejestrowanej w systemie P1 oraz usługi zapisu, odczytu i wyszukiwania zgód na świadczenie medyczne.
5.	Interfejs HIS powinien być podstawowym sposobem korzystania z e-Usług systemu regionalnego przez pracowników medycznych. W związku z powyższym w ramach interfejsu użytkownika systemu HIS pracownik medyczny powinien co najmniej mieć możliwość realizacji następujących zadań: <ol style="list-style-type: none"> 1) zapoznanie się z listą dokumentów pacjenta zaindeksowanych w systemie P1, z uwzględnieniem zadeklarowania trybu dostępu, 2) pobranie i wyświetlenie dokumentu medycznego pacjenta, z uwzględnieniem zadeklarowania trybu dostępu, 3) utworzenie i zapisanie dokumentu medycznego w repozytorium EDM (zgodnie z konfiguracją dla danego Partnera – lokalnym lub regionalnym), 4) przeglądanie Zdarzeń Medycznych zarejestrowanych w systemie P1.
6.	Interesariusze e-usługi: personel medyczny.
7.	Poziom dojrzałości usługi: 4 – transakcja.
8.	Typ usługi: A2C.



Rys. 17. Diagram: Elektroniczna Dokumentacja Medyczna

7.5 e-Dzienniczek pacjenta

7.5.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

e-Dzienniczek pacjenta				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsystemy do realizacji e-usługi	Brakujące moduły/systemy/podsystemy do realizacji e-usługi
1.	ZCO	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
2.	SPWSZ Arkońska	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
3.	SPSZOZ Zdroje	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	e-Dzienniczek, Powiadomienia
4.	RS Kołobrzeg	Partner nie realizuje usługi w projekcie ZEZ	HIS (Ruch Chorych, Lecznictwo otwarte)	Partner nie realizuje usługi w projekcie ZEZ
5.	SW Koszalin	Partner nie realizuje usługi w projekcie ZEZ	HIS (Ruch Chorych, Lecznictwo otwarte)	Partner nie realizuje usługi w projekcie ZEZ
6.	SZGiCHP Koszalin	Partner nie realizuje usługi w projekcie ZEZ	HIS (Ruch Chorych, Lecznictwo otwarte)	Partner nie realizuje usługi w projekcie ZEZ
7.	SPZOZ Gryfice	Partner nie realizuje usługi w projekcie ZEZ	HIS (Ruch Chorych, Lecznictwo otwarte)	Partner nie realizuje usługi w projekcie ZEZ
8.	ZOL Tuczno	Partner nie realizuje usługi w projekcie ZEZ	brak	HIS (dostawa i wdrożenie), , Powiadomienia
9.	WOMP Szczecin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
10.	WOMP Koszalin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
11.	WSPR Szczecin	Partner nie realizuje usługi dla pacjent a w projekcie ZEZ, tylko EDM dla lekarza CWL	Partner nie realizuje usługi dla pacjenta w projekcie ZEZ, tylko EDM dla lekarza CWL	Partner nie realizuje usługi w projekcie ZEZ,
12.	Willa Fortuna	Partner nie realizuje usługi w projekcie ZEZ	HIS	Partner nie realizuje usługi w projekcie ZEZ
13.	Stanomino	brak	HIS (Ruch Chorych, Lecznictwo otwarte)	Partner nie realizuje usługi w projekcie ZEZ
14.	UMWZ	Usługa na poziomie lokalnym	Usługa na poziomie lokalnym	Usługa na poziomie lokalnym

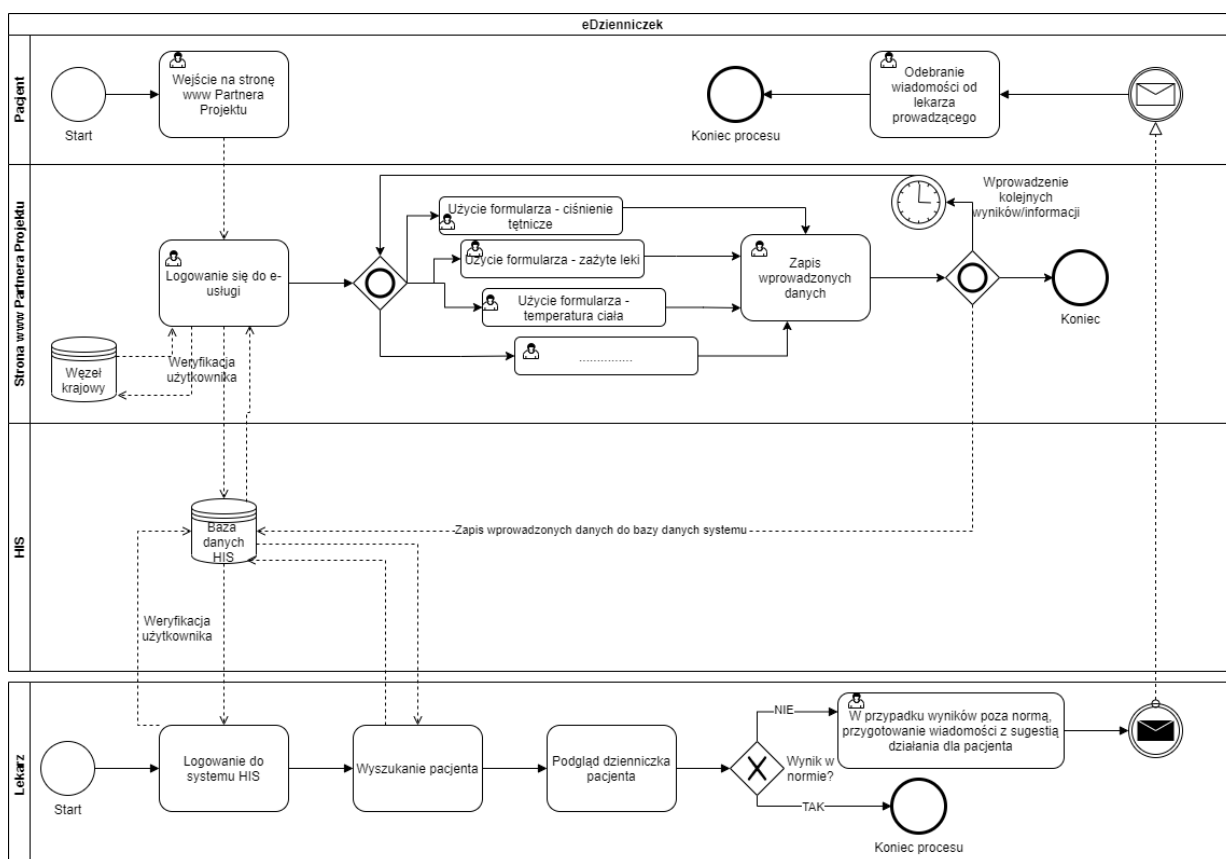
7.5.2 Opis usługi – e-Dzienniczek

Usługa e-Dzienniczek pacjenta będzie świadczona przez wybrane podmioty lecznicze.

e-Dzienniczek pacjenta będzie wykorzystany przez podmioty lecznicze prowadzące okresowy kontakt lub stałą opiekę nad pacjentem, który nie przebywa w sposób ciągły w podmiocie leczniczym np. pobyty terapeutyczne, alergiczne, zabiegi rehabilitacyjne, położnictwo oraz choroby przewlekłe. Usługa pozwoli na wprowadzanie indywidualnych danych medycznych pacjenta bezpośrednio przez niego samego lub jego opiekuna, a pracownikowi medycznemu na utrzymywanie kontraktu z pacjentem, obserwowanie i analizowanie danych oraz udzielanie teleporad jako element telemedycyny.

Część funkcjonalności e-Dzienniczka pacjenta powinna być zrealizowana jako rozszerzenia HIS/EDM na poziomie lokalnym z uwzględnieniem specyfikacji świadczeń medycznych u Partnera.

L.p.	Funkcjonalności minimalne
1.	Możliwość zdefiniowania mechanizmów samoobserwacji przez pracownika medycznego, z których będzie mógł korzystać pacjent.
2.	Dostęp pacjenta do periodycznie wyświetlających się formularzy w które będzie mógł wprowadzać informacje o swoim stanie zdrowia.
	Opis usługi:
3.	Przedmiotowa usługa realizowana będzie w oparciu o następujące cechy: <ol style="list-style-type: none"> 1) Możliwość zdefiniowania przez pracownika formularza zawierającego obserwacje o których wykonywanie chce prosić pacjenta oraz określenie częstości wypełniania formularza. 2) Definiowanie formularza na podstawie wyboru z wcześniej zdefiniowanego zestawu obserwacji. 3) Otrzymywanie przez pacjenta przypomnienia o konieczności wypełnienia formularza za pośrednictwem systemu e-Powiadomienia. 4) Możliwość dodania przez pacjenta dokumentów medycznych będących w jego posiadaniu, pochodzących z podmiotów medycznych nie uczestniczących w Projekcie zarówno w postaci dokumentów HL7 CDA jak i skanów dokumentów papierowych, do Lokalnego repozytorium EDM.-
4.	Interesariusze e-usługi: pacjenci podmiotu leczniczego.
5.	Poziom dojrzałości usługi: 4 – transakcja.
6.	Typ usługi: A2C.



Rys. 18. e-Dzienniczek

7.6 Systemy analityczne

Rozdział zawiera opisy systemów dziedzinowych klasy Business Intelligence (BI) umożliwiających świadczenie e-usług typu A2A.

7.6.1 System Analizy Sprawozdawczej SAS

Zgodnie z przyjętymi założeniami docelowo SAS będzie narzędziem nadzoru działalności systemu ZeZ. SAS ma umożliwić instytucji zarządzającej, poprzez dostarczone raporty, monitorowanie i analizę stanu wykorzystywania systemu ZeZ oraz publikację tych raportów. Usługa SAS będzie realizowana automatycznie, zaś jej użytkownikami będą pracownicy WZ UMWZ.

7.6.1.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

SAS System Analiz Sprawozdawczych				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsyst emy do realizacji e-usługi	Brakujące moduły/systemy/podsystemy do realizacji e-usługi
1.	ZCO	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM
2.	SPWSZ Arkońska	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM
3.	SPSZOZ Zdroje	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM e-Dzienniczek, EDM
4.	RS Kołobrzeg	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM , EDM
5.	SW Koszalin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Wdrożenie i dostosowanie do wymogów projektu: e- Rejestracja, e-Powiadomienia, EDM , EDM
6.	SZGiCHP Koszalin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM , EDM (rozszerzenie funkcjonalności i licencji)
7.	SPZOZ Gryfice	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM EDM (rozszerzenie funkcjonalności i licencji)
8.	ZOL Tuczno	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, EDM , e-Skierowania, EDM
9.	WOMP Szczecin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, , EDM
10.	WOMP Koszalin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, k, EDM
11.	WSPR Szczecin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
12.	Willa Fortuna	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, , EDM

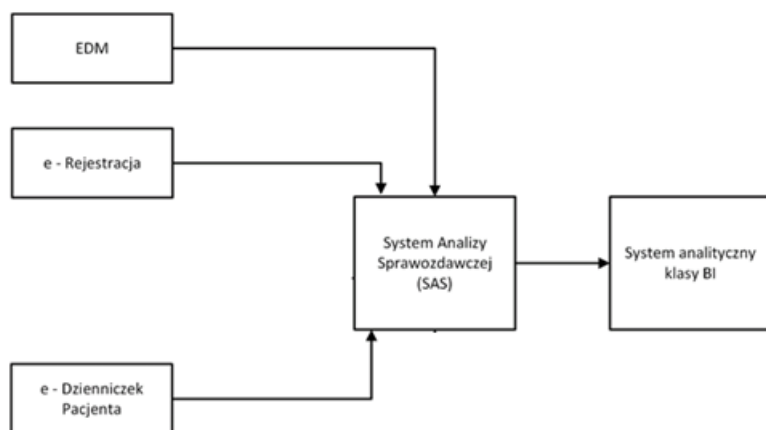
13.	Stanomino	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	e-Rejestracja, e-Powiadomienia, e-Dzienniczek, EDM
14.	UMWZ	brak	System powstanie na poziomie Warstwy Regionalnej	System powstanie na poziomie Warstwy Regionalnej

7.6.1.2 Gromadzenie i analiza danych o użytkowaniu e-usług

Celem procesu jest gromadzenie informacji o liczbie pobrań dokumentacji, wykorzystaniu usług i portalu przez użytkowników Projektu ZeZ. Proces będzie realizowany automatycznie.

Zakres gromadzonych danych:

- 1) poziom realizacji wskaźników,
- 2) efektywność wykorzystywania e-usług,
- 3) zasoby medyczne i ich wykorzystanie,
- 4) zdrowie i potrzeby medyczne mieszkańców,



Rys. 19. Diagram: System Analizy Sprawozdawczej SAS

7.6.2 System Analiz Zarządczych

7.6.2.1 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

SAZ System Analiz Zarządczych				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsystemy do realizacji e-usługi	Brakujące moduły/systemy/podsystemy do realizacji e-usługi
1.	ZCO	brak	HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM
2.	SPWSZ Arkońska	brak	HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM
3.	SPSZOZ Zdroje	brak	HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM, Blok Operacyjny, Zakażenia szpitalne, Integracja z LIS, Integracja z RIS/PACS, Blok porodowy, SOR
4.	RS Kołobrzeg	brak	HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM, Rehabilitacja, Blok Operacyjny, Zakażenia szpitalne, e-ZLA, e-Skierowanie
5.	SW Koszalin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM (dostosowanie do wymogów projektu), e-ZLA, e-ZWM, Pulpit Lekarski, RIS/PACS, Integracja HIS-RIS/PACS
6.	SZGiCHP Koszalin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM (dostosowanie do wymogów projektu), HIS (rozszerzenie licencji wybranych modułów), Zakażenia Szpitalne, Pulpit Lekarski i pielęgniarstwa
7.	SPZOZ Gryfice	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte), ERP	EDM, ZM (dostosowanie do wymogów projektu), HIS (rozszerzenie licencji wybranych modułów), Blok Porodowy, Rehabilitacja, Pulpit Lekarski i Pielęgniarski
8.	ZOL Tuczno	brak	ERP	EDM, ZM, HIS (dostawa i wdrożenie)
9.	WOMP Szczecin	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS, ERP	EDM, ZM (dostosowanie do wymogów projektu), Medycyna Pracy, Integracja HIS-RIS-PACS, e-rejestracja
10.	WOMP Koszalin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
11.	WSPR Szczecin	brak	brak	Partner nie realizuje usługi

				w projekcie ZEZ
12.	Willa Fortuna	brak	HIS	EDM, ZM, HIS (rozszerzenie licencji wybranych modułów), Przychodnia, eZLA, eZWM
13.	Stanomino	Partner posiada i wykorzystuje licencje na moduł EDM	EDM, HIS (Ruch Chorych, Lecznictwo otwarte)	EDM, ZM (dostosowanie do wymogów projektu), Integracja z LIS, Podpis Elektroniczny, e-ZLA, e-Skierowanie
14.	UMWZ	brak	brak	brak

7.6.2.2 Założenia

System umożliwia przekształcenie danych, rozproszonych w różnych systemach i aplikacjach, w informacje pozwalające na zdobycie wiedzy na temat kluczowych procesów oraz powiązań pomiędzy medyczną i finansową działalnością podmiotów, takich jak czas pobytu pacjenta, kompleksowość świadczeń, rehospitalizację.

Jest narzędziem wykorzystywanym do bieżącego operacyjnego zarządzania placówką zdrowotną, pozwala na monitorowanie kluczowych wskaźników wykorzystywanych do oceny sprawności operacyjną podmiotu, umożliwiając korygowanie działań zarządczych w newralgicznych punktach jego funkcjonowania – zarówno na najniższych szczeblach decyzyjnych (w tym nawet konkretnego lekarza i jego grupy pacjentów), jak w również w zarządzaniu centralnym.

System raportujący wspomaga zarządzanie w jednostkach ochrony zdrowia. System wspiera także decyzje z zakresu kreowania polityki zdrowotnej regionu z poziomu organu właścicielskiego.

System udostępnia funkcjonalność raportowania przekrojowych danych oraz ich pochodnych, dostępnych w systemach informatycznych jednostek ochrony zdrowia uczestniczących w projekcie, na różnych poziomach szczegółowości. Dane są prezentowane zarówno w formie zbiorczej, jak i na poziomie analitycznym.

Zapewnia interaktywny wybór każdego z analizowanych obszarów (oddział, rozpoznanie itp.) i powoduje każdorazową aktualizację wszystkich pulpitów wg wybranego kryterium.

Użytkownikami systemu analiz zarządczych będą pracownicy Partnerów Projektu, a także Wydziału Zdrowia Urzędu Marszałkowskiego Województwa Zachodniopomorskiego.

Aby osiągnąć planowany cel biznesowy zostanie wdrożony system klasy Business Intelligence. Systemy tej klasy umożliwiają zagregowanie danych rozproszonych w różnych systemach i aplikacjach i przetworzenie zgodnie z potrzebami analitycznymi/zarządczymi.

Wdrożony w ramach projektu system BI będzie służył między innymi do:

- 1) zdobycia wiedzy na temat struktury świadczeń,
- 2) czasu trwania procesów diagnostyczno-terapeutycznych,
- 3) monitorowania wskaźników efektywności organizacyjnej i ekonomicznej placówek opieki zdrowotnej.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 4) wspierania podejmowania decyzji dotyczących kreowania polityki zdrowotnej regionu przez UMWZ.

System Analiz Zarządczych będzie narzędziem wykorzystywanym do bieżącego operacyjnego zarządzania placówką zdrowotną przez Partnerów Projektu, a także do potrzeb sprawowania nadzoru ze strony podmiotu tworzącego przez WZ UMWZ.

System będzie posiadał funkcjonalność raportowania przekrojowych danych dostępnych w systemach informatycznych jednostek ochrony zdrowia, uczestniczących w projekcie, na różnych poziomach szczegółowości. Dane będą prezentowane w formie zbiorczej, jak i ujęciu szczegółowym.

Planuje się przygotowanie 18 rodzajów raportów w tym 7 raportów, których dane pochodzą z systemu ERP. Dane do pozostałych raportów będą pochodziły z systemów HIS i ERP.

Szacujemy, że ilość użytkowników systemów SAZ nie przekroczy 200 osób a systemu SAS do 5 użytkowników.

Wytypowano następujące profile użytkowników systemu SAZ Dyrektor, Ordynator, Pielęgniarka oddziałowa, Pracownik UMWZ. Profilom użytkowników będą przypisane określone kokpity pracownicze, które będą prezentowały dedykowane dla nich informacje.

7.6.2.3 Zakres prowadzonych analiz

System pozwala na przeprowadzenie wielowymiarowych analiz w następujących zakresach:

1. Medyczny – ogólny:

1) Analiza liczby wykonywanych hospitalizacji w szpitalu:

- a) na oddziałach,
- b) dla grup JGP,
- c) wg rozpoznań,
- d) wg lekarzy,
- e) w grupach wiekowych,
- f) w trybach przyjęć i wypisów.
- g) inne (możliwość rozszerzenia zgodnie z potrzebami SP ZOZ w oparciu o dane pochodzące z oprogramowania do statystyki medycznej i rozliczeń NFZ).

Możliwa jest analiza porównawcza szpitala wg:

- a) trybów przyjęć i wypisów,
- b) rozkładu liczby hospitalizacji w czasie wraz z możliwością zawężenia w oparciu o kryteria zawarte w punkcie 1), tj. np. rozpoznania, oddziały, grupy wiekowe itp.

2) Analiza poradni - w aspekcie liczby wykonywanych porad:

- a) w poradniach,
- b) dla produktów kontraktowych,
- c) rozpoznań,
- d) lekarzy,
- e) w grupach wiekowych.
- f) monitoring obciążenia lekarzy w oparciu o populację – struktura wiekowa, liczba wizyt pacjentów w zależności od wieku, koszty i struktura zleczanych badań diagnostycznych, przepływ pacjentów między lekarzami POZ.

Możliwa jest analiza również analiza rozkładu liczby porad w czasie.

2. Medyczny – szczegółowy:

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

- 1) Monitorowanie wybranych rodzajów świadczeń wraz z powiązaniem zużycia wybranych materiałów medycznych (np. endoprotezoplastyka).
 - 2) Benchmarking - porównanie wskaźników szpitala z innymi szpitalami z terenu województwa z możliwością porównania z podmiotami leczniczymi w innych regionach.
 - 3) Analiza wykorzystania łóżek w szpitalu oraz efektywność ich wykorzystania. Szacuje koszty nieefektywnych czasów pobytu w ujęciu szpitala i poszczególnych oddziałów. Odpowiada na pytanie, ile łóżek szpital lub poszczególne oddziały potrzebowałyby, gdyby czas pobytu pacjentów był optymalny.
 - 4) Analiza czasu pobytu pacjentów i ich odchyień od optymalnego poziomu.
 - 5) Analiza czasu pobytu pacjentów leczonych z danym rozpoznaniem, rozliczonych daną grupą JGP czy też prowadzonych przez danego lekarza.
 - 6) Analiza drogi pacjenta w podmiocie tj. jego leczenia w poszczególnych jednostkach organizacyjnych. Pozwala na analizę stosowania przez pacjentów zaleceń lekarzy związanych z różnymi formami terapii.
 - 7) Analiza hospitalizacji w wybranym przez użytkownika okresie od wypisania pacjenta z oddziału.
 - 8) Pozwala na identyfikację rehospitalizacji w momencie ponownego przyjęcia oraz analizę przyczyn powtórnego przyjęcia na oddział.
 - 9) Umożliwia śledzenie i analizę rehospitalizacji, informuje o wystąpieniu ponownej hospitalizacji przed upływem 14 dni od zakończenia leczenia na etapie przyjęcia Analiza czasu pobytu pacjentów i ich odchyień od optymalnego poziomu. Pozwala na analizę czasu pobytu pacjentów leczonych z danym rozpoznaniem, rozliczonych dana grupa JGP czy też prowadzonych przez danego lekarza.
 - 10) Monitorowanie wybranych rodzajów świadczeń wraz z powiązaniem zużycia wybranych materiałów medycznych (np. endoprotezoplastyka).
3. Finansowy:
- 1) Analiza wyników finansowych MPK, dynamiki kosztów i przychodów oraz prognoz wyników w okresie trzech lat, zarówno na poziomie centralnym (całego szpitala), jak i wybranych MPK.
 - 2) Analiza progów rentowności MPK oraz cen jednostkowych, dla których poszczególne MPK bilansowałyby swoją działalność operacyjną.
 - 3) Analiza kosztów jednostkowych w ujęciu punktów lub hospitalizowanego. Zawiera analizę struktury kosztów oraz dynamiki kosztu w stosunku do wzrostu liczby hospitalizacji lub punktów.
 - 4) Analiza kosztów MPK w ujęciu struktury kosztów, dynamiki w zakresie grupy, podgrupy i pojedynczych rodzajów kosztów.
 - 5) Analiza dynamiki kosztów MPK w ujęciu struktury kosztów, dynamiki w zakresie grupy, podgrupy i pojedynczych rodzajów kosztów.
 - 6) Symulacja wyników MPK w przypadku sfinansowania nadwykonań.
 - 7) Możliwość definiowania i monitorowania limitów wewnętrznych w ramach oddziałów i poradni objętych ryczałtem, a także monitorowania parametrów dodatkowych umożliwiających zwiększenie ryczałtu (np. odsetek porad).
 - 8) Monitorowanie środków trwałych dostępnych w ramach SP ZOZ oraz poszczególnych oddziałów – bardzo ważne w kontekście decyzji zakupowych.
 - 9) Symulacja wartości ryczałtu szpitala wchodzącego w skład sieci szpitali w przyszłych okresach rozliczeniowych. Obliczanie nowego ryczałtu dla szpitala wchodzącego w skład sieci szpitali.
 - 10) Symulacja zmian wartości ryczałtu w ramach Szpitalnego Oddziału Ratunkowego.
 - 11) Możliwość tworzenia symulacji wartości dla wybranych świadczeń pozaryczałtowych.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

7.6.2.4 Przykładowe elementy BI w zarządzaniu szpitalem

Na poziomie zarządzających placówkami Partnerów Projektu i Lidera Projektu będą dostępne pulpity o zróżnicowanym zakresie dostępu do danych analitycznych dla Dyrekcji, Pielęgniarek i innych wybranych grup zawodowych. Tworzenie pulpitu „na żądanie” będzie jedną z funkcjonalności systemu.

1. Sprawozdania wymagane przez Wydział Zdrowia Urzędu Marszałkowskiego Województwa Zachodniopomorskiego.

1) Dane finansowe:

- a) Raporty: Monitoring miesięczny, Informacja kwartalna z wynikami i danymi statystycznymi OPK, Majątek trwały w ujęciu miesięcznym i narastająco
- b) Raport o sytuacji ekonomiczno-finansowej – wskaźniki i oceny na podstawie sprawozdania, finansowego wraz z porównaniem z wprowadzonym planem finansowy,
- c) Plan finansowy w ujęciu Plan – Wykonanie – Odchylenie od planu,
- d) Program naprawczy – porównanie wykonania bieżącego z wartościami założonymi w programie,
- e) Rb-Z, Rb-N,
- f) Dane kadrowe:
 - liczba pracowników w poszczególnych grupach zawodowych wraz z możliwością filtrowania w wybranym zakresie danych,
 - wskaźniki absencji,
 - średnie wynagrodzenia z możliwością rozdziału składników wynagrodzenia i filtrowania w wybranym zakresie danych.
 - porównanie zatrudnienia z wymogami NFZ (głównie pielęgniarki i lekarze).
- g) Dane statystyczne i inne:
 - statystyki wykorzystania zasobów oddziałów i poradni np. liczba łóżek, obłożenie, średnie czasy leczenia, wiek pacjentów, itp.,
 - wskaźniki absencji,
 - raporty dla ośrodków medycyny pracy,
 - miejsce pochodzenia pacjentów wg powiatu/gminy zamieszkania (wraz z wyceną JGP),
 - kolejka medyczna wg poszczególnych zakresów działalności,
 - limity wykorzystania materiałów medycznych.
- h) Benchmarking - agregacja danych porównawczych Partnerów Projektu - System pozwoli na analizę zebranych w BI danych w zakresie. (Przykład: porównania kosztów procedur medycznych, długości pobytu pacjenta na oddziale dla podobnych jednostek).
- i) Wszystkie raporty i zestawienia przygotowane dla UMWZ (9.2.3 p.1.) będą zawierały tylko dane statystyczne i zostaną opracowane na podstawie danych zanonimizowanych.

2) Przykładowe elementy BI w zarządzaniu szpitalem.

Zgromadzone w BI lokalnym dane mogą być udostępniane różnym grupom zawodowym w postaci pulpitu, na którym użytkownik będzie miał przygotowane najbardziej oczekiwane

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

przez niego, zestawienia i raporty. System zapewni możliwość tworzenia pulpitu zgodnie z aktualnym zapotrzebowaniem użytkowników:

- a) Przykładowe rodzaje pulpitu:
 - Dyrekcja,
 - Ordynatorzy/pielęgniarki oddziałowe,
 - Kierownik apteki/laboratorium/innych wybranych pracowni.
- b) Analizy organizacyjno-logistyczne:
 - wizualizacja przepływu pacjentów (patient flow) – zarówno z perspektywy pojedynczego pacjenta, jak i statystyki globalne, identyfikacja wąskich gardeł,
 - limity wykorzystania materiałów medycznych – plan i wykonanie (dla Dyrektorów),
 - stopień wykorzystania poszczególnych komórek pomocniczych wraz z wizualizacją czasu ich wykorzystania (identyfikacja wolnych mocy przerobowych),
 - analizy dot. funkcjonowania SOR z uwzględnieniem czasu oczekiwania, wykonywanych procedur, dalszego postępowania z pacjentem (wypis, przyjęcie na oddział, itp.),
 - kolejki medyczne i czasy oczekiwania dla poszczególnych przypadków (wraz ze wskazaniem odchyleń, np. pozaplanowe przyjęcia),
 - monitoring grafików i nieobecności i odchyleń od nich,
 - raporty bieżące nt. obłożenia oddziałów (wraz z prognozami).
- c) Analizy medyczne/statystyka:
 - analizy trendów dla poszczególnych przypadków chorobowych,
 - statystyki wykonania badań i zadań pomocniczych wg komórek i rodzajów,
 - dane statystyczne w formie tabelarycznej oraz wykresów (możliwość filtracji w zależności od charakterystyki przypadków medycznych, wybranego okresu, trybu przyjęcia/wypisu).
 - analiza zgonów – wg Oddziałów, JGP, wieku,
 - elektroniczna księga dla bloku operacyjnego,
 - limity wykorzystania materiałów medycznych,
 - bieżący monitoring predefiniowanych limitów wewnętrznych dla ryczałtu w ramach sieci szpitali oraz ich bieżącego wykonania,
 - prognoza przychodów z NFZ na podstawie statystyk dot. rozpoznania i przeciętnego czasu trwania hospitalizacji aktualnie leczonych pacjentów,
 - migracje pacjentów (struktura geograficzna, podmioty kierujące).
- d) Kadrowe:
 - wskaźniki absencji z możliwością filtrowania – grupy zawodowe, oddziały, wyłączenie pracowników na zwolnieniach długoterminowych.

7.6.2.5 Źródła danych do analiz

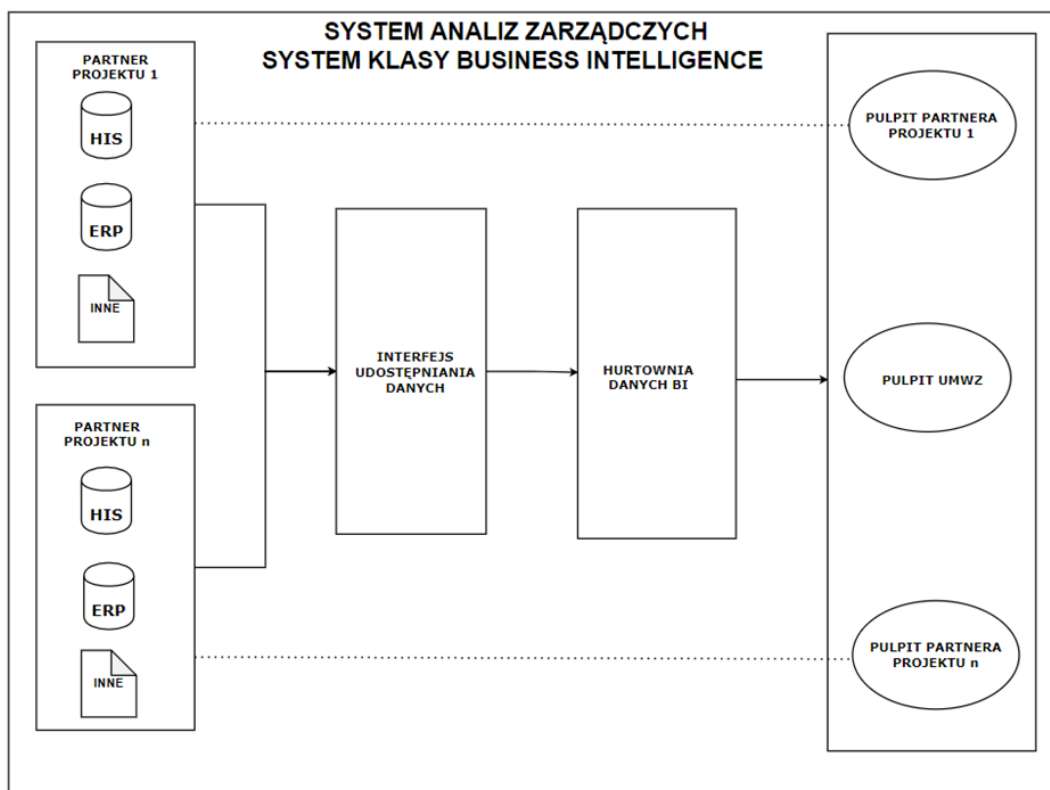
Dane będą pobierane z systemów dziedzinowych HIS i ERP Partnerów Projektu.

Przekazywanie danych będzie następowało przez interfejsy wymiany danych, które będą stale aktualizowane lub inny zaproponowany przez Wykonawcę systemu. W związku z tym, że dostawcy

systemów klasy BI mogą stosować różną architekturę związaną z gromadzeniem danych z systemów dziedzinowych, poniżej została przedstawiona informacja na temat wielkości baz danych.

Wielkość baz danych HIS i ERP (stan na 01.09.2021)

Lp.	Nazwa jednostki Partnera Projektu ZEZ	HIS	ERP
1.	Zachodniopomorskie Centrum Onkologii	160 GB	25 GB
2.	Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie,	870 GB	120 GB
3.	Samodzielny Publiczny Specjalistyczny Zakład Opieki Zdrowotnej „Zdroje” w Szczecinie	914 GB	16 GB
4.	Regionalny Szpital w Kołobrzegu	920 GB	55 GB
5.	Szpital Wojewódzki im. Mikołaja Kopernika w Koszalinie,	30 GB	200 GB
6.	Samodzielny Publiczny Specjalistyczny Zespół Gruźlicy i Chorób Płuc w Koszalinie,	44 GB	21 GB
7.	Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Gryficach,	380 GB	29 GB
8.	Zakład Opiekuńczo-Lecznicy Samodzielny Publiczny Zakład Opieki Zdrowotnej „Leśna Ustroń” w Tucznie	Brak HIS	1 GB
9.	Wojewódzki Ośrodek Medycyny Pracy – Zachodniopomorskie Centrum Leczenia i Profilaktyki	260 GB	60 GB
10.	Wojewódzki Ośrodek Medycyny Pracy w Koszalinie	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
11.	Wojewódzka Stacja Pogotowia Ratunkowego w Szczecinie	brak	20 GB
12.	Szpital Uzdrawiskowy „Willa Fortuna” Samodzielny Publiczny Zakład Opieki Zdrowotnej	40 GB	3 GB
13.	Samodzielny Publiczny Zakład Opieki Zdrowotnej Wojewódzki Ośrodek Terapii Uzależnienia od Alkoholu i Współuzależnienia w Stanominie	136 GB	12 GB



Rys. 20. Diagram: System Analiz Zarządczych SAZ

7.6.3 Platforma Zakupowa SPZOZ/Grupowe Zamówienia

7.6.3.1 Podstawa prawna

Nowa ustawa PZP⁹ wprowadziła pojęcie pomocniczych działań zakupowych.

Treść art. 37 ust. 3 Pzp zawiera definicję pomocniczych działań zakupowych polegających na zapewnieniu zamawiającemu wsparcia w związku z udzielaniem zamówienia lub organizacją konkursu. Pojęcie pomocniczych działań zakupowych Art. 37 Prawo zamówień publicznych zostało zaczerpnięte z art. 2 dyrektywy klasycznej. Działania te polegają na zapewnieniu wsparcia dla czynności podejmowanych przez zamawiającego w procesie planowania, przygotowania oraz przeprowadzenia postępowania o udzielenie zamówienia lub organizacji konkursu. Takie wsparcie może przybierać różnorodną formę.

Powierzenie pomocniczych działań zakupowych osobom trzecim następuje najczęściej na podstawie umowy lub dodatkowego pełnomocnictwa, co oznacza, że powinno zostać dokonane z zastosowaniem właściwych procedur przewidzianych w Pzp.

W świetle art. 37 ust. 2 Pzp, który zgodnie z dyspozycją art. 38 ust. 5 Pzp, możliwość przeprowadzenia jak również przygotowania takiego postępowania w imieniu wszystkich zamawiających, może zostać

⁹ Ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019)

powierzona przez zamawiających upoważnionemu przez nich pełnomocnikowi, będącemu osobą trzecią lub jednostką organizacyjną jednego z zamawiających.

W wyniku upoważnienia podmiotu trzeciego bądź jednego z zamawiających do przygotowania postępowania lub przeprowadzenia postępowania zamówienia publicznego w imieniu i na rzecz pozostałych zamawiających, tacy zamawiający nie tracą statusu „zamawiających”. Udzielenie upoważnienia w takiej sytuacji ma bowiem jedynie uzasadnienie organizacyjne i służy uzyskaniu formalnej podstawy do wykonywania przez upoważniony podmiot lub jednego z zamawiających czynności związanych z przygotowaniem lub przeprowadzeniem postępowania i udzieleniem zamówienia w imieniu i na rzecz pozostałych zamawiających.

Wspólne przeprowadzanie postępowania o udzielenie zamówienia lub konkursu nie zwalnia zamawiających z odpowiedzialności za jego przeprowadzenie. W przepisach art. 38 ust. 3 i 4 Pzp określone zostały zasady odpowiedzialności zamawiających w przypadku wspólnego przygotowywania lub przeprowadzania postępowania lub organizacji konkursu. Zamawiający odpowiadają wspólnie za zgodność postępowania lub konkursu z Pzp, w sytuacji przygotowania lub przeprowadzenia postępowania lub organizacji konkursu w całości dokonywanego przez nich zarówno wspólnie, jak również przez jednego z nich w imieniu i na rzecz wszystkich zamawiających. Oznacza to, że każdy zamawiający odpowiada za zgodność takiego postępowania lub konkursu z Pzp niezależnie od zakresu swoich obowiązków. Również wszyscy zamawiający ponoszą odpowiedzialność za zgodność z Pzp w zakresie części postępowania lub konkursu, która jest przygotowywana i prowadzona lub organizowana w imieniu i na rzecz wszystkich zamawiających w sytuacji, jeżeli postępowanie lub konkurs nie jest w całości przygotowywane i prowadzone lub organizowane w imieniu i na rzecz wszystkich zamawiających, tj. w przypadku ograniczenia współpracy do poszczególnych elementów.

7.6.3.2 Model gromadzenia danych

Model gromadzenia danych pod względem budowy będzie funkcjonował podobnie jak pozostałe sprawozdania i raporty.

Słowniki do modułu zamówień publicznych, będą tworzone na bieżąco z list zamówień od poszczególnych Partnerów. Każdy szpital posługuje się innym słownikiem, który budowany jest na bazie pojęć, które wynikają z poprzednich zakupów.

7.6.3.3 Dane dotyczące stopnia przygotowania Partnerów do realizacji e-usługi/funkcjonalności

Zamówienia wspólne				
Lp.	Nazwa jednostki/ stanowisko/funkcja w Projekcie	Stopień przygotowania do realizacji e-usługi	Posiadane moduły/systemy/podsystemy do realizacji e-usługi	Brakujące moduły/systemy/pod systemy do realizacji e-usługi
1.	ZCO	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych.	Zamówienia wspólne
2.	SPWSZ Arkońska	brak	Zamówienia produktów leczniczych i	Zamówienia wspólne

			<p>wyrobów medycznych jednoramowego użytku, jak również asortymentu niemedycznego odbywają się przy pomocy systemu informatycznego (elektroniczne zamówienie i realizacja).</p> <p>Leki (produkty lecznicze) zamawiane są przez jednostki medyczne (oddziały, poradnie, pracownie, bloki operacyjne i inne) w Aptece Szpitalnej,</p> <p>Pozostały asortyment w Dziale Zaopatrzenia. Baza dostępnego asortymentu tworzona jest praktycznie na bieżącą jako efekt zwartych umów na dostawy, przede wszystkim przetargowych.</p>	
3.	SPSZOZ Zdroje	brak	<p>Szpital posiada wewnętrzny moduł zamówień w ramach użytkowanego systemu HIS AMMS. Posiada 4 magazyny:- apteka - magazyn sprzętu medycznego - magazyn biurowy- magazyn techniczny</p> <p>Słowniki dla w/w magazynów tworzone są w dwojaki sposób:</p> <ul style="list-style-type: none"> - na podstawie faktur zakupowych (słownik tworzony przez użytkownika magazynu) - na podstawie zakupionego od firmy Kamsoft słownika BLOZ (leki). 	Zamówienia wspólne
4.	RS Kołobrzeg	brak	<p>Do zamówień na leki wykorzystuje się Receptariusz Szpitalny</p> <p>Zamówienia realizowane są za pośrednictwem dokumentów papierowych.</p>	Zamówienia wspólne
5.	SW Koszalin	brak	Brak systemu wspólnych zamówień	Zamówienia wspólne
6.	SZGiCHP Koszalin	brak	<p>Do zamówień na leki wykorzystuje się Receptariusz Szpitalny w MS Excel, Zamówienia realizowane są za pośrednictwem dokumentów papierowych.</p> <p>Wydania z modułu magazyn Impulse.</p> <p>Wydania z modułu magazyn Impulse.</p> <p>Wydania leków z modułu Apteka Eskulap</p> <p>Słownik tworzy się na podstawie bieżących zakupów.</p>	Zamówienia wspólne
7.	SPZOZ Gryfice	brak	Brak systemu wspólnych zamówień	Zamówienia wspólne

8.	ZOL Tuczno	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych	Zamówienia wspólne
9.	WOMP Szczecin	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych	Zamówienia wspólne
10.	WOMP Koszalin	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych	Zamówienia wspólne
11.	WSPR Szczecin	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ
12.	Willa Fortuna	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych	Zamówienia wspólne
13.	Stanomino	brak	Zamówienia realizowane są za pośrednictwem dokumentów papierowych	Zamówienia wspólne
14.	UMWZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ	Partner nie realizuje usługi w projekcie ZEZ

7.7 Zbiorcze zestawienie e-usług

<i>Nazwa e-usługi</i>	<i>Opis e-usługi</i>	<i>Poziom dojrzałości e- usług</i>	<i>Nazwa funkcjonalności</i>
e-Rejestracja	Umożliwia rejestrację drogą elektroniczną na usługi medyczne realizowane przez podmioty lecznicze	5	e-Rejestracja
EDM	Umożliwia wymianę elektronicznej dokumentacji medycznej pomiędzy podmiotami leczniczymi co pozwoli na dostęp do dokumentacji medycznej pacjentowi oraz pracownikom medycznym	4	EDM dla lekarza
		4	EDM dla pacjenta
e-Dzienniczek pacjenta	Komunikacja i wymiana informacji między pacjentem/lekarzem w procesie zdalnego leczenia i rehabilitacji	4	e-Dzienniczek pacjenta
Portal Projektu ZeZ	Portal zawierający aktualności, informacje o Projekcie oraz podmiotach leczniczych biorących udział w Projekcie, ankiety dotyczące poziomu jakości świadczenia usług przez podmioty lecznicze oraz satysfakcji pacjentów	1	Portal Projektu ZeZ
Systemy Analityczne	Gromadzenie z nadzorowanych podmiotów leczniczych danych statystycznych i zarządczych oraz zamówienia grupowe	Nie dotyczy	SAS/SAZ /zamówienia

8. Zasady komunikacji dla usług e-Rejestracji i EDM

8.1 Zasady komunikacji - e-Rejestracja lokalna

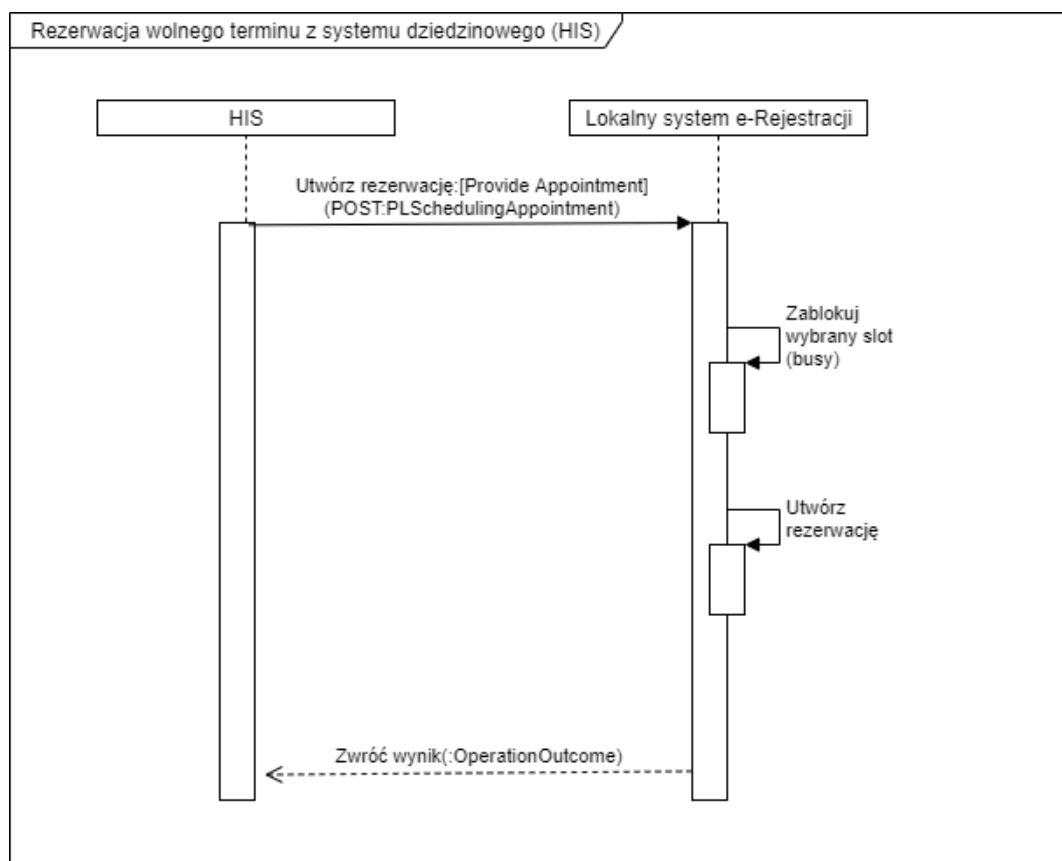
Komunikacja w ramach modułu e-Rejestracja została zaprezentowana na poniższych diagramach.

Rekomendowane jest zastosowanie standardu HL7 FHIR, planowanego do wykorzystania w ramach Systemu P1.

Zasady komunikacji dla e-Rejestracji Centralnej muszą być zgodne z takimi, jakie będą określone przez MZ/CeZ w dokumentacji integracyjnej..

8.1.1 Transakcja rezerwacji wolnego terminu dokonana z poziomu systemu HIS:

- 1) rezerwacja dokonywana jest w sposób dotychczasowy na poziomie systemu HIS i zapisywana w bazie systemu HIS,
- 2) informacja o zarezerwowaniu wizyty przekazywana jest do modułu systemu e-Rezerwacji dostępnej na stronie internetowej i przekazywana jest za pomocą podsystemu e-Powiadomienia pacjentowi,
- 3) pacjent ma dostęp do swoich rezerwacji za pośrednictwem własnego konta w systemie lokalnej e-rejestracji na stronie www Partnera Projektu:.



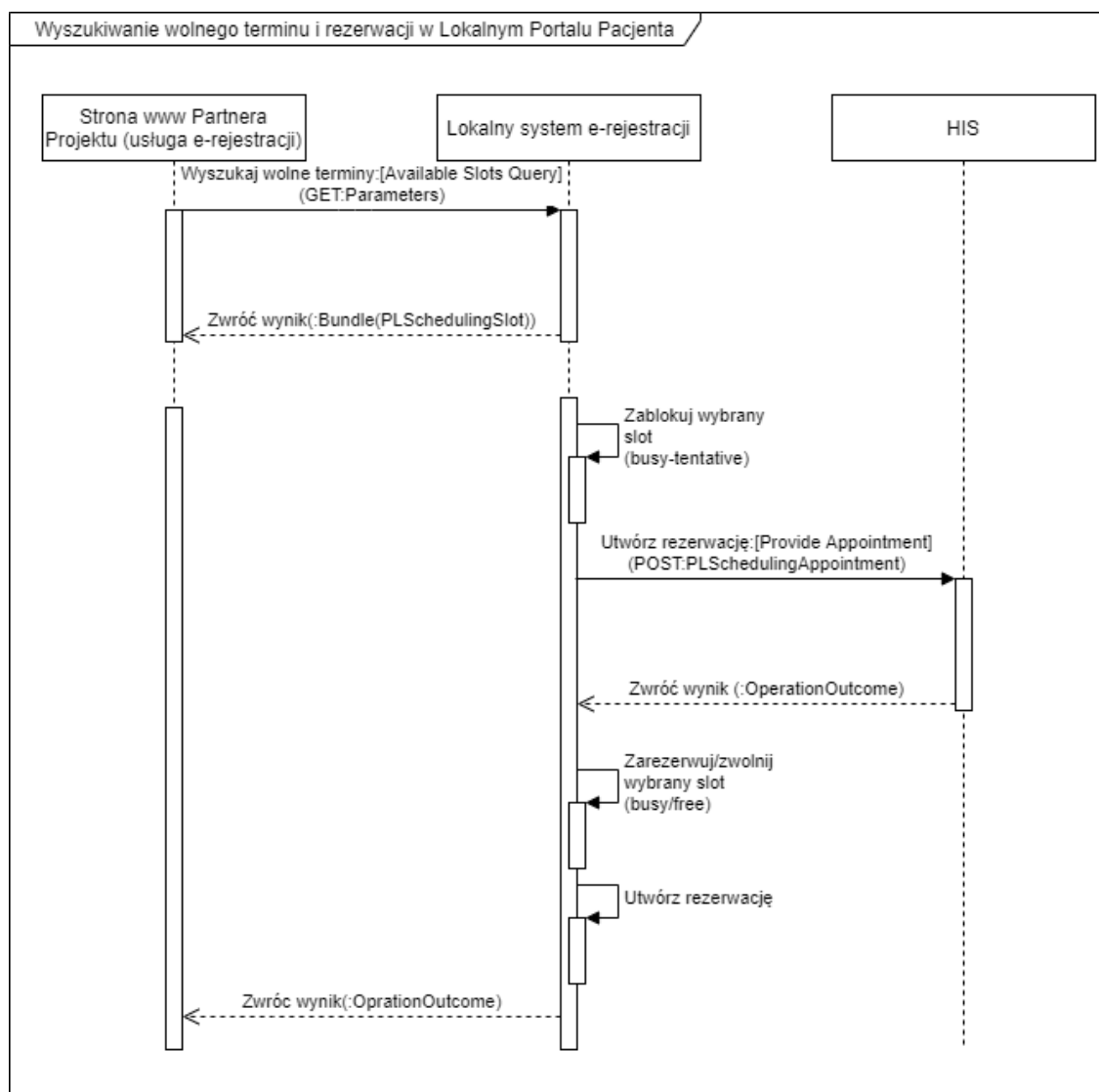
Rys. 21. Diagram: Rezerwacja wolnego terminu dokonana z poziomu systemu HIS

8.1.2 Transakcja wyszukiwania wolnego terminu dokonana z poziomu strony www Partnera Projektu:

- 1) transakcja odbywa się za pomocą operacji Available Slots Query, zgodnej ze standardem HL7 FHIR i standardowej operacji Search RESTful API (<http://hl7.org/fhir/search.html>),
- 2) moduł e-Rejestracji wysyła sekwencyjnie zapytanie do lokalnego systemu HIS w podmiocie leczniczym, w którym zdefiniowana jest usługa, na którą pacjent chce się zarejestrować,
- 3) w odpowiedzi otrzymuje z systemu HIS zasób Bundle zawierający listę dostępnych terminów.

8.1.3 Transakcja rezerwacji wolnego terminu dokonana z poziomu strony www Partnera Projektu:

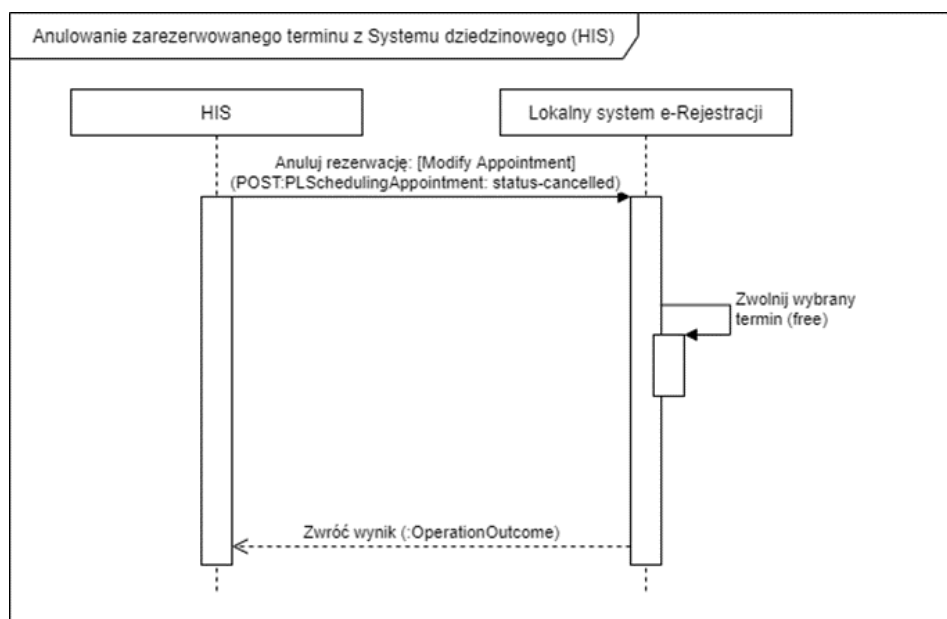
- 1) transakcja odbywa się za pomocą operacji Provide Appointment, zgodnej ze standardem HL7 FHIR i standardowej operacji POST RESTful API,
- 2) moduł e-Rejestracji wysyła zapytanie do systemu HIS,
- 3) System HIS blokuje wybrany termin i tworzy nową rezerwację,
- 4) odpowiedź jest propagowana przez system HIS do modułu e-Rejestracji .



Rys. 22. Diagram: Rezerwacja wolnego terminu ze strony www podmiotu leczniczego

8.1.4 Transakcja anulowania zarezerwowanego terminu dokonana z poziomu HIS:

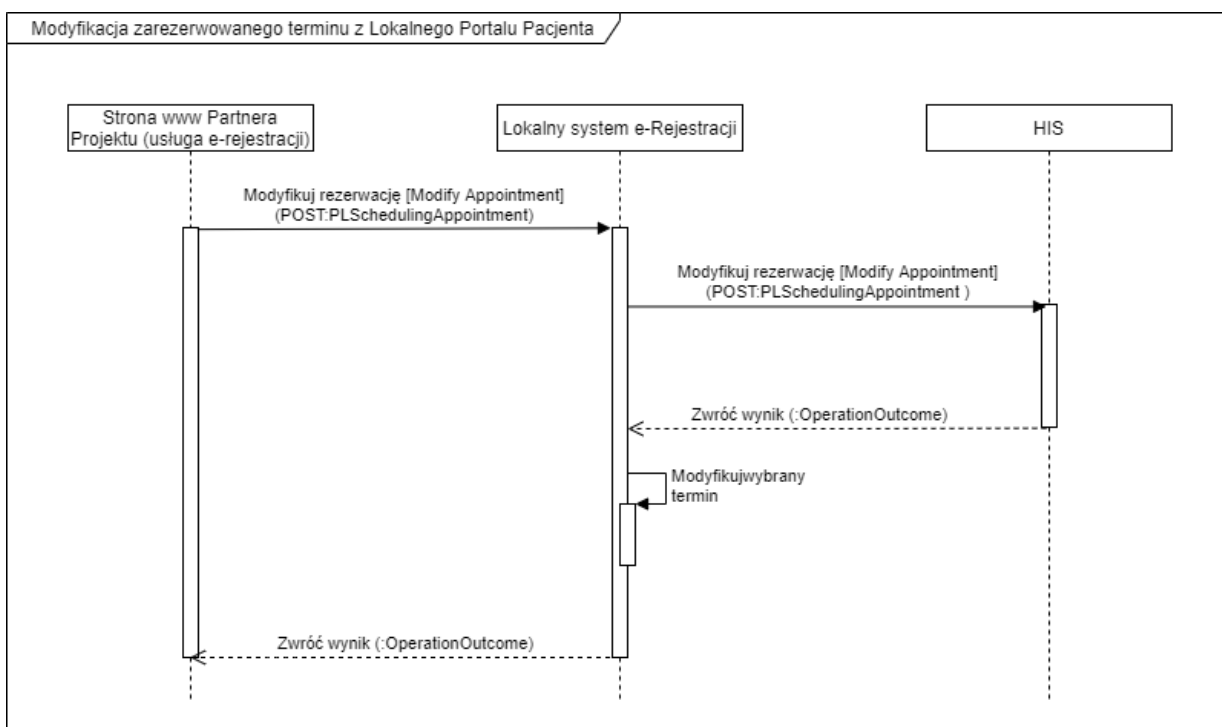
- 1) transakcja odbywa się w lokalnej bazie danych HIS,
- 2) następnie system HIS za pomocą operacji Modify Appointment, zgodnej ze standardem HL7 FHIR i standardowej operacji POST RESTful API przesyła informację o anulowaniu terminu do Lokalnego systemu e-Rejestracja,
- 3) Lokalny system e-Rejestracja anuluje obiekt rezerwacja i potwierdza to zwrotnie do systemu HIS oraz za pośrednictwem systemu e-Powiadomienia przesyła powiadomienie do pacjenta.



Rys. 23. Diagram: Anulowanie zarezerwowanego terminu z systemu HIS

8.1.5 Transakcja anulowania zarezerwowanego terminu dokonana z poziomu strony www Partnera Projektu:

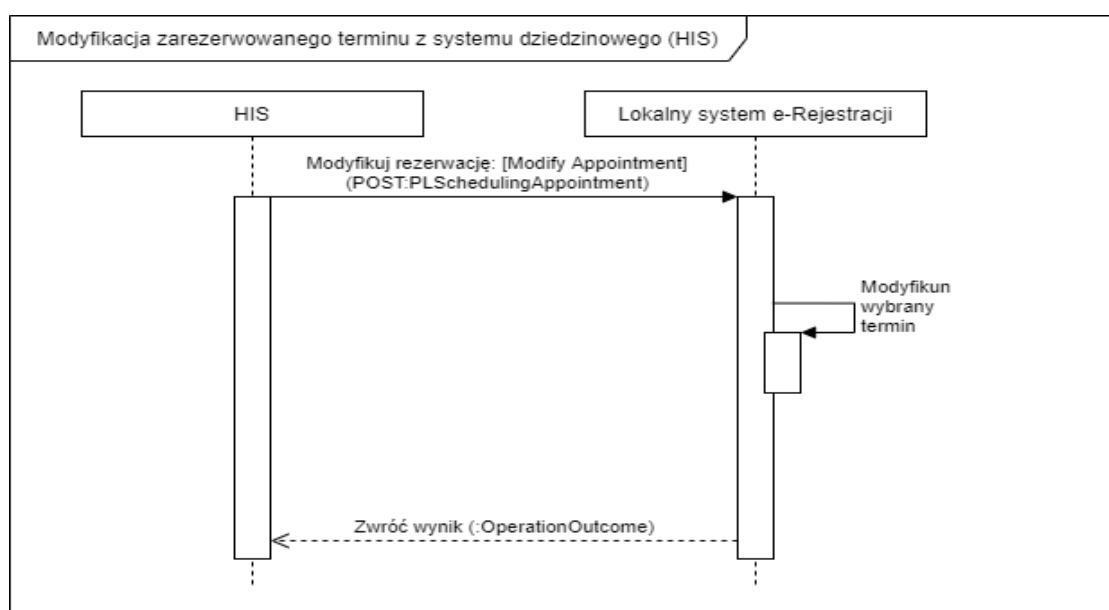
- 1) transakcja odbywa się za pomocą operacji Modify Appointment, zgodnej ze standardem HL7 FHIR i standardowej operacji POST RESTful API,
- 2) moduł e-Rejestracji przesyła zapytanie do systemu HIS, który zwalnia termin,
- 3) po zwolnieniu terminu następuje usunięcie terminu.



Rys. 24. Diagram: Anulowanie zarezerwowanego terminu z Portalu Pacjenta

8.1.6 Transakcja modyfikacji zarezerwowanego terminu dokonana z poziomu HIS:

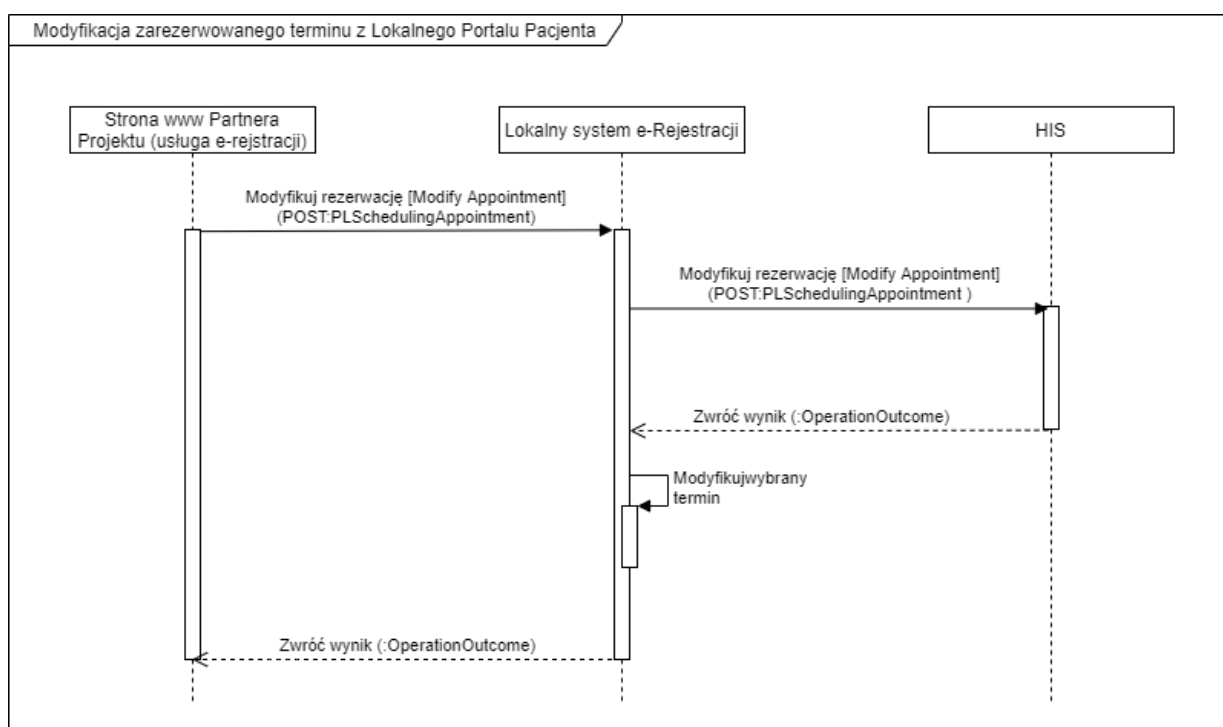
- 1) transakcja odbywa się za pomocą operacji Modify Appointment, zgodnej ze standardem HL7 FHIR i standardowej operacji POST RESTful API,
- 2) moduł e-Rejestracji przesyła zapytanie do systemu HIS,
- 3) system HIS modyfikuje zarezerwowany wcześniej zasób oraz propaguje odpowiedź do systemu lokalnego.



Rys. 25. Diagram: Modyfikacja zarezerwowanego terminu z systemu HIS

8.1.7 Transakcja modyfikacji zarezerwowanego terminu dokonana z poziomu strony www Partnera Projektu:

- 1) transakcja odbywa się za pomocą operacji Modify Appointment, zgodnej ze standardem HL7 FHIR i standardowej operacji POST RESTful API,
- 2) moduł e-Rejestracji przesyła zapytanie do systemu HIS,
- 3) system HIS modyfikuje zarezerwowany wcześniej zasób oraz propaguje odpowiedź do modułu e-Rejestracji.



Rys. 26. Diagram: Modyfikacja zarezerwowanego terminu

8.2 Zasady komunikacji - Elektroniczna Dokumentacja Medyczna

Komunikacja w ramach obszaru została zaprezentowana na poniższych diagramach. Dla uproszczenia, na diagramach pominięto wywołania transakcji ITI-20 Record Audit Event. Transakcja ta musi występować we wszystkich transakcjach zarówno wywoływana przez komponent w roli klienta jak i serwera chyba, że w profilu IHE opisującym daną transakcję wskazano inaczej. W przypadku komunikacji z systemem P1 konieczne jest wywoływanie transakcji ITI-20 udostępnianej przez system P1.

8.2.1 Wyszukanie dokumentu medycznego przez Pracownika Medycznego (PM) z poziomu systemu HIS podmiotu należącego do Projektu

Celem procesu jest zaprezentowanie pracownikowi medycznemu listy dokumentów pochodzących z innego podmiotu leczniczego możliwych do pobrania zgodnie z jego uprawnieniami

System HIS wyszukuje dokumenty pacjenta:

- 1) wysyła żądanie wydania tokena SAML w celu uwierzytelnienia dalszej komunikacji z platformą P1,
- 2) wysyła zapytanie ITI-18 Registry Stored Query do Rejestru Dokumentów w domenie krajowej XDS.b. systemu P1, deklarując przy tym tryb dostępu

Rejestr Dokumentów XDS.b P1:

- 1) wysyła zapytanie o dostęp do Modułu polityk dostępu i zgód SOZ P1,

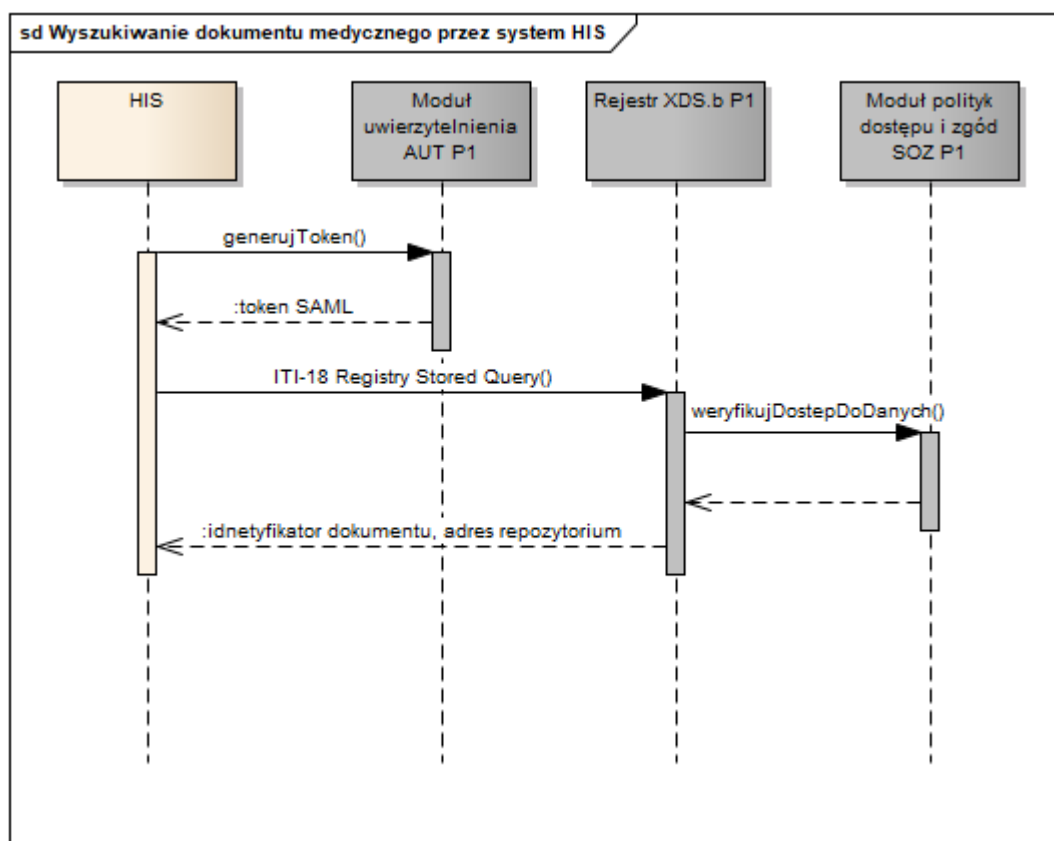
Moduł polityk dostępu i zgód SOZ P1 na podstawie zawartości zapytania:

- 1) weryfikuje prawo dostępu do dokumentu na podstawie zadeklarowanego trybu i ew. zgody,

Rejestr Dokumentów XDS.b:

- 1) uwzględnia dostęp i odsyła do systemu HIS listę identyfikatorów dokumentów wraz z identyfikatorami repozytoriów w których zapisany jest dokument.

System HIS: Prezentuje listę dokumentów PM.



Rys. 27. Diagram: Pobranie dokumentu medycznego przez HIS

8.2.2 Pobranie dokumentu przez Pracownika Medycznego (PM) z poziomu systemu HIS podmiotu należącego do Projektu

Celem procesu jest dostarczenie PM dokumentu i umożliwienie zapoznania się z treścią lub dołączenia do historii choroby pacjenta. Proces rozpoczyna się od wybrania przez PM dokumentu do pobrania z listy zaprezentowanej przez system HIS.

System HIS:

- 1) wysyła żądanie wydania tokena SAML w celu uwierzytelnienia dalszej komunikacji z platformą P1,
- 2) wysyła żądanie ITI-43 Retrieve Document Set do Repozytorium EDM w którym zapisany jest dokument, podając przy tym token SAML oraz deklarując tryb dostępu.

Repozytorium EDM (w innym podmiocie):

wysyła żądanie potwierdzające dostęp do Modułu polityk dostępu i zgód SOZ P1.

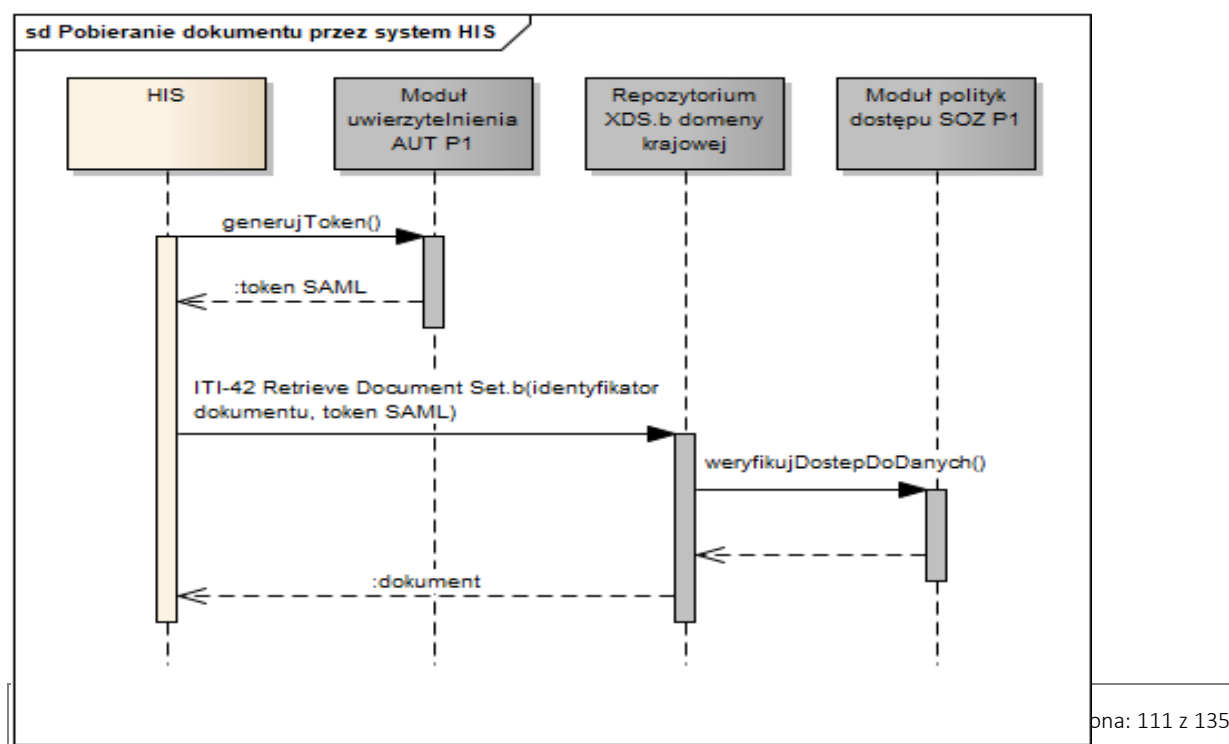
Moduł polityk dostępu i zgód SOZ P1 na podstawie zawartości zapytania: weryfikuje prawo dostępu do dokumentu na podstawie zadeklarowanego trybu i ew. zgody.

Repozytorium EDM:

przesyła dokument zgodnie z otrzymanym dostępem

System HIS:

prezentuje dokument PM lub zapisuje go we własnym repozytorium EDM (Lokalnym Repozytorium EDM).



Rys. 28. Diagram: Pobranie dokumentu medycznego przez HIS

8.2.3 Dodanie dokumentu medycznego przez Pracownika Medycznego (PM) z poziomu systemu HIS

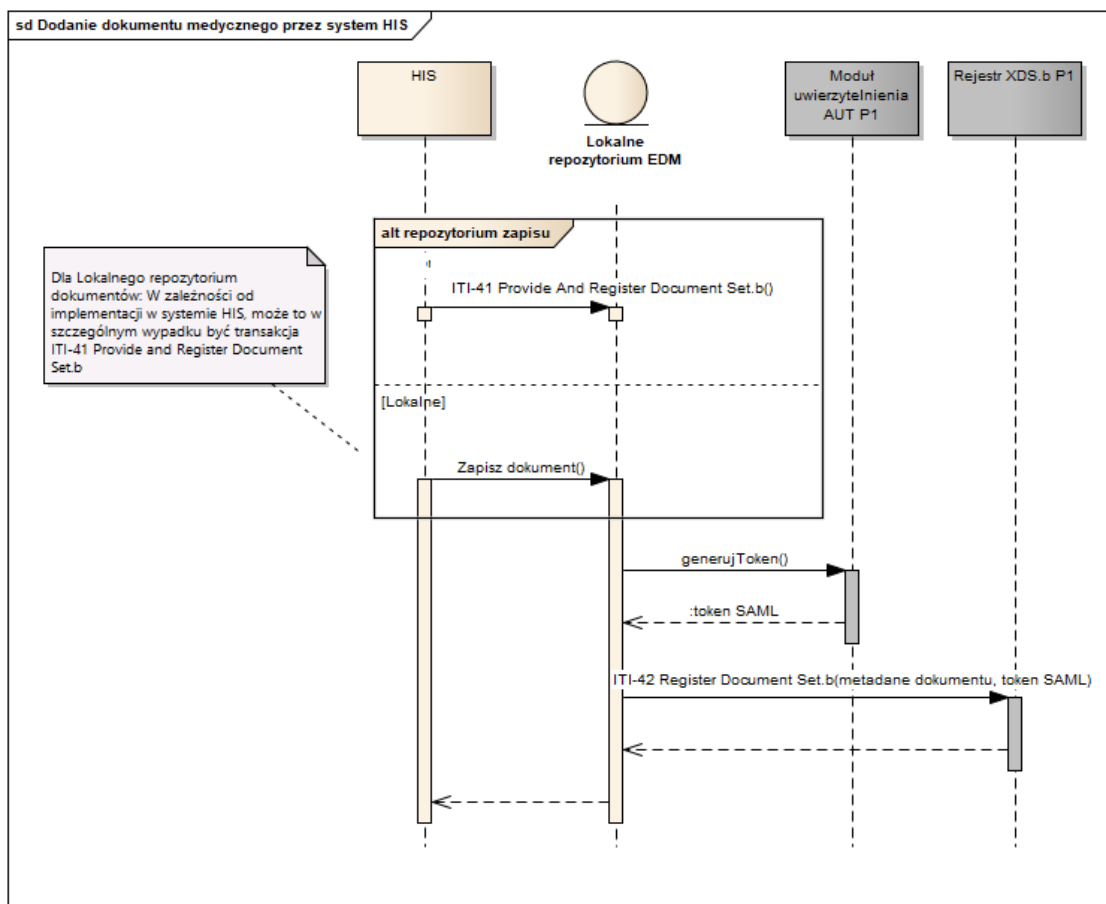
Celem procesu jest dodanie dokumentu medycznego do repozytorium i zaindeksowanie zgodnie z przyjętą polityką indeksowania.

System HIS:

- 1) wytwarza dokument zgodnie ze standardem HL7 CDA,
- 2) PM autoryzuje dokument zgodnie z przyjętą polityką z poziomu systemu HIS,
- 3) wysyła żądanie:
 - a) Zapisania dokumentu – do Lokalnego repozytorium EDM (w szczególności może to być ITI-41 Provide Document Set.b dla wewnętrznej komunikacji HIS zgodnej z IHE XDS.b),
lub
 - b) ITI-41 Provide Document Set.b – do Regionalnego repozytorium EDM, jeśli Partner nie posiada Lokalnego repozytorium EDM do Lokalnego Repozytorium EDM żądanie Provide and Register Document Set.

Lokalne Repozytorium EDM:

- 1) zapisuje dokument,
- 2) wysyła żądanie o token SAML w celu uwierzytelnienia dalszej komunikacji z platformą P1,
- 3) wysyła do Rejestru Dokumentów na platformie P1 żądanie ITI-42 Register Document Set.b.



Rys. 29. Diagram: Dodanie dokumentu medycznego przez HIS

8.2.4 Dodanie dokumentu medycznego wytworzonego przez e-Uслуги

Celem procesu jest dodanie dokumentu medycznego wytworzonego przez e-Uслуги (e-Dzienniczek pacjenta) do repozytorium i zaindeksowanie zgodnie z przyjętą polityką indeksowania.

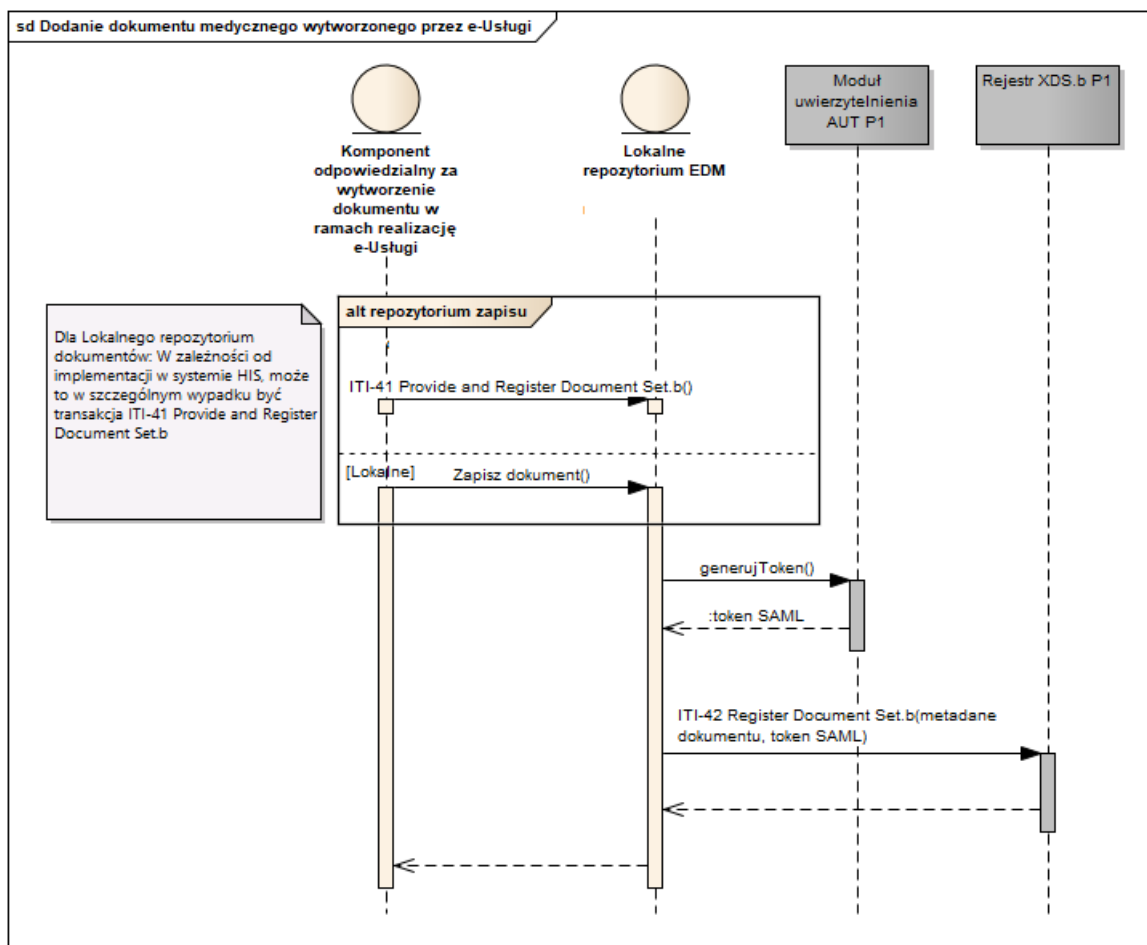
e-Usluga:

- 1) wytwarza dokument zgodnie ze standardem HL7 CDA,
- 2) wysyła do Lokalnego Repozytorium EDM żądanie ITI-41 Provide and Register Document Set.b.

Lokalne Repozytorium EDM:

- 1) zapisuje dokument,
- 2) wysyła do Krajowego Rejestru Dokumentów żądanie Register Document Set.b.

Rejestr Krajowy: rejestruje dokument.



Rys. 30. Diagram: Dodanie dokumentu medycznego wytworzonego przez e-Uslugi

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

9. Architektura infrastruktury teleinformatycznej

9.1 Warstwa regionalna – założenia projektowe

Przedstawione rekomendacje mają za zadanie dokonać skwantyfikowania dotyczącego zakładanego poziomu korzystania z e-usług w Projekcie przez pacjentów oraz pozostałych interesariuszy. W chwili obecnej nie jest dostępny przekrojowy raport dotyczący analizy wykorzystania e-usług w ochronie zdrowia, w tym ukazujący tendencje wzrostowe w zapotrzebowaniu na e-usługi zdrowotne.

Dostępne raporty:

- 1) Raport CSiOZ: Badanie stopnia informatyzacji podmiotów wykonujących działalność leczniczą, III edycja. Warszawa, czerwiec 2018,
- 2) Raport NIK: System Ochrony Zdrowia W Polsce – Stan Obecny i Pożądane Kierunki Zmian Warszawa maj 2019,
- 3) Raport MZ i NFZ z badania satysfakcji pacjentów korzystających z teleporad u lekarza podstawowej opieki zdrowotnej w okresie epidemii COVID-19. Warszawa sierpień 2020.

Ostatni z raportów ukazuje tendencje w wykorzystaniu e-usług już w stanie pandemii. Okazuje się, że spośród e-usług największą popularność zyskały teleporady – skorzystało ok. 80% ankietowanych co jest wynikiem szerokiej dostępności w okresie pandemii tej formy świadczenia usług. Natomiast mniejszym powodzeniem cieszy się e-rejestracja, z której skorzystało zaledwie 2 proc. ankietowanych co jest wynikiem ograniczonej dostępności tej e-usługi w badanej próbie pacjentów. Mając na uwadze następujące czynniki: zwiększenie dostępności e-usług oraz sytuację pandemiczną wymuszającą ograniczenie bezpośredniego kontaktu z placówką zdrowia do niezbędnego minimum, oraz wyniki ww. raportu MZ /NFZ, przyjęto jako podstawę do szacowania liczby pacjentów korzystających z e-usług wskaźnik wynoszący 1/3 ogółu pacjentów, którzy zapisali się na porady w placówkach ochrony zdrowia będących partnerami w Projekcie. Za punkt wyjścia przyjęto łączną liczbę pacjentów ambulatoryjnych we wszystkich podmiotach biorących udział w Projekcie w skali roku wynoszącą: ok. 1 500 tys. Jako wartość wskaźnika: liczba świadczonych e-usług w Projekcie, w szacowaniu kosztów realizacji usługi w analizie procesów biznesowych przyjęto 500 tys. świadczonych usług o różnym charakterze: e-Rejestracja, EDM dla pacjenta, EDM dla lekarza.

Według dostępnych danych z 2018 r. poniżej przedstawiono ilości pacjentów ambulatoryjnych oraz stacjonarnych wynoszących 1.3 mln tylko w podmiotach uczestniczących w ZeZ.

Podmiot	Liczba pacjentów ambulatoryjnych w skali roku	Liczba pacjentów stacjonarnych w skali roku
1. Zachodniopomorskie Centrum Onkologii w Szczecinie	104 608	12 994
2. Samodzielny Publiczny Wojewódzki Szpital Zespolony w Szczecinie	240 085	31 125
	34 599	16 726
3. Samodzielny Publiczny Zakład Opieki Zdrowotnej „Zdroje	170 000	30 000

4. Wojewódzka Stacja Pogotowia Ratunkowego	nie dotyczy	nie dotyczy
5. Wojewódzki Ośrodek Medycyny Pracy - Zachodniopomorskie Centrum Leczenia i Profilaktyki	72 621	0
6. Samodzielny Publiczny Zespół Zakładów Opieki Zdrowotnej w Gryficach	96 974	33 981
7. Szpital Wojewódzki w Koszalinie im. Mikołaja Kopernika	230 813	62 041
8. Specjalistyczny Zespół Gruźlicy i Chorób Płuc w Koszalinie	25 027	3 395
9. Regionalny Szpital w Kołobrzegu	102 386	16 499
10. SP ZOZ Woj. Ośrodek Terapii Uzależnienia od Alkoholu i Współuzależnienia w Stanominie	1 419	821
11. Szpital Uzdrowski "Willa Fortuna"- Samodzielny Publiczny Zakład Opieki Zdrowotnej w Kołobrzegu	brak	2 000
12. Zakład Opiekuńczo-Leczniczy SP ZOZ "Leśna Ustroń" w Tucznie	0	1 200
13. Wojewódzki Ośrodek Medycyny Pracy w Koszalinie	19 400	nie dotyczy
RAZEM	1 097 932	210 782

Powyższe dane posłużyły jako założenia projektowe do określenia liczby potencjalnych użytkowników e-usług, a w konsekwencji do oszacowania wydajności oraz skalowalności planowanych rozwiązań.

Planowane komponenty w warstwie regionalnej:

- 1) Portal Projektu ZEZ
- 2) Regionalne repozytorium EDM
- 3) Regionalny kontroler polityki dostępu,
- 4) Walidator dokumentów,
- 5) Regionalne repozytorium zdarzeń na potrzeby audytu,
- 6) Moduł Uwierzytelniania i autoryzacji,
- 7) System Analizy Sprawozdawczej (SAS),
- 8) System Analiz Zarządczych (SAZ/BI),
- 9) Platforma Zakupowa SPZOZ,
- 10) Panel administracyjny.

9.1.1 Opis rozwiązania

Wdrożenie e-Usług wynikających z Architektury funkcjonalnej Systemu ZeZ wymusza konieczność utworzenia na szczeblu regionalnym dedykowanego Centrum Przetwarzania Danych, którego zadaniem jest między innymi dostarczanie funkcjonalności tych usług. Do sprawnego działania centrum wymagane jest posiadanie na poziomie regionalnym odpowiednio wydajnej infrastruktury sieci teleinformatycznej.

W związku z realizacją Projektu zostanie zakupiona cała infrastruktura informatyczna dla części regionalnej, niezbędna do jej uruchomienia i eksploatacji w okresie trwałości. Dotyczy to w szczególności serwerowni - Głównego Centrum Przetwarzania Danych GCPD (serwery z oprogramowaniem systemowym i narzędziowym, pamięci masowe, urządzenia archiwizujące, urządzenia transmisji danych, UTM/firewalle) umiejscowione w Lokalizacji nr 1 - nowo budowanej siedzibie Urzędu Marszałkowskiego przy ul. Piłsudskiego 40.

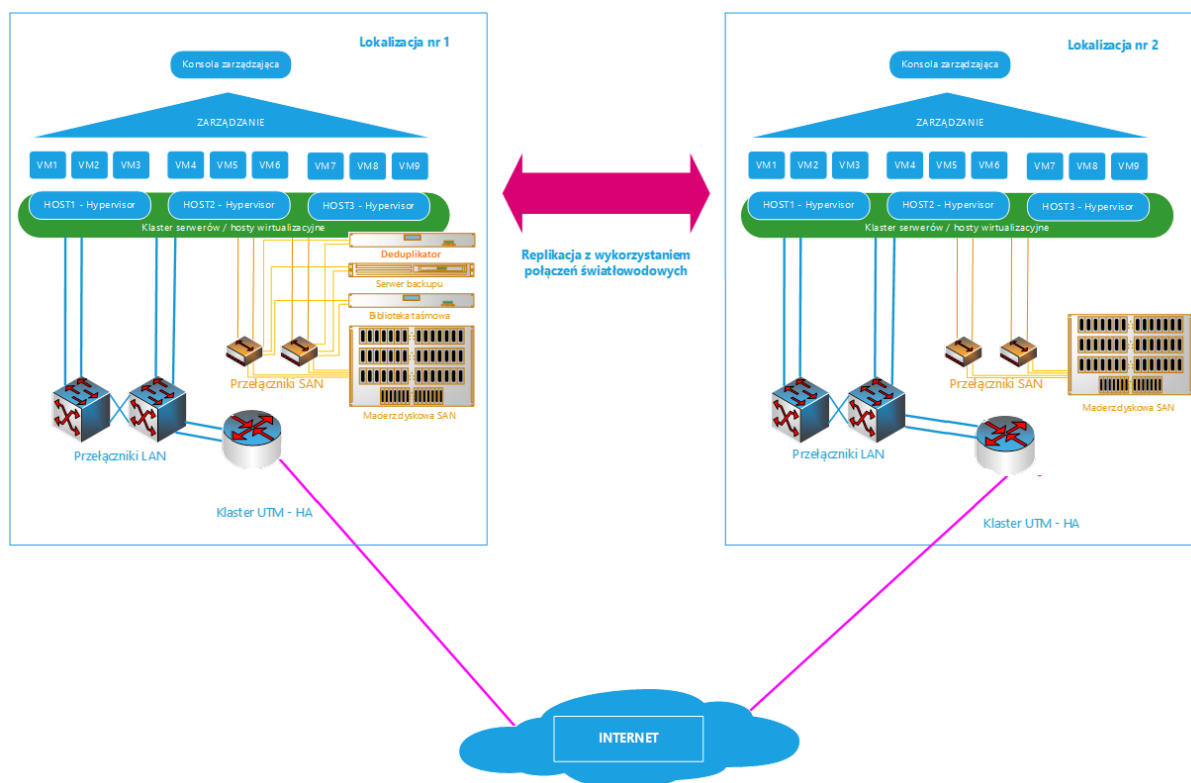
Lokalizacja nr 2 GCPD powinna być umiejscowiona w takiej serwerowni, aby umożliwić konfigurację klastra wysokodostępowego w trybie active-active. Aby zapewnić tryb HA, a jednocześnie zabezpieczyć środowisko przed zagrożeniami występującymi lokalnie, druga Lokalizacja GCPD powinna być oddalona max 40 km od pierwszej i powinna być z nią połączona dedykowanym światłowodem. Serwerownia zapasowa zlokalizowana będzie w odległości ok. 100 m od GCPD zlokalizowanego w innej części Urzędu Marszałkowskiego przy ul. Piłsudskiego.40

Biuro eksploatacji Lidera w zależności od modelu będzie zarządzać infrastrukturą serwerowni w warstwie sprzętowej i aplikacyjnej lub dla zewnętrznej lokalizacji, wyłącznie w warstwie aplikacyjnej.

Zadaniem części regionalnej jest zbieranie dokumentacji medycznej wytworzonej w systemach lokalnych. Repozytorium regionalne powinno spełniać wszystkie wymagania stawiane dla repozytoriów lokalnych, z którymi komunikacja powinna odbywać się automatycznie po wydzielonych, szyfrowanych łączach przy wykorzystaniu urządzeń umożliwiających zestawienie połączeń VPN lub innego bezpiecznego kanału komunikacji.

Głównym założeniem takiego repozytorium jest zarówno bezpieczne przechowywanie danych wytworzonych w jednostkach lokalnych, ale również udostępnianie dokumentacji pomiędzy poszczególnymi jednostkami. Jest to następstwem wymaganego prawnie zachowania ciągłości leczenia pacjenta. Repozytorium powinno pozwalać na dostęp do dokumentów pacjenta, który wyraził zgodę na udostępnianie jego dokumentów za pośrednictwem repozytorium regionalnego pozostałym podmiotom leczniczym łączącym się z repozytorium.

Przygotowano rozwiązanie tradycyjne oparte na serwerach wirtualizacyjnych oraz macierzach dyskowych do przechowywania danych,



Rys. 31. Schemat topologii sieci przy rozwiązaniu tradycyjnym

Serwery

Optymalnym rozwiązaniem w Głównym Centrum Przetwarzania Danych (GCPD) – będzie budowa rozproszonego klastra niezawodnościowo-wydajnościowego, czyli instalacja środowiska wirtualnego na sześciu serwerach hostujących maszyny wirtualne, z czego trzy serwery będą znajdowały się w Lokalizacji nr 1, natomiast trzy pozostałe serwery w Lokalizacji nr 2. Dodatkowo elementem wchodzącym w skład klastra będzie zdublowana macierz dyskowa, replikująca dane synchronicznie oraz udostępniająca je w obu lokalizacjach jednocześnie (metrocluster).

Zakupione serwery zostaną połączone w klaster, który posłuży do obsługi wielu serwerów/maszyn wirtualnych VM zapewniając im odpowiedni poziom wydajności nawet w przypadku awarii, lub niedostępności, jednej z lokalizacji (Nr 1 lub Nr 2).

Ciągła dostępność dla serwera wirtualnego VM zostanie zapewniona poprzez utworzenie i uruchomienie kopii maszyny wirtualnej VM (która jest identyczna i stale dostępna) w drugiej lokalizacji, tak aby móc zastąpić podstawową w przypadku awarii. Podstawowa maszyna wirtualna VM jest w sposób ciągły replikowana do maszyny wirtualnej VM w drugiej lokalizacji, dzięki czemu kopia maszyny wirtualnej VM może przejąć ją w dowolnym momencie, zapewniając w ten sposób ochronę przed awariami.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

W stworzonym środowisku zostanie uruchomione Repozytorium Regionalne EDM jak również wszystkie usługi towarzyszące niezbędne do poprawnej pracy systemu. Konfiguracja klastra serwerów musi spełniać nie tylko wymagania narzucane przez oprogramowanie, które będzie używane. Z uwagi na fakt, że oprogramowanie do zarządzania będzie używane przez wielu użytkowników, serwer musi mieć odpowiednio dużą wydajność – szybkie wielordzeniowe procesory oraz dużą ilość pamięci są w tym przypadku szczególnie wskazane. Duża ilość pamięci RAM przewidziana do serwerów zapewni wzmocnienie klastra i tym samym podniesienie wydajności.

Zgodnie z powyższym Infrastruktura serwerowa od strony technicznej będzie redundantna w postaci zwirtualizowanych serwerów pracujących w klastrze niezawodnościowo-wydajnościowym HA.

Macierze

Macierze dyskowe będą pod względem parametrów będą identyczne w obu lokalizacjach. W rozwiązaniu tym macierze będą udostępniały zasoby dyskowe dla potrzeb serwerów wirtualnych VM oraz przechowywały kopie zapasowe.

Zostanie uruchomiona pomiędzy macierzami replikacja synchroniczna, w celu zapewnienia odporności na awarię lub w przypadku niedostępności jednej z lokalizacji zapewnienia ciągłości działania.

Archiwizacja Regionalnego Repozytorium EDM (RREDM) będzie odbywać się z wykorzystaniem macierzy SAN oraz biblioteki taśmowej. Zapewni to odpowiedni poziom bezpieczeństwa dla zabezpieczanych danych.

Do realizacji założeń bezpieczeństwa w Projekcie niezbędne jest wykorzystanie dwóch różnych rodzajów nośników. Właściwe rozwiązanie to zastosowanie pamięci dyskowej o pojemności użytkowej min. 250TB opisanej poniżej oraz biblioteki taśmowej LTO jako uzupełnienie.

Istnieje możliwość rozbudowy macierzy do pojemności użytkowej 500TB, poprzez dołożenie kolejnych półek dyskowych.

Na potrzeby archiwizacji danych obrazowych przewiduje się zastosowanie jednej biblioteki taśmowej, wyposażonej w dwa napędy LTO8 oraz 40 slotów na taśmy w lokalizacji nr 1. Takie rozwiązanie pozwoli na szybkie wykonanie i przywracanie kopii danych jak również umożliwi tworzenie codziennych kopii przy minimalnym przyroście zajętej przestrzeni. Ilość i rodzaj zastosowanych taśm LTO8, umożliwi sumarycznie archiwizację do 480TB natywnej pojemności.

Do obsługi systemu kopii bezpieczeństwa zainstalowany zostanie osobny serwer w Lokalizacji nr 1. Serwer ten wyposażony zostanie w 100TB przestrzeni dyskowej, umożliwiając tym samym przechowywanie najbardziej kluczowych systemów (maszyn wirtualnych) z zasobów dyskowych Flash macierzy (10 x 7,84TB SSD). Pozwoli to, w razie konieczności, na ich szybkie odtworzenie. Backup danych obrazowych przewidziany jest na macierzach (36 x 8TB NLSAS) oraz na bibliotece taśmowej (taśmy LTO8).

Przełączniki SAN zasobowe

Na potrzeby klastra wirtualizacyjnego niezbędne będzie zainstalowanie po dwa przełączniki SAN na każdą lokalizację, w celu połączenia urządzeń z zapewnieniem redundancji, aby awaria pojedynczego kontrolera w serwerze/macierzy nie powodowała jego wyłączenia z sieci.

Rekomendacja IK

Mając na uwadze informacje pozyskane w trakcie Wstępnych Konsultacji Rynkowych, Inżynier Kontraktu rekomenduje wybór rozwiązania opartego o model tradycyjny. Umożliwia on bardziej elastyczną rozbudowę infrastruktury, uniknięcie „vendor lock-in”, większą kontrolę nad zasobami i możliwością przydzielenia odpowiednich zasobów odpowiednim systemom.

Urządzenia sieciowe

Przełączniki LAN rdzeniowe

Przełączniki rdzeniowe mają za zadanie agregować ruch sieciowy: wszystkie połączenia z klastrów, pozostałych przełączników rdzeniowych, połączenia z dodatkowymi serwerowniami i kluczowymi punktami dystrybucyjnymi.

Przełączniki powinny mieć możliwość łączenia ich w stos, co w dużym stopniu uprości architekturę rozwiązania oraz zarządzanie - zmniejsza się narzut pracy związany z zarządzaniem wieloma urządzeniami.

W obu lokalizacji Serwerowni przewidziane zostały dwa przełączniki rdzeniowe LAN połączone w stos z wykorzystaniem dedykowanych do tego celu modułów.

UTM

Zakłada się zastosowanie w każdej lokalizacji dwóch urządzeń klasy UTM pracujących w klastrze. Rozwiązania Unified Threat Management pozwalają zabezpieczyć sieć na wielu płaszczyznach.

Zapora sieciowa typu UTM dostarcza wielu funkcji ochrony brzegu sieci zgromadzonych w jednym sprzętowym urządzeniu.

Połączenie sieci wewnętrznej z Internetem chronione będzie przez wysokiej klasy klaster aktywny dwóch urządzeń UTM, który spełnia wszystkie wymagania Projektu wraz z redundancją. Dwa urządzenia będą pracowały wspólnie i będą zarządzane z poziomu jednego interfejsu. W przypadku awarii jednego z urządzeń pozostałe sprawne przejmie obsługę całej komunikacji w sposób niezauważalny tym samym utrzymując ciągłość działania.

Zakup ten jest niezbędny dla zapewnienia bezpieczeństwa przechowywanych i przetwarzanych danych. Ciągłość komunikacji, w przypadku awarii jednej z lokalizacji, możliwa będzie przy odpowiedniej konfiguracji protokołu BGP. Zaplanowane zostało wdrożenie polityk QoS w celu ochrony krytycznych aplikacji oraz utrzymania jakości świadczonych usług.

Niezbędne jest doprowadzanie do podmiotu dwóch niezależnych łączy światłowodowych z przepustowością min. 100 Mb/s.

Szafy rack

Zakłada się (jako liczbę wystarczającą) dostawę jednej szafy o wysokości 42U na każdą lokalizację. Szafa będzie wyposażona w listwy zasilające oraz przetącnik konsolowy KVM+KMM 8 portowy.

Zasilanie awaryjne oraz klimatyzacja po stronie Zamawiającego. **Zarządzanie infrastrukturą**

Zaplanowane rozwiązania będą umożliwiały w sposób ciągły bieżące monitorowanie wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz będą zapewniały możliwość zdefiniowania alertów informujących o przekroczeniu wartości progowych. Alerty te będą dostępne dla zespołu inżynierów i specjalistów, nadzorujących wdrożone systemy. Zapewniony będzie zdalny dostęp do zarządzania infrastrukturą, z wykorzystaniem szyfrowanych połączeń VPN skonfigurowanych na UTM-ach.

9.1.2 Wyposażenie poszczególnych lokalizacji

Wyposażenie Lokalizacji nr 1 GCPD zapewnione będzie przez UM WZ, natomiast w przypadku Lokalizacji nr 2 GCPD zapewnione będzie przez UMWZ lub inne Data Center (kolokacja, która wiąże się z dodatkowymi opłatami).

Zasilanie niezbędne do podtrzymania napięcia w każdej szafie w obu lokalizacjach przy pełnym obsadzeniu to 10kW (z zapasem).

Niezbędna moc chłodząca dla każdej lokalizacji w wariancie maksymalnym kształtuje się na poziomie 9kW (z zapasem). Klimatyzacja musi działać w trybie redundantnym.

Za względu na ograniczoną rolę warstwy regionalnej oraz szacowaną wielkość ruchu sieciowego na poziomie regionalnym nie jest konieczne zapewnienie dedykowanych łączy Internetowych na potrzeby projektu ZeZ. Wystarczające będą łącza internetowe, w jakie będzie wyposażone Centrum przetwarzania danych na ul. Piłsudskiego.

W przypadku wykupienia przez UMWZ internetowego łącza zapasowego (od operatorów/dostawców Internetowych), rozwiązanie będzie przygotowane do podłączenia go, uwzględniając wykorzystanie protokołu BGP (Border Gateway Protocol).

		Rodzaj	Objętość jednostkowa [MB]	Ilość	Wielkość [MB/rok]	Kierunek ruchu	Udział %
BI	System analityczny BI + zamówienie publiczne	tekst/liczby	1,50	312	468	przychodzące	0,042%
		tekst/liczby	2,00	156	312	wychodzący	0,028%
EDM	EDM - przesłanie do regionu danych opisowych	tekst	0,25	1 500 000	375 000	przychodzące	33,310%
	EDM - pobranie z regionu danych opisowych	tekst	0,25	3 000 000	750 000	wychodzący	66,620%

			Suma rocznej objętości [MB]	1 125 780
--	--	--	-----------------------------	------------------

Razem ruch ZeZ [MB]		Średni godzinny* ruch ZeZ [Mb/s]		Ruch chwilowy* wartość szczytowa [Mb/s]		Długość okresu ruchu szczytowego [s]
Ruch przychodzący	375 468	0,35	Mb/s	50,00	Mb/s	0,42
Ruch wychodzący	750 312	0,69	Mb/s	50,00	Mb/s	0,83

* przy założeniach koncentracji ruchu sieciowego dla 300 dni w roku w ciągu 8 godzin roboczych (7:15).

* przy założeniu ograniczenia max. zajętości łącza dla przesyłu danych obrazowych na poziomie 50% dostępności łącza Internetowego dla pliku obrazu DICOM o dużej objętości (tomograf lub rezonans magnetyczny).

Analiza wyników badania ankietowego pozwoliła na określenie potrzeb dla ich przechowywania na poziomie regionalnym w macierzach dyskowych oraz szacowaną wielkość ruchu sieciowego, a także na określenie zapotrzebowania na przepustowość łączy internetowych dla Warstwy regionalnej. Przechowywanie danych dla szacowanych objętości w Warstwie regionalnej nie wymaga zapewnienia dedykowanych łączy internetowych na potrzeby Projektu ZeZ. Wystarczające będą łącza internetowe o przepustowości min. 100 Mb/s (upload/download), w które zostanie wyposażone Centrum Przetwarzania Danych na ul. Piłsudskiego.

Inżynieria ruchu sieciowego musi być obsługiwana w następujący sposób:

- sieć zostanie podzielona na VLANy,
- pomiędzy którymi ruch będzie filtrowany i routowany poprzez dwa niezależne firewalle/UTMy sprzętowe pracujące w klastrach HA.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego**Uwagi:**

- 1) Powyższe konfiguracje oparto na podstawie wiedzy eksperckiej, zweryfikowanej z uwzględnieniem analogicznych projektów zrealizowanych w innych regionach.
- 2) Środowisko testowe jest przewidziane w ramach środowiska wirtualnego.
- 3) Szczegółowe wymagania techniczne zostaną określone na etapie opracowywania SIWZ (OPZ) z uwzględnieniem wymagań i będą zweryfikowane przez wykonawcę systemu.
- 4) Głównym założeniem koncepcji architektury infrastruktury serwerowej jest zapewnienie przez ZeZ funkcjonowania Głównego Centrum Przetwarzania Danych.

Oprogramowanie środowiskowe

Wdrożenie systemu ZeZ wymaga wielu serwerów pozwalających na separację kluczowych i krytycznych usług. Rozwiązaniem pozwalającym wygenerowanie oszczędności na zakupie dużej ilości serwerów jest zastosowanie oprogramowania wirtualizacyjnego, które tworzy warstwę pośrednią pomiędzy fizycznym sprzętem a oprogramowaniem (systemowym). Ponadto takie rozwiązanie pozwala oddzielić serwery i usługi od sprzętu, który to obsługuje, jest narzędziem nadzorującym i zarządzającym procesami wirtualizacji - hipernadzorca (inaczej hiperwizor, od ang. hypervisor). Za pomocą rozwiązania tej klasy będzie możliwe wdrożenie wielu maszyn wirtualnych/serwerów osobno dla każdej z potrzebnych usług.

Przyjmuje się dostępność e-usług publicznych (ang. availability) na poziomie min. 99,9%, klasa dostępności 3. Dla zapewnienia wymaganego poziomu dostępności koniecznym jest zapewnienie ciągłości świadczenia usług sieciowych oraz systemów. Osiągnięte to zostanie w wyniku wdrożenia konfiguracji złożonej z fizycznych serwerów pracujących w klastrze z zainstalowanym oprogramowaniem wirtualizacyjnym. Taka konfiguracja zapewnia ciągłość działania na wypadek awarii pojedynczego serwera, a w przypadku odpowiednio dobranego sprzętu pozwoli na utrzymanie wydajności niezbędnej do płynnego działania usług. Przy wyborze platformy wirtualizującej, należy wziąć pod uwagę możliwość współpracy platformy z publicznymi chmurami obliczeniowymi. Pozwoli to, w razie konieczności, na skorzystanie z oferty dostawców takich infrastruktur.

W związku z realizacją Projektu zostaną również zakupione licencje na system operacyjny zapewniające prawo do użytkowania dowolnej liczby maszyn wirtualnych w klastrze. System operacyjny zostanie dobrany odpowiednio aby umożliwić wdrożenie usług i serwerów niezbędnych do uruchomienia Projektu Zachodniopomorskie e-Zdrowie.

Niezbędna jest również budowa/rozbudowa systemu do wykonywania kopii bezpieczeństwa. System zapewni tworzenie kopii bezpieczeństwa całych maszyn wirtualnych oraz fizycznych z systemem Windows lub Linux. Kopie będą wykonywane zarówno w całości jak i z możliwością wyboru poszczególnych dysków. Rozwiązanie musi zapewniać możliwość odzyskania całej maszyny wirtualnej. Niezbędna możliwość częściowego odtwarzania zasobów z maszyny wirtualnej na poziomie plików.

Oprogramowanie kopii bezpieczeństwa musi współpracować z zasobami dyskowymi oraz biblioteką taśmową, aby zapewnić spójne tworzenie kopii bezpieczeństwa zgodnie z zasadą 3-2-1.

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

Kluczowe dane będą zapisywane w 3 kopiach na dwóch różnych nośnikach danych, z czego przynajmniej jedna z kopii znajdzie się w innej lokalizacji niż dane produkcyjne (taśmy LTO).

9.2 Warstwa lokalna

W ramach Projektu zakupiona zostanie infrastruktura informatyczna dla Partnerów Projektu. Zakres planowanych zakupów jest różny dla poszczególnych podmiotów leczniczych uczestniczących w Projekcie i jest wynikiem przeprowadzonej szczegółowej analizy potrzeb.

Rozbudowa/modernizacja istniejącej infrastruktury teleinformatycznej ma na celu zapewnienie możliwości świadczenia przez dany podmiot leczniczy e-usług a także tworzenie a następnie udostępnianie Elektronicznej Dokumentacji Medycznej. Ponadto, zgodnie z założeniami procesu obsługi Zdarzeń Medycznych, konieczne będzie zapewnienie środowiska teleinformatycznego umożliwiającego wdrożenie i użytkowanie wymienionych systemów oprogramowania.

Szczegółowe wymagania techniczne zostaną określone na etapie opracowywania SWZ (OPZ).

Poniżej przedstawiona jest referencyjna architektura środowiska przetwarzania danych w warstwie lokalnej zapewniająca bezpieczne przetwarzanie dokumentacji medycznej w postaci elektronicznej. Przedstawiona architektura jest zgodna z rekomendacjami Centrum e-Zdrowia.

9.2.1 Opis środowiska referencyjnego

Środowisko serwerowe przeznaczone dla aplikacji zalecane jest w oparciu o klaster wysokiej dostępności składający się z min. dwóch serwerów-hostów (S1, S2 – zalecane są 3 hosty) z zainstalowanym oprogramowaniem do wirtualizacji. Wysoką dostępność zapewni zastosowanie macierzy dyskowej MD1 podłączonej do serwerów z wykorzystaniem przełącznika/przełączników oraz drugiej macierzy dyskowej MD2 pracującej jako replika macierzy podstawowej MD1.

Pamięć masowa NAS wyposażona będzie w dyski SATA/SAS lub dyski SSD z przeznaczeniem do zapisu plikowego. Wydzielony w ten sposób zasób dyskowy przeznaczony będzie do archiwizacji danych EDM podmiotu leczniczego.

W zależności od szczegółowego rozwiązania do archiwizacji danych przeznaczony będzie deduplikator lub dedykowany serwer archiwizacji z biblioteką taśmową.

Środowisko serwerowe przeznaczone dla bazy danych zbudowane będzie z dwóch serwerów bazodanowych (B1, B2) pracujących w oparciu o mechanizmy wysokiej dostępności.

Połączenie sieci wewnętrznej z Internetem chronione będzie przez urządzenie brzegowe UTM. W zależności od potrzeb mogą to być dwa urządzenia, które będą pracowały wspólnie i będą zarządzane z poziomu jednego interfejsu (klaster HA). W przypadku awarii jednego z urządzeń drugie urządzenie przejmie obsługę całej komunikacji w sposób niezauważalny tym samym utrzymując ciągłość działania.

10. Założenia i wytyczne dotyczące bezpieczeństwa

10.1 Uwarunkowania prawne

Ze względu na przetwarzanie i dostęp do danych pacjentów, które mają charakter danych wrażliwych, podmioty lecznicze muszą spełnić określone założenia związane z bezpieczeństwem. Wytyczne dotyczące ochrony danych osobowych w podmiotach medycznych zawierają następujące akty prawne:

- 1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- 2) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247),
- 3) ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 poz. 1369 z późn. zm.),
- 4) ustawa z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz.U z 2020 r. poz. 295, z późn. zm.),
- 5) ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2020 r. poz. 849 z późn. zm.).

Należy zwrócić uwagę w szczególności na wymienione powyżej Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, które w § 20 stanowi, iż:

1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:
 - 1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
 - 2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;
 - 3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
 - 4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu

- adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
- 5) bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4;
 - 6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
 - a) zagrożenia bezpieczeństwa informacji;
 - b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna;
 - c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
 - 7) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
 - a) monitorowanie dostępu do informacji,
 - b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
 - c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
 - 8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
 - 9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;
 - 10) zawierania w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
 - 11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
 - 12) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
 - a) dbałości o aktualizację oprogramowania,
 - b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
 - c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
 - d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
 - e) zapewnieniu bezpieczeństwa plików systemowych,
 - f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
 - g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
 - h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
 - 13) bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących;
 - 14) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:

- 1) PN-ISO/IEC 27002 - w odniesieniu do ustanawiania zabezpieczeń;
 - 2) PN-ISO/IEC 27005 - w odniesieniu do zarządzania ryzykiem;
 - 3) PN-ISO/IEC 24762 - w odniesieniu do odtwarzania techniki informatycznej po katastrofie w ramach zarządzania ciągłością działania.
4. Niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.

Wymienione powyżej akty prawne odnoszą się do szeroko rozumianego bezpieczeństwa informacji,, w szczególności zakres koniecznych działań w związku z ochroną danych osobowych określa RODO. Nie wskazują jednak „wprost” jak wymagania te powinny być zaimplementowane. Co więcej, nie ma obowiązującego aktu prawnego, który szczegółowo warunkowałby to zagadnienie, w szczególności w odniesieniu do sektora ochrony zdrowia.

Mając na uwadze wyróżniony powyżej §20 ust. 4 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, właściwym odniesieniem w tym zakresie mogą być zapisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. (Dz.U. 2019 poz. 125 z późn. zm.). W odniesieniu do zabezpieczenia danych osobowych ustawa stanowi **Art. 39**. Administrator i podmiot przetwarzający stosują środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, które w szczególności mają na celu:

- 1) uniemożliwienie osobom nieuprawnionym dostępu do sprzętu używanego do przetwarzania (**kontrola dostępu do sprzętu**),
- 2) zapobiegnięcie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu nośników danych (**kontrola nośników danych**),
- 3) zapobiegnięcie nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych (**kontrola przechowywania**),
- 4) zapobiegnięcie korzystaniu z systemów zautomatyzowanego przetwarzania przez osoby nieuprawnione, używające sprzętu do przesyłu danych (**kontrola użytkowników**),
- 5) zapewnienie osobom, uprawnionym do korzystania z systemu zautomatyzowanego przetwarzania, dostępu wyłącznie do danych osobowych objętych posiadaniem przez siebie uprawnieniem (**kontrola dostępu do danych**),
- 6) umożliwienie zweryfikowania i ustalenia podmiotów, którym dane osobowe zostały lub mogą zostać przesłane lub udostępnione, za pomocą sprzętu do przesyłu danych (**kontrola przesyłu danych**),
- 7) umożliwienie następczej weryfikacji i ustalenia, które dane osobowe zostały wprowadzone do systemów zautomatyzowanego przetwarzania, kiedy i przez kogo (**kontrola wprowadzania danych**),



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 8) zapobieżenie nieuprawnionemu odczytywaniu, kopiowaniu, zmienianiu lub usuwaniu danych osobowych podczas ich przekazywania lub podczas przenoszenia nośników danych (**kontrola transportu**),
- 9) zapewnienie przywrócenia zainstalowanych systemów w razie awarii (**odzyskiwanie**),
- 10) zapewnienie działania funkcji systemu, zgłaszania występujących w nich błędów (niezawodność) oraz odporności przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu (integralność).

Drugą kluczową kwestią jest kontekst cyberbezpieczeństwa. Wdrażane i użytkowane systemy informatyczne integrują się w ramach krajowego Systemu Informacji Medycznej wykorzystując usługi sieciowe. Koniecznym staje się spełnienie wymogów regulacji dotyczących szeroko rozumianego bezpieczeństwa w sieci.

W wymiarze unijnym określa to Dyrektywa NIS, czyli dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

Jest to akt prawa europejskiego, który musiał zostać zaimplementowany do porządków prawnych poszczególnych państw członkowskich. W Polsce dokonało się to za pośrednictwem ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ustawa o cyberbezpieczeństwie).

Dyrektywa NIS nie obejmuje swoim zakresem wszystkich przedsiębiorców. Jej przepisy mają zastosowanie do operatorów usług kluczowych oraz dostawców usług cyfrowych (znaczenie obu tych pojęć zostało określone w ustawie o cyberbezpieczeństwie).

Operatorzy usług kluczowych to podmioty z określonych przez ustawę o cyberbezpieczeństwie strategicznych sektorów gospodarki. W odniesieniu do sektora ochrony zdrowia:

- w zakresie udzielania świadczenia opieki zdrowotnej przez podmiot leczniczy jest to świadczeniodawca zakwalifikowany do systemu podstawowego szpitalnego zabezpieczenia świadczeń opieki zdrowotnej w ramach tzw. „sieci szpitali” oraz posiadający Szpitalny Oddział Ratunkowy,
- w zakresie gromadzenia i udostępniania Elektronicznej Dokumentacji Medycznej wymagane jest zapewnienie dostępu do usługi dla wszystkich usługobiorców.

Mając na uwadze omówione powyżej uwarunkowania, wdrażane w ramach Projektu *Zachodniopomorskie e-Zdrowie* systemy informatyczne muszą spełnić wymagania szczegółowo przedstawione w dalszej części rozdziału.

10.2 Szczegółowe wymagania – bezpieczeństwo fizyczne

Zabezpieczenia fizyczne systemu powinny zapewniać co najmniej:

- 1) zabezpieczenie obszaru, w którym przetwarzane są dane osobowe przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 2) przebywanie osób nieuprawnionych w obszarze, w którym przetwarza się dane osobowe dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.

Zalecane środki ochrony fizycznej w zakresie bezpieczeństwa danych osobowych są następujące:

- 1) Przechowywanie zbioru danych osobowych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności ogniowej ≥ 30 min.
- 2) Przechowywanie zbioru danych osobowych w pomieszczeniu zabezpieczonym drzwiami o podwyższonej odporności na włamanie - drzwi klasy C.
- 3) Przechowywanie zbioru danych osobowych w pomieszczeniu, w którym okna zabezpieczone są za pomocą krat, rolet lub folii antywłamaniowej.
- 4) Pomieszczenia, w którym przetwarzany jest zbiór danych osobowych wyposażone w system alarmowy przeciw włamaniom.
- 5) System kontroli dostępu do pomieszczeń, w których przetwarzany jest zbiory danych osobowych.
- 6) Kontrolowanie dostępu do obszarów (grup pomieszczeń), w których przetwarzany jest zbiór danych osobowych kontrolowany przez system monitoringu z zastosowaniem kamer przemysłowych.
- 7) Dostęp do pomieszczeń, w których przetwarzany jest zbiór danych osobowych w czasie nieobecności zatrudnionych tam pracowników nadzorowany przez służbę ochrony.
- 8) Nadzorowanie przez służbę ochrony dostępu do pomieszczeń, w których przetwarzany jest zbiór danych osobowych przez całą dobę.
- 9) Przechowywanie kopii zapasowych/archiwalnych zbioru danych osobowych w zamkniętej ogniotrwałej metalowej szafie znajdującej się w innej lokalizacji niż ta, w której znajdują się serwery bazodanowe i aplikacyjne.
- 10) Zabezpieczenie pomieszczenia, w którym przetwarzane są zbiory danych osobowych przed skutkami pożaru za pomocą systemu przeciwpożarowego, który musi być neutralny dla sprzętu. Wskazaniem jest stosowanie rozwiązań zapewniających wczesną detekcję dymu oraz automatyczne gaszenie pożaru gazowym środkiem gaśniczym (tzw. "stałe urządzenie gaśnicze").

10.3 Szczegółowe wymagania – bezpieczeństwo systemów informatycznych

Zabezpieczenia w zakresie bezpieczeństwa systemów informatycznych przetwarzających dane medyczne powinny zapewniać co najmniej aby:

- 1) w systemie informatycznym służącym do przetwarzania danych osobowych zastosowane były mechanizmy kontroli dostępu do tych danych, a w przypadku, kiedy dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, zapewnione było, aby:
 - a) w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator,
 - b) dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia,

- c) zaimplementowane były mechanizmy odnotowywania każdej czynności wykonywanej na bazie danych (włącznie z jej przeglądaniem) w celu zapewnienia rozliczalności działania na danych,
- 2) identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie mógł być przydzielony innej osobie,
- 3) w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry i znaki specjalne,
- 4) system informatyczny służący do przetwarzania danych osobowych zabezpieczony był w szczególności przed:
 - a) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego,
 - b) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
- 5) dane osobowe przetwarzane w systemie informatycznym zabezpieczone muszą być przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych,
- 6) kopie zapasowe były:
 - a) przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem,
 - b) przechowywane jeżeli to możliwe w formie zaszyfrowanej,
 - c) usuwane niezwłocznie po ustaniu ich użyteczności,
- 7) urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do:
 - a) likwidacji — muszą zostać pozbawione wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
 - b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — urządzenie przekazywane podmiotowi nieuprawnionemu do przetwarzania danych (np. zwrot leasingowanego sprzętu) powinno zostać pozbawione nośników, (wyjęte np. dyski twarde),
 - c) naprawy — urządzenia, które mogą zawierać nośniki danych przed przekazaniem ich do serwisu, muszą być pozbawione tych nośników (wyjęte np. dyski twarde). Nie jest dopuszczalna naprawa uszkodzonych nośników danych - uszkodzone nośniki danych podlegają jedynie likwidacji (przy założeniu, że poprawnie wykonywana jest kopia bezpieczeństwa),
- 8) systemy informatyczne służące do przetwarzania danych osobowych muszą być chronione przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. Wdrożenie fizycznych zabezpieczeń powinno obejmować systemy automatycznego wykrywania zagrożeń (np. IPS/IDS lub równoważnego. W przypadku zastosowania logicznych zabezpieczeń, o których mowa powyżej, muszą one obejmować:

- a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną,
 - b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych,
- 9) administrator danych musi stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej, które uniemożliwiają uzyskanie dostępu do danych przez osoby nieuprawnione nawet w przypadku gdy zostaną one przez nie przejęte,
 - 10) osoba użytkująca komputer przenośny zawierający dane osobowe musi zachowywać szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym dane są przetwarzane, w tym muszą zostać zastosowane środki ochrony kryptograficznej wobec przetwarzanych danych osobowych,
 - 11) urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar, w którym dane są przetwarzane były zabezpieczone w sposób zapewniający poufność i integralność tych danych m.in. poprzez przechowywanie ich na tych urządzeniach i nośnikach w formie zaszyfrowanej.

10.4 Bezpieczeństwo systemów informatycznych w cyberprzestrzeni

Do najpopularniejszych zagrożeń w cyberprzestrzeni należą:

- ataki z użyciem szkodliwego oprogramowania (malware, wirusy, robaki, trojany, keyloggers),
- kradzieże tożsamości,
- kradzieże, wyłudzenia, modyfikacje bądź niszczenie danych,
- blokowanie dostępu do usług,
- wirusy,
- phishing i inne oszustwa,
- upublicznienie intymnych informacji, zdjęć, filmów,
- kontakt z pornografią, przemocą, materiałami promującymi nielegalne treści,

Dla zapewnienia bezpieczeństwa w sieci Internet wymagane jest przestrzeganie podstawowych zasad bezpiecznego użytkowania Internetu. Są to:

- 1) regularna aktualizacja oprogramowania:
 - urządzeń sieciowych,
 - systemów operacyjnych,
 - oprogramowania aplikacyjnego w zakresie stwierdzonych luk w bezpieczeństwie,
- 2) zainstalowanie na wszystkich urządzeniach klienckich (PC, notebooki, tablety itp.) programów antywirusowych z firewallem i na bieżąco ich aktualizowanie,
- 3) rygorystyczne przestrzeganie zakazu otwierania e-maili nieznanego pochodzenia,
- 4) rygorystyczne przestrzeganie zakazu udostępniania komukolwiek swoich haseł i loginów,
- 5) regularne przeprowadzenie testów bezpieczeństwa, w tym testów penetracyjnych.

10.5 Szczegółowe wymagania proceduralne oraz techniczne

Rzeczpospolita
PolskaUnia Europejska
Europejski Fundusz
Rozwoju Regionalnego

10.5.1 Bezpieczny dostęp do danych

Zapewnienie bezpiecznego dostępu do danych wymaga wdrożenia i przestrzegania następujących zasad:

- 1) **Granulacja uprawnień** - ograniczenie dostępu pracownikom tylko do danych lub plików niezbędnych do wykonywania ich pracy;
- 2) **Bezpieczne połączenie do danych** - dostęp do infrastruktury IT, w której znajdują się dane, powinien odbywać się poprzez bezpieczne połączenie sieciowe, w przypadku połączeń zdalnych stosowanie szyfrowanego połączenia VPN (Virtual Private Network) oraz innych dostępnych obecnie lub w przyszłości rozwiązań o równoważnej funkcjonalności;
- 3) **Bezpieczne stacje robocze** - blokowanie komputerów po odejściu od biurka, nie klikanie w reklamy przychodzące w spamowych emailach, zakaz używania niewspieranych przeglądarek, blokowanie portów USB, ograniczanie i kontrola odwiedzanych stron www, możliwość blokowania w przeglądarkach i innym oprogramowaniu, automatycznego uzupełniania/podpowiadania wartości w polach formularzy (np. adresów mail);;
- 4) **Bezpieczeństwo sieci WiFi** - sieci powinny być oddzielne dla pracowników i dla gości. Należy stosować np. loginy w postaci imienia i nazwiska, lub innego przypisanego ciągu znaków odpowiadającego pracownikowi w bazie danych. Urządzenia końcowe (np. smartfony, tablety, smartwatche) na poziomie warstwy sieciowej powinny być oddzielone od zasobów danych.

10.5.2 Bezpieczeństwo danych

- 1) **Kopia zapasowa** - sprawdzona metoda na ochronę przed utratą danych. Składowanie danych na serwerach backupowych, które posiadają duże przestrzenie dyskowe z wykorzystaniem narzędzi do wykonywania kopii zapasowej. Kopie zapasowe przechowywane na osobnych zasobach sprzętowych - im większa separacja, tym lepiej. Regularne przeprowadzanie testów w zakresie możliwości odtworzenia danych po awarii w oparciu o przyjęte i wdrożone procedury odzyskiwania danych oraz odtwarzania środowiska po awarii.
- 2) **Redundancja na poziomie sprzętowym** – stosowanie rozwiązań zgodnie z zasadą „n+1”. Każdy krytyczny element jest redundantny, (np. serwery aplikacyjne, bazodanowe, UPS-y, listwy zasilające, akumulatory).
- 3) **Systemy zasilania awaryjnego** - oprócz UPS-ów odpowiedniej pojemności powinny być brane pod uwagę agregaty prądotwórcze i procedury konserwacji i zasilania ich w paliwo.
- 4) **Serwery w serwerowni** – użytkowanie krytycznej dla przetwarzania danych infrastruktury w dedykowanym do tego celu, odpowiednim miejscu – serwerowni z właściwym wyposażeniem: nieprzerwane zasilanie urządzeń, zapewnienie i utrzymanie właściwych warunków środowiskowych (temperatura, wilgotność), kontrola dostępu, zabezpieczenia antywłamaniowe oraz p.poż.).
- 5) **Serwis gwarancyjny i pogwarancyjny** – zapewnienie akceptowalnego czasu na usunięcie awarii np. 4 godziny.



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- 6) **Zapaszowe Centrum Danych** – z wykorzystaniem zapaszowej lokalizacji, która znajduje się w innej lokalizacji geograficznej, w celu uniknięcia wspólnych awarii zasilania lub internetu. Połączona jest z serwerownią główną (HQ) za pomocą dedykowanego tunelu sieciowego.

10.5.3 Szczegółowe wymagania bezpiecznego przetwarzania EDM

- 1) Dostęp do systemu EDM możliwy jest tylko z sieci wewnętrznej podmiotu leczniczego zintegrowanego.
- 2) Pomieszczenia, w których możliwy jest dostęp do systemu EDM muszą być chronione przed dostępem osób nieuprawnionych.
- 3) Komputery, z których następuje dostęp do systemu EDM muszą być:
 - a) wyposażone w system operacyjny wymagający uwierzytelnienia użytkownika,
 - b) chronione za pomocą systemów antywirusowych.
- 4) Użytkownicy systemu EDM muszą być uwierzytelnieni i autoryzowani w systemach dziedzicznych podmiotu leczniczego. Warstwa regionalna traktuje system integrujący się z warstwą regionalną jako system zaufany, który dokonuje autoryzacji użytkowników w zakresie uprawnień do wyszukiwania i przeglądania dokumentacji medycznej gromadzonej w warstwie regionalnej. W związku z tym warstwa regionalna nie autoryzuje użytkowników z podmiotów leczniczych.
- 5) Dostęp do systemu EDM jest możliwy tylko dla użytkowników uwierzytelnionych.
 - a) każdy użytkownik korzystający z systemu musi być uwierzytelniony,
 - b) każdy użytkownik musi posiadać unikalny identyfikator,
 - c) nie wolno ponownie wykorzystywać identyfikatory nadane wcześniej innym użytkownikom,
 - d) nie wolno korzystać z kont grupowych, gdzie wielu użytkowników korzysta z jednego konta.
- 6) Jeśli do uwierzytelnienia w systemie (systemach) dziedzicznym używa się hasła, to w podmiocie leczniczym musi być zdefiniowana i wprowadzona w życie polityka haseł.
- 7) Dostęp do systemu EDM jest możliwy tylko dla użytkowników zautoryzowanych.
 - a) każdy użytkownik korzystający z systemu musi być zautoryzowany w warstwie lokalnej,
 - b) w podmiocie musi być zdefiniowana i wprowadzona w życie procedura nadawania uprawnień,
 - c) musi być wskazana osoba/osoby odpowiedzialna za nadawanie uprawnień,
 - d) uprawnienia użytkowników muszą być nadawane tylko w zakresie niezbędnym (i adekwatnym) do wykonywania obowiązków służbowych,
 - e) w podmiocie musi być zdefiniowana procedura okresowej weryfikacji nadanych uprawnień, a w razie potrzeby ich modyfikacji lub cofnięcia.
- 8) W podmiocie leczniczym muszą być opracowane procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

- 9) Dokumentacja medyczna podlegająca wymianie z innymi podmiotami musi być podpisana podpisem elektronicznym. Dokumentacja medyczna musi być również zabezpieczona przed dostępem osób nieuprawnionych w trakcie jej przekazywania (np. hasłowanie, szyfrowanie, pseudonimizacja danych lub rozwiązania równoważne).
- 10) System (systemy) dziedzinowy w warstwie lokalnej musi zapewniać mechanizm audytowania zdarzeń, w szczególności:
 - a) wprowadzania i aktualizacji danych osobowych/medycznych (kto, kiedy, co),
 - b) wyszukiwania danych osobowych/medycznych (kto, kiedy, co),
 - c) udostępniania danych osobowych/medycznych (kto, kiedy, co).
- 11) Informacje audytowe o zdarzeniach przetwarzania danych osobowych (w tym medycznych) zgromadzone w logach muszą być chronione przed niepożądanym dostępem.
- 12) Systemy dziedzinowe muszą umożliwiać rejestrowanie zgód i sprzeciwów pacjentów na udostępnianie ich dokumentacji medycznej. Informacje o zgodach i sprzeciwach muszą być przekazywane do systemu ZeZ i zastosowane w podmiotach zintegrowanych z systemem ZeZ.
- 13) Rozwiązanie funkcjonujące w podmiocie leczniczym integrujące się z systemem ZeZ musi zapewniać sporządzenie i wydrukowanie (w czytelnej postaci) raportu zawierającego:
 - a) informacje o wprowadzeniu danych osobowych/medycznych (kto, kiedy, co),
 - b) informacje o aktualizacji danych osobowych/medycznych (kto, kiedy, co),
 - c) informacje o zdarzeniach udostępniania danych osobowych/medycznych (kto, kiedy, co),
 - d) informacje o sprzeciwach pacjenta na przetwarzanie danych osobowych/medycznych.
- 14) W podmiocie musi być opracowana i wdrożona polityka udostępniania dokumentacji medycznej, określająca, które z dokumentów podlegają udostępnieniu do systemu ZeZ w celu wymiany z innymi podmiotami.
- 15) W podmiocie leczniczym musi być opracowana i wdrożona procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania. W szczególności muszą być określone:
 - a) okres przechowywania kopii zapasowych,
 - b) lokalizacje przechowywania kopii zapasowych,
 - c) sposób zabezpieczenia przed nieuprawnionym dostępem,
 - d) sposób trwałego i bezpiecznego usuwania kopii zapasowych.
- 16) Systemy zintegrowane muszą spełniać wytyczne Centrum eZdrowia w zakresie budowy i stosowania systemu bezpiecznego przetwarzania EDM.
- 17) System regionalny wystawia certyfikaty X.509 dla systemów lokalnych zintegrowanych z ZeZ.
- 18) System regionalny wykonuje tylko uwierzytelnienie i autoryzację systemu lokalnego.
- 19) Każde wywołanie usługi regionalnej zawiera token SAML w wersji 2.0.
- 20) W ramach tokenu SAML muszą być przekazane następujące informacje o osobie wywołującej usługi regionalne:
 - a) identyfikator osoby z systemu dziedzinowego,



Rzeczpospolita
Polska



Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



- b) imię osoby,
- c) nazwisko osoby,
- d) identyfikator systemu dziedzinowego,
- e) identyfikator Zakładu Opieki Zdrowotnej,
- f) lista ról użytkownika.

Komunikacja pomiędzy systemem regionalnym i Lokalnymi Repozytoriami Dokumentacji Medycznej zintegrowanymi z ZeZ musi odbywać się z wykorzystaniem protokołów SSL 3.0/ TLS 1.2.