

OPIS USŁUG BIZNESOWYCH

Niniejszy dokument stanowi opis przewidywanych do realizacji usług biznesowych dla Systemu P1. Opis usług został opracowany w konwencji podziału na obszary biznesowe. Każdy z obszarów biznesowych jest podzielony na dwie sekcje informacyjne: sekcja, w której opisane zostały usługi biznesowe realizowane w ramach danego obszaru, oraz sekcja z zakresem danych.

Zakres projektu

Projekt swoim zakresem obejmuje:

1. Obsługę elektronicznych recept (e-Recepty)

Celem realizacji e-Recepty jest usprawnienie związane z pełną elektronizacją obsługi procesu wystawiania dokumentu recepty wraz z jej realizacją. Usługa ma na celu wyeliminowanie błędów na receptach i związanych z tym utrudnień dla pacjenta oraz optymalizację pracy personelu medycznego wystawiającego receptę. Elektronizacja procesu wystawiania i realizacji recepty umożliwi gromadzenie historii stosowanej farmakoterapii i wykorzystanie jej w procesie leczenia. Celem wdrożenia usługi jest również usprawnienie procesu realizacji recepty przez pacjenta.

Obsługa e-Recepty umożliwi w szczególności

- utworzenie i zapis elektronicznego dokumentu recepty,
- przekazanie usługobiorcy informacji o receptach w pakiecie, w tym kodów dostępowych,
- anulowanie recepty,
- wystawianie recepty farmaceutycznej,
- anulowanie recepty farmaceutycznej,
- realizację recepty,
- korektę realizacji recepty,
- przeglądanie recept i dokumentów realizacji przez uprawnionego pracownika usługodawcy,

- przeglądanie recept i dokumentów realizacji przez uprawnionego pracownika apteki,
- przeglądanie recept i dokumentów realizacji przez usługobiorcę.

2. Obsługę elektronicznych skierowań (e-Skierowanie) Celem realizacji e-Skierowania jest usprawnienie związane z pełną elektronizacją obsługi procesu wystawiania dokumentu skierowania wraz z jego realizacją.

Obsługa e-Skierowania umożliwi w szczególności:

- utworzenie i zapis elektronicznego skierowania,
- dołączanie elektronicznej dokumentacji medycznej do skierowań,
- przekazanie usługobiorcy informacji o skierowaniu i kodach dostępowych,
- anulowanie skierowania,
- przeglądanie skierowania przez uprawnionego pracownika usługodawcy,
- realizacja skierowania,
- przeglądanie skierowania przez usługobiorcę,
- przeglądanie dokumentacji załączonej do skierowania.

3. Obsługę zdarzeń medycznych

Celem obsługi zdarzeń medycznych jest centralne gromadzenie danych o zdarzeniach medycznych pacjentów pozyskanych od usługodawców. Zdarzenia medyczne pozwolą na gromadzenie informacji o kontaktach pacjenta ze służbą zdrowia, informacji o udzielonych procedurach, jednostkach chorobowych, a także informacji o wytworzonej elektronicznej dokumentacji medycznej (EDM) w związku ze zdarzeniem.

Obsługa zdarzeń medycznych umożliwi w szczególności:

- utworzenie i zapis zdarzenia medycznego (wraz z indeksem EDM),
- anulowanie zdarzenia medycznego,

- przeglądanie zdarzeń medycznych przez uprawnionego pracownika usługodawcy,
- przeglądanie zdarzeń medycznych przez usługobiorcę.

4. Wymianę EDM

Celem obsługi wymiany EDM jest wsparcie usługodawców w wymianie EDM oraz umożliwienie pacjentom pobrania EDM za pośrednictwem Internetowego Konta Pacjenta (IKP). Wsparcie w zakresie wymiany EDM polegało będzie na udostępnieniach informacji o indeksach EDM zawierających informację o podmiocie odpowiedzialnym za jego przechowywanie wraz z informacją o dostępności on-line. Ponadto system będzie wspierał wzajemne uwierzytelnienie usługodawców oraz zapewniał, że dostęp do dokumentacji będzie odbywał się na podstawie uprawnień nadanych przez pacjenta.

5. Platformę publikacyjną

Platforma pozwoli na zarządzanie oraz publikację treści na internetowym portalu edukacyjno-informacyjnym. Portal powinien zapewnić szerokiej grupie odbiorców, m.in. pacjentom, pracownikom medycznym i usługodawcom, przydatne i wartościowe informacje dotyczące ochrony zdrowia. Na portalu będą udostępniane artykuły oraz komunikaty Ministra Zdrowia, wspierające pozostałe działania w realizacji zadania promocji wiedzy w zakresie ochrony zdrowia. Ponadto publikacje będą zawierały informacje dla usługodawców oraz wytwórców oprogramowania na temat systemów informacyjnych, struktur i formatów danych, komunikatów, a także będą dotyczyły aspektów eksploatacyjnych systemów. W tym celu PPP umożliwi publikowanie treści tekstowych oraz multimedialnych takich jak pliki muzyczne, obrazy graficzne i pliki video. Podsystem dostarczy również zestaw narzędzi do zarządzania publikowaną treścią redaktorom oraz narzędzia do zarządzania użytkownikami i uprawnieniami administratorowi systemu. Wszystkie autoryzowane przez redaktorów treści będą udostępniane każdemu użytkownikowi portalu. W szczególności w celu zapewnienia użytkownikowi szybkiego odnajdywania poszukiwanych informacji portal posiadać będzie mapę strony oraz wyszukiwarkę treści. Użytkownicy portalu zainteresowani nowymi treściami tematycznymi zyskają możliwość po wskazaniu odpowiedniej grupy tematycznej otrzymania e-maila z informacją o zmianie treści lub subskrybować kanał RSS. Portal pozwoli także na przeglądanie Katalogu Usługodawców opartego o dane gromadzone w Centralnym Wykazie Usługodawców.

6. Hurtownię danych i system wykrywania nadużyć

W związku z gromadzeniem szerokiego zakresu danych dot. ochrony zdrowia zostaną one wyselekcjonowane, zanonimizowane i wykorzystane do celów analityczno-statystycznych pozwalających m.in. na usprawnianie funkcjonowania obszaru ochrony zdrowia. W oparciu o dane i narzędzia BI możliwa będzie analiza danych w celu wykrycia potencjalnych nadużyć.

7. Obsługę Centralnych Wykazów Usługobiorców, Usługodawców, Pracowników Medycznych, Rejestru Leków i Płatników

Na potrzeby zapewnienia poprawności, spójności i wiarygodności danych gromadzonych w Systemie poza danymi słownikowymi zostaną wykorzystane rejestry w obszarze ochrony zdrowia (powołane w Ustawie o systemie informacji w ochronie zdrowia).

8. Internetowe Konto Pacjenta oraz Aplikacja Usługodawców i Aptek

Projekt obejmuje również utworzenie aplikacji internetowych dedykowanych:

- pacjentom – m.in. w celu zarządzania dostępem do danych medycznych, dostępem do recept, skierowań i zdarzeń medycznych, a także pobierania EDM;
- usługodawcom i pracownikom medycznym usługodawcy – pozwalających m.in. na wystawienie e-Recept, e-Skierowań czy zdarzeń medycznych, takie rozwiązanie dedykowane będzie tym podmiotom, które nie będą posługiwać się własnym systemem, a będą zobowiązane do wypełnienia obowiązku ustawowego wystawiania elektronicznych dokumentów.

W ramach II fazy Projektu wymagane jest zbudowanie w całości podsystemów:

- System Administracji – Zabezpieczenia i Prywatność (SAZ)
- System Administracji – Audyt (SAU)
- System Administracji – Administracja (SAA)
- Szyna Usług (SUS)

W ramach II fazy Projektu zaplanowano wykorzystanie następujących podsystemów (re-użycie) po wcześniejszym dostosowaniu:

- System Gromadzenia Danych Medycznych – Recepty (SGR)

- System Gromadzenia Danych Medycznych – Skierowania (SGS)
- System Gromadzenia Danych Medycznych – Zdarzenia medyczne (SGZ)
- System Weryfikacji Danych (SWD)
- System Obsługi Rejestrów – Rejestry (SRR)
- System Obsługi Rejestrów – Słowniki (SRS)
- System Obsługi Rejestrów – Zarządzanie Danymi Podstawowymi (ZDP)
- Internetowe Konto Pacjenta (IKP)
- Aplikacja Usługodawców i Aptek (AUA)
- Portal – Platforma Publikacyjna (PPP)
- Hurtownia Danych – Analizy, Statystyki, Raporty (ASR)
- Hurtownia Danych – Monitorowanie (HDM)
- System Wykrywania Nadużyć (SWN)

1 OBSZAR CENTRALNEGO WYKAZU USŁUGODAWCÓW

1.1 Opis usług biznesowych obszaru

1.1.1 Zasilenie i aktualizacja Centralnego Wykazu Usługodawców

Podsystemu ZDP zapewni mechanizm aktualizacji wpisów w Centralnym Wykazie Usługodawców, na podstawie danych otrzymanych z:

- Rejestru Podmiotów Wykonujących Działalność Leczniczą,
- Rejestru Aptek,
- podsystemu AUA.

W komunikacji pomiędzy AUA i systemami usługodawców a ZDP uczestniczyć będzie SUS. Podsystem ZDP na podstawie przekazanych danych dokona aktualizacji Centralnego Wykazu Usługodawców w podsystemie SRR.

1.1.2 Udostępnianie Centralnego Wykazu Usługodawców

Aby zapewnić spójność danych w systemie P1 poza słownikami wykorzystuje się dane rejestrowe. W tym celu zapewnia się pozostałym podsystemom dostęp do danych o charakterze referencyjnym.

Podsystem SRR udostępnia Centralny Wykaz Usługodawców m.in. podsystemom w szczególności na potrzeby:

- SWD w celu prowadzenia weryfikacji danych,
- AUA w celu wskazania usługodawcy realizującego skierowanie,
- IKP w celu konfiguracji mechanizmu preautoryzacji, zasilenia rejestru,
- SAZ w celu wsparcia obsługi kont i autoryzacji,
- ASR w celu udostępnienia rejestru hurtowni danych.

Podsystem SRR udostępnia Centralny Wykaz Usługodawców systemom dziedzinowym, o których mowa w ustawie o systemie informacji w ochronie zdrowia:

- Systemowi Monitorowania Kształcenia - SMK,
- Systemowi Monitorowania Zagrożeń - SMZ.

1.2 Zakres danych

Zawartość wpisu do Centralnego Wykazu Usługodawców reguluje art. 16 ustawy o systemie informacji w ochronie zdrowia (Dz. U. 2011 Nr 113 poz. 657).

2 OBSZAR CENTRALNEGO WYKAZU USŁUGOBIORCÓW

2.1 Opis usług biznesowych obszaru

2.1.1 Zasilenie i aktualizacja Centralnego Wykazu Usługobiorców

Podsystemu ZDP zapewni mechanizm aktualizacji wpisów w Centralnym Wykazie Usługobiorców, na podstawie danych otrzymanych z Rejestru PESEL oraz podsystemu IKP, w którym usługobiorca zaktualizował własne dane. W komunikacji pomiędzy PESEL oraz IKP a ZDP uczestniczyć będzie SUS. Podsystem ZDP na podstawie przekazanych danych dokona aktualizacji Centralnego Wykazu Usługobiorców w podsystemie SRR.

2.1.2 Udostępnianie Centralnego Wykazu Usługobiorców

Aby zapewnić spójność danych w systemie P1, poza słownikami, wykorzystuje się dane rejestrowe. W tym celu zapewnia się pozostałym podsystemom dostęp do danych o charakterze referencyjnym.

Podsystem SRR udostępnia Centralny Wykaz Usługobiorców podsystemom, w szczególności na potrzeby:

- SWD w celu prowadzenia weryfikacji,
- AUA dla realizacji funkcjonalności obsługi pacjenta,
- IKP w celu prezentacji danych pacjenta,
- ZDP w celu jego aktualizacji i zarządzania nim,
- SAZ w celu blokowania kont użytkowników,
- ASR na potrzeby analiz i raportów w hurtowni danych,

Podsystem SRR udostępnia Centralny Wykaz Usługobiorców systemom dziedzicznym:

- SMK,
- SMZ.

2.2 Zakres danych

Zawartość wpisu do Centralnego Wykazu Usługobiorców reguluje art. 15 Ustawy o systemie informacji w ochronie zdrowia (Dz. U. 2011 Nr 113 poz. 657).

3 OBSZAR CENTRALNEGO WYKAZU PRACOWNIKÓW MEDYCZNYCH

3.1 Opis usług biznesowych obszaru

3.1.1 Zasilenie i aktualizacja Centralnego Wykazu Pracowników Medycznych

Podsystem ZDP zapewni mechanizm aktualizacji wpisów w Centralnym Wykazie Pracowników Medycznych, na podstawie danych otrzymanych z:

- Centralnego Rejestru Lekarzy,
- Centralnego Rejestru Pielęgniarek i Położnych,
- Centralnego Rejestru Farmaceutów,
- Rejestru Diagnostów Laboratoryjnych,

W komunikacji pomiędzy Centralnymi Rejestrami Lekarzy oraz Pielęgniarek i Położnych a ZDP uczestniczyć będzie SUS. Podsystem ZDP na podstawie przekazanych danych dokona aktualizacji Centralnego Wykazu Pracowników Medycznych w podsystemie SRR.

3.1.2 Udostępnianie Centralnego Wykazu Pracowników Medycznych

Aby zapewnić spójność danych w Systemie P1, poza słownikami wykorzystuje się dane rejestrowe. W tym celu zapewnia się pozostałym podsystemom dostęp do danych o charakterze referencyjnym.

Podsystem SRR udostępnia Centralny Wykaz Pracowników Medycznych podsystemom, w szczególności na potrzeby:

- SWD w celu prowadzenia weryfikacji danych,
- AUA w celu wsparcia zakładania kont,
- IKP w celu wsparcia konfiguracji preautoryzacji,
- ZDP w celu przeglądu rejestru oraz jego zasilenia,
- SAZ w celu wsparcia obsługi kont oraz mechanizmów autoryzacji,
- ASR w celu zasilania hurtowni danych,

3.2 Zakres danych dla Obszaru Biznesowego

Zawartość wpisu do Centralnego Wykazu Pracowników Medycznych reguluje art. 17 ustawy o systemie informacji w ochronie zdrowia (Dz. U. 2011 Nr 113 poz. 657).

4 OBSZAR REJESTRU LEKÓW

4.1 Opis usług biznesowych obszaru

4.1.1 Zasilanie i aktualizacja Rejestru Leków

Podsystemu ZDP zapewni mechanizm aktualizacji wpisów w Rejestrze Leków na podstawie danych otrzymanych z:

- Rejestru Produktów Leczniczych,
- Systemu Obsługi List Refundacyjnych.

Podsystem ZDP na podstawie przekazanych danych dokona aktualizacji Rejestru Leków w podsystemie SRR.

4.1.2 Udostępnianie Rejestru Leków

Podsystem SRR udostępnia Rejestr Leków podsystemom, w szczególności na potrzeby:

- SWD w celu prowadzenia weryfikacji,
- AUA pozwalając wskazać produkt leczniczy na receptach,
- ZDP w celu jego aktualizacji i zarządzania nim,
- ASR na potrzeby analiz i raportów w hurtowni danych.

4.2 Zakres danych

Zawartość wpisu do Rejestru Leków obejmuje zakres danych Centralnego Wykazu Produktów Leczniczych, regulowany art. 17a Ustawy o systemie informacji w ochronie zdrowia, za wyjątkiem danych dot. środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych, a także za wyjątkiem punktów 2j), 2m), 3 i 4.

5 OBSZAR REJESTRU PŁATNIKÓW

5.1 Opis usług biznesowych obszaru

5.1.1 Zasilenie i aktualizacja rejestru płatników

Administrator podsystemu ZDP z poziomu graficznego interfejsu użytkownika będzie miał możliwość dodawania, modyfikowania i usuwania wpisów w rejestrze płatników. Podsystem ZDP zrealizuje operacje wskazane przez administratora przekazując żądanie zmiany rejestru płatników w podsystemie SRR.

5.1.2 Udostępnianie rejestru płatników

Aby zapewnić spójność danych w systemie P1, poza słownikami, wykorzystuje się dane rejestrowe. W tym celu zapewnia się pozostałym podsystemom dostęp do danych o charakterze referencyjnym.

Podsystem SRR udostępnia rejestr płatników podsystemom, w szczególności na potrzeby:

- SWD w celu prowadzenia weryfikacji,
- AUA pozwalając wskazać płatnika w danych recepty, skierowania czy zdarzenia medycznego,
- ZDP w celu jego aktualizacji i zarządzania nim,
- ASR na potrzeby analiz i raportów w hurtowni danych.

5.2 Zakres danych

Zawartość wpisu do rejestru płatników obejmuje w szczególności:

- identyfikator płatnika;
- nazwę płatnika.

6 OBSZAR DOSTĘPU DO DANYCH

6.1 Opis usług biznesowych obszaru

6.1.1 Nadawanie uprawnień przez usługobiorców (Deklaracja Zgody Pacjenta)

W systemie P1 usługobiorcy decydują o tym komu nadać dostęp do własnych danych. W aplikacji IKP usługobiorca wskazuje:

- komu (poprzez wskazanie usługodawcy, w tym jego poziomu struktury organizacyjnej lub konkretnego pracownika medycznego bez kontekstu usługodawcy),
- do czego (rodzaj udostępnianych danych/kategorie uprawnień:
 - recepty,
 - skierowania,
 - zdarzenia medyczne i powiązane z nimi indeksy elektronicznej dokumentacji medycznej),
- na jaki okres nadaje uprawnienia do własnych danych (poprzez określenie daty, do której ma obowiązywać nadane uprawnienie),
- z jakiego okresu mają pochodzić dane lub/i dokumenty medyczne, do których nadawane są uprawnienia.

Po określeniu tych atrybutów dane (Deklaracja Zgody Pacjenta) przesyłane są przez SUS do SAZ, który tworzy i przechowuje uprawnienia.

6.1.2 Dostęp do szczegółów nadanych uprawnień dostępów do danych oraz odbieranie uprawnień

Podsystem IKP zapewni usługobiorcom możliwość przeglądania listy nadanych uprawnień dostępów do danych oraz wyświetlenia ich szczegółów, a także odebrania uprawnień dostępów do danych. W przypadku odbierania uprawnień dostępów do danych IKP przesyła za pośrednictwem SUS żądanie do SAZ, który realizuje operację.

6.1.3 Nadanie uprawnień na wniosek pracownika medycznego (Wniosek o dostęp do danych pacjenta)

W celu nadania uprawnień dostępu do danych usługobiorcy, który nie nadał tego prawa przed wizytą u usługodawcy pracownik medyczny tworzy elektroniczny dokument wniosku o dostęp do danych, który podpisuje i przesyła do P1. Dokument za pośrednictwem SUS trafia do SWD, który dokonuje jego weryfikacji, a następnie zwraca wynik na SUS, która w przypadku pozytywnej weryfikacji przekazuje dokument do SAZ w celu zapisania dokumentu oraz wygenerowania kodu autoryzującego (który zostanie przekazany usługobiorcy w ramach

funkcjonalności powiadomień). SAZ zwraca wynik zapisu dokumentu na SUS, która przekazuje wynik całej operacji zapisu dokumentu do systemu, który inicjował operację zapisu. W przypadku wystąpienia błędów związanych z zapisaniem wniosku zostaną one zwrócone w celu poprawy treści wniosku. Pracownik medyczny po otrzymaniu kodu autoryzacyjnego od usługobiorcy wprowadza kod do systemu, z którego wystawił wniosek. Kod wraz z identyfikatorem wniosku zostanie przekazany za pośrednictwem SUS do SAZ w celu nadania uprawnienia dostępu do danych usługobiorcy. W przypadku błędnego podania kodu dla danego identyfikatora usługodawca będzie mógł ponowić aktywację dostępu do danych usługobiorcy jeszcze dwa razy. Po trzech błędnych próbach aktywowania uprawnień wnioski zostaną zablokowane.

6.1.3.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie wniosku o przechowywane w P1 dane pracownika medycznego, usługodawcy, usługobiorcy oraz unikalny numer dokumentu nadany w podsystemie SAZ. W systemie AUA będzie możliwość wyświetlenia wniosków złożonych przez pracownika medycznego oraz na aktywację uprawnień poprzez wprowadzenie kodu otrzymanego od usługobiorcy.

6.1.3.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem wniosku zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru wniosku generowanego w systemie usługodawcy odpowiada usługodawca.

6.1.4 Autoryzacja dostępu do danych

Każde działanie związane z dostępem do danych gromadzonych w systemie i wywołania usług wymaga weryfikacji prawa do ich wywołania, którą realizuje podsystem SAZ. Podsystemy P1 (IKP, AUA) oraz systemy usługodawców chcąc pobrać dane z P1 przesyłają przez SUS zapytanie, które trafia do SAZ. Podsystem SAZ tworzy decyzję autoryzacyjną, która wraz z zapytaniem jest przekazywana do podsystemów gromadzących dane. Następnie podsystemy gromadzące dane zwracają wynik zapytania do systemów żądających dostępu do danych za pośrednictwem SUS.

Decyzję autoryzacyjną stanowi komunikat żądania ograniczony w swoim zakresie do uprawnień wynikających z:

- ról (zgodnie z Macierzą ról i uprawnień),
- kontekstu usługodawcy,
- reguł dostępu do danych (zgodnie z Regułami dostępu do danych),

- uprawnień wynikających z Deklaracji Zgody Pacjenta oraz Wniosku o dostęp do danych,
- parametrów globalnych.

Przykład: pracownik medyczny, który otrzymał uprawnienia dostępu do recept z marca 2015 r. przesyła żądanie o dostęp do wszystkich recept pacjenta. Podsystem SAZ przekazuje do SGR żądanie dostępu do wszystkich recept pacjenta wyłącznie z marca 2015 r.

6.2 Zakres danych

Zakres danych przetwarzanych w obszarze obejmuje w szczególności:

- Deklarację Zgody Pacjenta:
 - identyfikator dokumentu,
 - typ dokumentu,
 - data utworzenia,
 - wskazanie na usługobiorcę, którego dane dotyczą,
 - autor (np. pełnomocnik),
 - pracownik medyczny lub usługodawca (podmiot, któremu nadajemy uprawnienia z dokładnością do poziomu struktury organizacyjnej),
 - kategoria uprawnień,
 - okres obowiązywania.
- Wniosek o dostęp do danych pacjenta:
 - identyfikator dokumentu,
 - typ dokumentu,
 - data utworzenia,
 - wskazanie na usługobiorcę, którego dane dotyczą,
 - autor,
 - pracownik medyczny,
 - usługodawca,
 - kategoria uprawnień,
 - okres obowiązywania (udostępnianych danych),

- podpis elektroniczny.
- Dane związane z wnioskiem o dostęp do danych pacjenta, które są wymagane do nadania uprawnień:
 - kod autoryzacji dostępu do danych,
 - status wniosku (Utworzony/Aktywny/Zablokowany),
 - liczba prób potwierdzenia.
- Uprawnienia dla poszczególnych ról biznesowych określono w Tabeli 1. Macierz ról i uprawnień.

6.3 Obszar dostępu do danych – reguły

6.3.1 Ogólne

REG.OG.001	Każdy pracownik usługodawcy posiada uprawnienia do danych przez siebie wytworzonych.
REG.OG.002	Każdy usługobiorca posiada uprawnienia dostępu do swoich danych i danych osób, których jest pełnomocnikiem.

6.3.2 Recepty elektroniczne

REG.RCP.001	Pracownik apteki uprawnienia do danych uzyskuje wyłącznie na podstawie klucza lub kodu autoryzacyjnego recepty elektronicznej.
REG.RCP.002	NFZ posiada dostęp do wszystkich recept elektronicznych, realizacji których są odpłatne na poziomie mniejszym niż 100%.
REG.RCP.003	Oddziały NFZ posiadają dostęp do wszystkich recept elektronicznych, realizacji których są odpłatne na poziomie mniejszym niż 100%, i w których oddział oznaczony jest jako płatnik.
REG.RCP.004	Pracownik apteki musi mieć dostęp do wszystkich recept farmaceutycznych oraz dokumentów realizacji recept wytworzonych przez siebie i powiązanych z nimi recept elektronicznych.

6.3.3 Skierowania elektroniczne

REG.SKR.001	Pracownik usługodawcy uprawnienia do zmiany statusu skierowania elektronicznego uzyskuje wyłącznie na podstawie klucza lub kodu autoryzacyjnego skierowania elektronicznego.
REG.SKR.002	Każdy pracownik usługodawcy posiada uprawnienia do odczytu wszystkich skierowań elektronicznych realizowanych u tego usługodawcy.

REG.SKR.003	NFZ posiada dostęp do skierowań elektronicznych, w realizacjach których jest oznaczony jako płatnik.
--------------------	--

6.3.4 Wymiana elektronicznej dokumentacji medycznej

REG.WDM.001	Usługobiorca może pobierać swoje dokumenty.
REG.WDM.002	Usługobiorca może pobierać dokumenty osób, których jest pełnomocnikiem.

Tabela 1. Macierz ról i uprawnień

Uprawnienia\Role		Lekarz / lekarz dentysta / Felczer	Pielęgniarka / Położna	Pracownik ratownictwa	Inny profesjonalista	Personel administracyjny	Farmaceuta (poza AUA)	Technik farmacji (poza AUA)	Administrator lokalny	Usługobiorca	Pełnomocnik	Usługobiorca małoletni	Użytkownik SOW	Administrator biznesowy P1
RECEPTY														
	Wystawianie Recept	x	x											
	Anulowanie wystawionej recepty	x	x											
	Przeglądanie wystawionych recept	x	x				x	x		x	x	x		
	Pobieranie recept do realizacji						x	x						
	Realizowanie recept lekarskich						x	x						
	Wyszukiwanie realizacji recept						x	x						
	Przeglądanie historii zrealizowanych recept						x	x		x	x	x		
	Eksport informacji o zrealizowanych receptach do pliku						x	x						
	Wystawianie i realizacja recepty farmaceutycznej						x							



CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Uprawnienia\Role		Lekarz / lekarz dentysta / Felczer	Pielegniarka / Położna	Pracownik ratownictwa	Inny profesjonalista	Personel administracyjny	Farmaceuta (poza AUA)	Technik farmacji (poza AUA)	Administrator lokalny	Uslugobiorca	Pełnomocnik	Uslugobiorca maloletni	Użytkownik SOW	Administrator biznesowy P1
	Przeglądanie szczegółów leków	x	x	x			x	x		x	x	x		
	Przeglądanie zamienników dla leków	x	x	x			x	x						
SKIEROWANIA														
	Wystawianie skierowania	x												
	Anulowanie wystawionego skierowania	x												
	Przeglądanie wystawionych skierowań	x								x	x	x		
	Zmiana statusu skierowania	x	x		x	x								
ZDARZENIA MEDYCZNE														
	Rejestracja zdarzenia medycznego / indeksu dokumentacji	x	x	x	x	x								



Uprawnienia\Role		Lekarz / lekarz dentysta / Felczer	Pielegniarka / Położna	Pracownik ratownictwa	Inny profesjonalista	Personel administracyjny	Farmaceuta (poza AUA)	Technik farmacji (poza AUA)	Administrator lokalny	Usługobiorca	Pełnomocnik	Usługobiorca maloletni	Użytkownik SOW	Administrator biznesowy P1
	Modyfikacja danych zdarzenia lub indeksu dokumentacji powiązanej ze zdarzeniem	x	x	x	x	x								
	Anulowanie zdarzenia medycznego	x	x	x	x	x								
	Przeglądanie zdarzenia medycznego lub indeksu	x	x	x	x	x				x	x	x		
DOSTĘP DO DANYCH i EDM														
	Autoryzowanie dostępu do danych medycznych usługobiorcy	x	x		x	x				x	x	x		
	Wycofanie wniosku o zgodę na dostęp do danych medycznych									x	x	x		
	Składanie wniosku o pobranie dokumentacji medycznej	x				x				x	x	x		



CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel.: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Uprawnienia\Role		Lekarz / lekarz dentysta / Felczer	Pielęgniarka / Położna	Pracownik ratownictwa	Inny profesjonalista	Personel administracyjny	Farmaceuta (poza AUA)	Technik farmacji (poza AUA)	Administrator lokalny	Usługobiorca	Pełnomocnik	Usługobiorca maloletni	Użytkownik SOW	Administrator biznesowy P1
	Przeglądanie złożonych wniosków o pobranie dokumentacji i dokumentów udostępniania	x				x				x	x	x		
	Pobranie dokumentacji medycznej	x				x				x	x	x		
	Akceptacja wniosków i tworzenie dokumentu specyfikującego udostępnianie	x				x								
DANE USŁUGODAWCY														
	Generowanie certyfikatów								x					
	Wpisanie informacji technicznych o obsłudze udostępniania EDM								x					
	Uzupełnienie innych informacji o usługodawcy								x					
	Rejestracja informacji o zapisach online na wizyty								x					





CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Uprawnienia\Role		Lekarz / lekarz dentysta / Felczer	Pielegniarka / Położna	Pracownik ratownictwa	Inny profesjonalista	Personel administracyjny	Farmaceuta (poza AUA)	Technik farmacji (poza AUA)	Administrator lokalny	Usługobiorca	Pełnomocnik	Usługobiorca maloletni	Użytkownik SOW	Administrator biznesowy P1
	Zarządzanie kanałami powiadomień	x	x		x	x			x	x		x	x	
	Zmiana hasła	x	x		x	x			x	x		x	x	
	Przeglądanie pełnomocników usługobiorcy									x	x	x		
	Zarządzanie uprawnieniami pełnomocników									x		x		
ADMINISTRACJA P1														
	Odczyt wniosków o założenie konta													x
	Akceptacja wniosków o założenie konta													x
	Konfiguracja szablonów powiadomień													x
	Konfiguracja parametrów globalnych													x
	Brakowanie dokumentów													x
	Archiwizacja dokumentów													x





CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska
tel.: +48 22 597-09-27 • fax: +48 22 597-09-47
biuro@csioz.gov.pl • www.csioz.gov.pl
Skrytka ESP: /csiozgovpl/skrytka

Uprawnienia\Role	Administrator biznesowy P1	Użytkownik SOW	Ustugobiorca małoletni	Pełnomocnik	Ustugobiorca	Administrator lokalny	Technik farmacji (poza AUA)	Farmaceuta (poza AUA)	Personel administracyjny	Inny profesjonalista	Pracownik ratownictwa	Pielęgniarka / Położna	Lekarz / lekarz dentysta / Felczer
Konfiguracja reguł walidacji	x												



7 OBSZAR KONT

7.1 Opis usług biznesowych obszaru

Architektura Systemu P1 zakłada wykorzystanie Systemu P2 jako elementu odpowiedzialnego za uwierzytelnienie usługobiorców oraz pracowników usługodawców. Takie rozwiązanie wymusza, aby niżej wymienieni użytkownicy posiadali tożsamość w P2, aby do uwierzytelnienia w P1 wykorzystywać metodę: login i hasło. System P2 przechowuje dwie instancje kont – jedną dla usługobiorców oraz drugą dla pracowników usługodawcy. Pozostali użytkownicy są uwierzytelniani mechanizmami P1.

7.1.1 Zakładanie kont użytkowników

Aby korzystać z aplikacji dostarczanych w ramach Systemu P1 wymagane jest posiadanie konta. W Systemie P1 zakłada się wykorzystanie następujących kont użytkowników:

- Konta Usługobiorców - w celu korzystania z IKP przez:
 - Usługobiorców
 - Usługobiorców małoletnich,
- Konta Pracowników Medycznych - w celu korzystania z AUA przez:
 - Lekarzy/lekarzy dentystów / Felczerów,
 - Pielęgniarki/Położne,
 - Innych profesjonalistów medycznych:
- Konta Personelu Administracyjnego u Usługodawcy w celu korzystania z AUA:
- Konta Administratorów Usługodawców, czyli osób wskazanych przez Usługodawcę do pełnienia roli administratora w celu korzystania z AUA,
- Konta Użytkowników Platformy Publikacyjnej:
 - Administratorów,
 - Redaktorów,
 - Moderatorów,

konta te nie będą przechowywane w module obsługi kont, lecz obsługiwane w całości w PPP.

- Konta Administratorów Biznesowych w celu administrowania Systemem P1 w warstwie biznesowej:

- Konta Administratorów Systemu P1 – w celu administrowania Systemem P1 w warstwie techniczno-systemowej. Konta Administratorów Systemu P1 nie będą przechowywane w module obsługi kont i zakładane będą poza Systemem P1;
- Konta Użytkowników SOW – w celu korzystania z SOW;
- W przypadku, gdy usługodawca posiada system, który wykorzystuje do wymiany danych z Systemem P1, wówczas dla jego użytkowników (poza administratorem systemu) nie jest wymagane zakładanie kont w Systemie P1. System usługodawcy w ramach realizacji poszczególnych usług deklaruje użytkownika oraz rolę, w której charakterze dany użytkownik występuje. Katalog ról, w których może występować pracownik usługodawcy jest ograniczony do listy ról zdefiniowanych w P1 i inicjalnie obejmuje on role: Lekarz/lekarz dentysta/Felczer, Pielęgniarka/Położna, Inny profesjonalista medyczny, Administrator Usługodawcy, Personel Administracyjny.

7.1.1.1 Konta Usługobiorców

Warunkiem założenia konta usługobiorcy w P1 jest konieczność posiadania profilu zaufanego lub kwalifikowanego podpisu elektronicznego (z identyfikatorem usługobiorcy).

7.1.1.1.1 Zakładanie konta usługobiorcy

Założenie konta usługobiorcy w P1 realizowane jest w oparciu o następujące działania:

1. Usługobiorca z poziomu PPP lub strony logowania IKP ma możliwość złożenia wniosku o założenie konta poprzez wybór opcji: „Załącz konto usługobiorcy”.
2. Usługobiorca w SOW (module SAA) uzupełnia elektroniczny formularz wniosku o założenie konta usługobiorcy.
3. Wniosek zostaje podpisany przez usługobiorcę jedną z dwóch metod, kwalifikowanym podpisem elektronicznym lub podpisem elektronicznym potwierdzanym profilem zaufanym, po czym trafia do SWD celem weryfikacji i po pozytywnej weryfikacji zostaje zapisany w SOW. Usługobiorcy składającemu wniosek o założenie konta zostaje wyświetlona w SOW informacja o założeniu konta lub błędnym przetworzeniu wniosku.
4. SOW przekazuje za pośrednictwem SUS żądanie utworzenia tożsamości w P2, a w podsystemie SAZ zostaje stworzone konto i przypisana zostaje rola usługobiorcy (zgodnie z Macierzą ról i uprawnień do OB.06), następuje powiązanie tożsamości w P2 z kontem SAZ. System P2 wysyła na wskazany we wniosku kontakt tymczasowe hasło do zmiany podczas pierwszego logowania. Dodatkowo P1 wygeneruje powiadomienie dla autora wniosku o zapisaniu wniosku.

7.1.1.1.2 Zakładanie konta usługobiorcy małoletniego

Usługobiorca małoletni z poziomu PPP lub strony logowania IKP ma możliwość złożenia wniosku o założenie konta poprzez wybór opcji: „Założ konto usługobiorcy małoletniemu”.

Pozostałe działania związane z zakładaniem kont osoby małoletniej (pomiędzy ukończonym 16, a 18 rokiem życia) jest realizowane w taki sam sposób jak w przypadku zakładania konta usługobiorcy 8.1.1.1.1. z tą różnicą, iż w kroku 4 Zakładania konta w przypadku usługobiorcy małoletniego przypisana zostaje rola usługobiorcy małoletniego (zgodnie z Macierzą ról i uprawnień do obszaru OBSZAR DOSTĘPU DO DANYCH).

W przypadku zakładania obu kont usługobiorcy system P1 będzie kontrolował wiek osoby wnioskującej celem zapewnienia przypisania właściwego typu konta usługobiorcy

7.1.1.2 Konta Pracowników Usługodawców

Warunkiem założenia konta pracownika medycznego w P1 jest poprawna weryfikacja danych pracownika z wniosku z danymi gromadzonymi w Centralnym Wykazie Pracowników Medycznych.

7.1.1.2.1 Zakładanie konta pracownikowi medycznemu

Konta dla pracowników podmiotu zakłada administrator systemu usługodawcy, który wykorzystuje dedykowany panel graficzny do tworzenia kont w aplikacji AUA. Administrator systemu usługodawcy realizuje to poprzez uzupełnienie danych pracownika medycznego (wypełniając formularz z danymi konta pracownika medycznego, część danych formularza zostaje wstępnie uzupełniona na podstawie danych z CWPM). Dane formularza trafiają za pośrednictwem SUS do P2 w celu utworzenia tożsamości w P2, a w podsystemie SAZ zostaje stworzone konto i przypisana zostaje rola pracownika medycznego wskazana przez Administratora systemu usługodawcy z listy dostępnych dla AUA ról (Lekarz/lekarz dentysta / Felczer, Pielęgniarka/Położna, Inny profesjonalista medyczny - zgodnie z Macierzą ról i uprawnień do obszaru OBSZAR DOSTĘPU DO DANYCH), następuje powiązanie tożsamości w P2 z kontem SAZ. System P2 wysyła na wskazany w danych kontakt tymczasowe hasło do zmiany podczas pierwszego logowania.

7.1.1.2.2 Zakładanie konta personelowi administracyjnemu usługodawcy

Zakładanie kont dla personelu administracyjnego usługodawcy jest realizowane w tożsamy sposób jak w przypadku zakładania konta pracownikowi medycznemu 8.1.1.2.1., z tą różnicą, że dane personelu administracyjnego nie będą automatycznie uzupełnione, a wszystkie konta są tworzone z rolą Personel Administracyjny- zgodnie z Macierzą ról i uprawnień do OB.06.

7.1.1.2.3 Zakładanie konta administratorowi usługodawcy

Konto dla pierwszego administratora usługodawcy w P1 realizowane jest w ramach zakładania konta podmiotu zgodnie z opisem ujętym w podrozdziale 8.1.4.



Konta kolejnych administratorów usługodawcy zakłada się w tożsamy sposób jak dla pozostałych pracowników usługodawcy zgodnie z 8.1.1.2.1., z tą różnicą, że dane personelu administracyjnego nie będą automatycznie uzupełnione, a wszystkie konta są tworzone z rolą Administrator Usługodawcy- zgodnie z Macierzą ról i uprawnień do obszaru OBSZAR DOSTĘPU DO DANYCH).

7.1.1.3 Zakładanie kont pozostałym użytkownikom Systemu P1

7.1.1.3.1 Zakładanie konta administratorowi biznesowemu

Zakładanie kont administratorom biznesowym jest realizowane przez Administratora Systemu P1. Administrator w ramach realizacji procedury administracyjnej dodaje konta administratorów biznesowych, które zostają zapisane w SAZ. Nowi użytkownicy otrzymają powiadomienie e-mail lub sms o utworzeniu konta oraz automatycznie wygenerowane hasło na adres e-mail.

7.1.1.3.2 Zakładanie konta administratorowi Systemu P1

Konta administratorów Systemu P1 nie są zakładane w sposób wspierany przez System P1, lecz w ramach oddzielnych procedur. Dane kont administratorów Systemu P1 nie są także przechowywane w podsystemie SAZ.

7.1.1.3.3 Zakładanie konta administratorom, redaktorom i moderatorom Platformy Publikacyjnej

Zakładanie kont dla administratorów, redaktorów i moderatorów PPP jest realizowane w ramach aplikacji PPP. Oparto je na standardowych funkcjonalnościach przyjętego narzędzia CMS.

7.1.1.3.4 Zakładanie konta w SOW

Administrator Systemu P1 nadaje uprawnienia dla użytkownika SOW, którzy odpowiadać będą za akceptowanie wniosków o założenie kont usługodawców i administratorów zgodnie z rozdziałem 8.1.1.3.1. Konta użytkowników SOW będą przechowywane w SAZ, a ich uwierzytelnienie także będzie realizowane w ramach SAZ, analogicznie do danych administratorów biznesowych.

7.1.2 Blokowanie, usuwanie i odblokowanie kont

7.1.2.1.1 Zablokowanie konta przez usługobiorcę

System P1 zapewni możliwość blokowania konta przez usługobiorcę, która polegać będzie na wskazaniu przez usługobiorcę w IKP takiej woli, a na jej podstawie IKP za pośrednictwem SUS przekaze do SAZ żądanie zablokowania konta oraz odebrania wszystkich uprawnień.

Zablokowanie konta przez Usługobiorcę w Systemie P1 nie będzie oznaczać zaprzestania gromadzenia danych danego Usługobiorcy w Systemie P1, co jest regulowane odpowiednimi przepisami prawa.



7.1.2.1.2 Odblokowanie konta przez usługobiorcę

Usługobiorcy, w tym małoletniemu zostanie zapewniona funkcjonalność odblokowania konta polegająca na złożeniu w SOW wniosku o odblokowanie konta (przekierowanie do wniosku zostanie zrealizowane w PPP oraz IKP). Wniosek po jego wypełnieniu i podpisaniu zostanie przekazany przez SUS do SWD celem weryfikacji. W przypadku pozytywnej weryfikacji wniosek zostanie zapisany w SOW, a SAZ odblokuje konto usługobiorcy, w przeciwnym przypadku usługobiorcy zostanie wyświetlony formularz ze wskazaniem błędów uniemożliwiający jego zapisanie.

7.1.2.1.3 Odbieranie uprawnień i usuwanie konta pracownika usługodawcy

Podsystem AUA zapewni możliwość odebrania poszczególnych ról, które pracownik usługodawcy pełni u usługodawcy. Odebranie roli polegać będzie na usunięciu relacji pomiędzy kontem i rolą pracownika usługodawcy. W przypadku gdyby usługodawca (występujący w jego imieniu administrator), który odbiera rolę pracownika usługodawcy, byłby ostatnim podmiotem/usługodawcą w kontekście którego pracował pracownik usługodawcy nastąpi całkowite usunięcie konta w P1.

W systemie P2 nie znajdą natomiast w związku z powyższym żadne zmiany.

7.1.2.1.4 Zablokowanie konta na podstawie informacji o zgonie usługobiorców oraz pracowników usługodawcy

W ramach procesu aktualizacji danych CWUb podsystem SRR będzie przekazywał informacje o zgonie do podsystemu SAZ, który na podstawie pozyskanych informacji dokona zablokowania konta oraz wszystkich uprawnień użytkownika lub odblokowania w przypadku anulowania informacji o zgodzie.

7.1.2.1.5 Blokowanie konta usługodawcy

Podsystem SOW zapewni możliwość złożenia uprawnionemu przedstawicielowi usługodawcy wniosku o zablokowanie konta usługodawcy oraz jego podpisania. Podpisany dokument zostanie przekazany za pośrednictwem SUS do SWD celem weryfikacji i po pozytywnej weryfikacji zostanie zapisany w SOW. P1 wygeneruje powiadomienie o złożeniu wniosku o zamknięcie konta dla usługodawcy. Jeżeli wniosek zostanie pozytywnie rozpatrzony przez uprawnionego użytkownika SOW, za pośrednictwem SUS zostanie przekazane żądanie zablokowania konta w SAZ.

Alternatywą dla powyższej funkcjonalności jest możliwość blokowania konta przez administratora P1 dostępna z podsystemu SAZ.

7.1.3 Zarządzanie kontem użytkownika

Podsystemy IKP oraz AUA zapewnią użytkownikom możliwość edycji danych konta (zależnych od typu konta) polegającą na przekazaniu z jednego z tych podsystemów przez SUS żądania modyfikacji danych konta w podsystemie SAZ i/lub systemie P2.

Podsystem SAZ zapewni użytkownikom SOW, SAA oraz SWD interfejs graficzny umożliwiający uwierzytelnienie do tych aplikacji oraz możliwość edycji danych konta.

Modyfikacji nie podlegają dane podstawowe takie jak imię, nazwisko, identyfikator.

Edycja danych umożliwia modyfikację hasła użytkownika, danych dodatkowych konta takich jak np. specjalizacje czy tytuł naukowy.

7.1.4 Zakładanie konta usługodawcy

W Systemie P1 poza kontami użytkowników będą zakładane konta usługodawców:

- podmiotów działalności leczniczej,
- praktyk zawodowych,
- aptek i punktów aptecznych

Zakładanie kont usługodawcy będzie realizowane:

- automatycznie – na podstawie danych z rejestrów źródłowych oraz
- automatycznie i manualnie – w ramach akceptacji składanego przez usługodawcę wniosku o założenie konta, przez uprawnionego użytkownika.

7.1.5 Zarządzanie kontem usługodawcy

Architektura Systemu P1 wymaga wykorzystania aplikacji AUA przez administratorów usługodawców posługujących się własnym systemem do celów zarządzania kontem usługodawcy.

Administrator podmiotu w aplikacji AUA będzie miał możliwość rejestracji systemu (punktu dostępowego) jeżeli do komunikacji z Systemem P1 będzie wykorzystywał własny system. Po wprowadzaniu i zatwierdzeniu danych systemu przez administratora lokalnego AUA za pośrednictwem SUS prześle do SAZ żądanie rejestracji systemu usługodawcy. Operacja jest dostępna dla określonej parametrem globalnym liczby punktów dostępowych dla jednego usługodawcy.

System AUA zapewni także, możliwość generowania identyfikatora systemu oraz certyfikatu, którym będzie posługiwał się system usługodawcy (z wykorzystaniem Centrum Certyfikacji). Zarządzania procesem generowania certyfikatu będzie realizowane z poziomu Centrum Certyfikacji, a identyfikatora systemu z poziomu podsystemu SAZ.

7.1.5.1 Zarządzanie kontami pracowników usługodawcy (przypisanie pracowników usługodawcy do ról i poziomów struktury organizacyjnej usługodawcy)

Podsystem AUA zapewni możliwość wskazania pracowników, którym administrator usługodawcy przypisze role pełniące u usługodawcy, w szczególności pracownik np. z powodu zakończenia świadczenia pracy nie będzie miał przypisanej żadnej roli. Administrator usługodawcy podaje identyfikator pracownika, AUA za pośrednictwem SUS weryfikuje w SAZ czy konto dla wskazanej osoby istnieje oraz pobiera dane w celu przypisania pracownika do danej roli (zgodnie z Macierzą ról i uprawnień do OB.06 - OBSZAR DOSTĘPU DO DANYCH) i poziomu struktury organizacyjnej usługodawcy (na podstawie danych z RPWDL) w AUA, o czym decyduje administrator usługodawcy. AUA dla wskazanej funkcjonalności przekaże za pośrednictwem SUS żądanie zmiany uprawnień w podsystemie SAZ. Pracownik usługodawcy otrzyma z P1 powiadomienie o zmodyfikowaniu uprawnień w kontekście usługodawcy.

7.1.6 Zakładanie kont podmiotów administracji publicznej i rejestracja ich systemów

Zakładanie kont dla podmiotów administracji publicznej i rejestracja ich systemów będzie realizowane przez administratora Systemu P1, który wygeneruje certyfikat do komunikacji systemu administracji publicznej z Systemem P1 oraz, w trybie komunikacji urzędowej, poinformuje podmiot o fakcie rejestracji.

7.1.7 Logowanie do aplikacji IKP oraz AUA

Podsystemy odpowiednio IKP oraz AUA zapewnią interfejs graficzny do logowania użytkowników. Po wprowadzeniu loginu i hasła dane trafią z podsystemu IKP/AUA przez SUS do P2, który dokona uwierzytelnienia użytkownika. Z poziomu interfejsu graficznego do logowania użytkownikom zapewnione zostanie przejście do złożenia wniosków o założenie konta w SOW. Ponadto w przypadku zapomnienia hasła zapewniono zostanie możliwość wywołania usługi resetu hasła w przypadku jego braku po uprzednim podaniu loginu użytkownika, wówczas IKP lub AUA przekaże za pośrednictwem SUS do P2 żądanie resetu hasła.

7.1.8 Zarządzanie rolami i uprawnieniami w Systemie P1

Podsystem SAZ zapewni administratorowi Systemu P1 możliwość zarządzania rolami (definiowania, usuwania, modyfikacji) i uprawnieniami przypisanymi do poszczególnych ról.

7.1.9 Wyszukiwanie i podgląd wniosków

Podsystem SOW zapewni możliwość dla użytkowników z uprawnieniami do potwierdzania kont usługodawców oraz administratorów wyszukiwania złożonych wniosków, ich przeglądania i akceptacji bądź odrzucenia.

7.2 Zakres danych

Zakres danych obszaru kont w szczególności powinien uwzględniać:

Dane wniosków o założenie konta:

- Usługobiorcy:
 - Identyfikator wniosku
 - Imiona
 - Nazwisko
 - PESEL
 - Email (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
 - Numer telefonu (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
 - Adres zamieszkania/korespondencji
- Usługobiorcy małoletniego:
 - Identyfikator wniosku
 - Imiona
 - Nazwisko
 - PESEL
 - Email (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
 - Numer telefonu (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
 - Identyfikator opiekuna
- Podmiotu:
 - Identyfikator wniosku
 - Rodzaj podmiotu
 - Nazwa
 - REGON
 - Numer Księgi Rejestrowej
 - Adres
 - Numer telefon
 - Email
 - Dane osoby reprezentującej podmiot
 - Załączniki do wniosku

- Dane administratora podmiotu:
 - Imiona
 - Nazwisko
 - PESEL
 - Email (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
 - Numer telefonu (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
- Status wniosku

Zakres danych formularza Pracownika Medycznego/Personelu Pracującego w podmiocie:

- Identyfikator wniosku
- Imiona
- Nazwisko
- Numer Prawa Wykonywania Zawodu
- PESEL
- Typ dokumentu tożsamości
- Rodzaj dokumentu tożsamości
- Email (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)
- Numer telefonu (Email lub Numer telefonu musi zostać podany, w celu przekazania hasła)

Dane wniosków o zablokowanie konta:

- Usługobiorcy:
 - Identyfikator wniosku
 - Imiona
 - Nazwisko
 - PESEL
 - Powód zablokowania
- Usługodawcy
 - Identyfikator wniosku



- Rodzaj podmiotu
- Nazwa
- REGON
- Numer Księgi Rejestrowej
- Powód zablokowania
- Dane osoby reprezentującej podmiot
- Załączniki do wniosku
- Status wniosku (dla wniosku o odblokowanie)

Dane wniosków o odblokowanie konta:

- Usługobiorcy:
 - Identyfikator wniosku
 - Imiona
 - Nazwisko
 - PESEL
 - Status wniosku (dla wniosku o odblokowanie)

Zakres danych kont:

- Usługobiorcy:
 - Login
 - Imiona
 - Nazwisko
 - PESEL
 - Typ dokumentu tożsamości
 - Rodzaj dokumentu tożsamości
 - Data urodzenia
 - Status konta
 - Identyfikator techniczny w P2
 - Numer telefonu
 - Email
 - Dane dodatkowe

- Rodzaj konta (usługobiorcy/usługobiorcy małoletniego)
 - Data urodzenia
 - Powiązania pomiędzy kontami (relacja pełnomocnictwa)
 - Data nadania pełnomocnictwa
 - Data odebrania/rezygnacji z pełnomocnictwa
- Pracownika usługodawcy:
 - Login
 - Imiona
 - Nazwisko
 - PESEL
 - Numer Prawa Wykonywania Zawodu
 - Typ dokumentu tożsamości
 - Rodzaj dokumentu tożsamości
 - Data urodzenia
 - Status konta
 - Identyfikator techniczny w P2
 - Numer telefonu
 - Email
 - Dane dodatkowe
 - Przypisanie konta pracownika do roli i poziomu struktury organizacyjnej
- Podmiotu:
 - Identyfikator OID podmiotu
 - Status konta
 - Rodzaj podmiotu
 - Nazwa
 - REGON
 - NIP
 - Numer Księgi Rejestrowej
 - Adres

- Numer telefon
- Email
- Dane osoby reprezentującej podmiot
- Dane administratora podmiotu
- Konfiguracja kanałów powiadomień
- Informacja o punktach dostępowych:
 - Adres IP
 - Lokalizacja serwerowni
 - Identyfikator systemu
- Dane dodatkowe
- Administratorów biznesowych/Użytkowników SOW:
 - Identyfikator wniosku
 - Imiona
 - Nazwisko
 - PESEL
 - Typ dokumentu tożsamości
 - Rodzaj dokumentu tożsamości
 - Email
 - Numer telefonu
 - Konfiguracja kanałów powiadomień
 - Login
 - Hasło
- Role biznesowe i zdefiniowane uprawnienia, które mogą być przypisane do poszczególnych ról.

8 OBSZAR PEŁNOMOCNIKÓW I OPIEKUNÓW

8.1 Opis usług biznesowych obszaru

8.1.1 Ustanawianie pełnomocnika

W celu zapewnienia kompleksowej funkcjonalności oraz użyteczności dla usługobiorców, w systemie P1 udostępniona zostanie użytkownikom IKP możliwość nadawania pełnomocnictwa do obsługi konta innego użytkownika P1 (zgodnie z Macierzą ról i uprawnień do OB.06). Pełnomocnictwo uprawnia pełnomocnika do dostępu do danych mocodawcy gromadzonych w systemie oraz daje możliwość wnioskowania w imieniu mocodawcy o jego dokumentację. Każdy użytkownik posiadający konto w IKP w celu nadania pełnomocnictwa wskazuje, poprzez podanie danych –użytkownika, któremu chce nadać pełnomocnictwo do konta oraz zatwierdza operację. IKP przesyła za pośrednictwem SUS do podsystemu SAZ żądanie zapisania relacji pełnomocnictwa pomiędzy użytkownikami. W komunikacie zwrotnym przekazany przez SUS użytkownik aplikacji IKP uzyska informacje o wyniku operacji. Podsystem SAZ po utworzeniu relacji pełnomocnictwa przekaże żądanie utworzenia powiadomienia wysłanego do pełnomocnika.

8.1.2 Przeglądanie i odbieranie nadanych pełnomocnictw

Podsystem IKP zapewni użytkownikom możliwość przeglądania listy nadanych przez nich pełnomocnictw oraz z poziomu jej przeglądania odebrania tych uprawnień. IKP, za pośrednictwem SUS pobierze listę pełnomocnictw (lub usunie pełnomocnictwo) w podsystemie SAZ.

8.1.3 Przeglądanie i rezygnacja z otrzymanych pełnomocnictw

Podsystem IKP zapewni użytkownikom możliwość przeglądania listy otrzymanych pełnomocnictw oraz z poziomu jej przeglądania rezygnacji z pełnomocnictwa. IKP, za pośrednictwem SUS pobierze listę (lub usunie pełnomocnictwo) w podsystemie SAZ.

8.2 Zakres danych

Zakres danych listy pełnomocnictw powinien zawierać w szczególności:

- Identyfikator użytkownika
- Imię
- Nazwisko
- Data nadania pełnomocnictwa
- Data odebrania/rezygnacji z pełnomocnictwa
- Status pełnomocnictwa:
 - Aktywne



- Nieaktywne

Zakres danych przetwarzanych w obszarze w szczególności zawiera się w zdefiniowanym zakresie dla obszaru kont (OBSZAR KONT).

9 OBSZAR ADMINISTRACJI BIZNESOWEJ

9.1 Opis usług biznesowych obszaru

9.1.1 Obsługa parametrów globalnych

Podsystem SAA udostępni administratorowi P1 graficzny interfejs do zarządzania i konfiguracji parametrów globalnych, pozwalających sterować systemem. Administrator będzie miał możliwość definiować parametry globalne, zmieniać ich wartość i odczytywać wartość bieżących parametrów w poszczególnych podsystemach.

Podsystemy P1 w momencie ich uruchomienia pobierać będą, przy wykorzystaniu SUS z podsystemu SAA wszystkie niezbędne do ich działania parametry konfiguracyjne. W przypadku pozytywnego pobrania i zmiany parametru przez podsystem P1, SAA odnotuje obsługiwaną wartość parametru w podsystemie SAA. W przypadku nieudanego pobrania i nieskutecznej zmiany parametru, podsystem ponowi operację, gdy to także nie przyniesie skutku podsystem pobierający parametr z SAA zakończy działanie.

Administrator P1 ma możliwość zmiany parametru w danej chwili lub może zaplanować termin zmiany parametru w systemie, wówczas informacja o zmianie parametru zostanie przez SUS przekazana do wszystkich podsystemów, które obsługują parametr w czasie, od którego ma obowiązywać nowy parametr. Podsystemy pobiorą i zaktualizują wartość obsługiwanego parametru, jeżeli ta operacja się nie powiedzie podsystemy będą ponawiać operację i do czasu realizacji zmiany będą działać według poprzedniej wersji i wartości parametru.

Administrator P1 w SAA z poziomu graficznego interfejsu będzie miał możliwość pobrania rzeczywistej, bieżącej wartości dowolnego parametru globalnego z podsystemów P1.

9.1.2 Archiwizacja

Podsystem SGR (dla dokumentów recept i realizacji recept oraz dokumentów anulowania recepty), SGS (dla dokumentów skierowań i dokumentów anulowania skierowania) i SGZ (dla zdarzeń medycznych i indeksów elektronicznej dokumentacji medycznej) zapewnią funkcjonalności zarządzania mechanizmem archiwizacji dokumentów i metadanych gromadzonych w P1. Administrator P1 będzie miał możliwość:

- wskazania dokumentów podlegających archiwizacji, także przez określenia ich zbioru poprzez wskazanie okresu, z którego pochodzą,
- uruchomienia/wstrzymania/ponowienia/anulowania archiwizacji,
- monitorowania procesu archiwizacji,
- prezentacji listy identyfikatorów dokumentów podlegających archiwizacji oraz informacji, dla których zakończyła się ona niepowodzeniem, w przypadku wystąpienia niepowodzenia archiwizacji,

- przywrócić zarchiwizowane dokumenty i metadane ze wskazanego archiwum.

9.1.3 Brakowanie

Podsystem SGR (dla dokumentów recept i realizacji recept oraz dokumentów anulowania recepty), SGS (dla dokumentów skierowań i dokumentów anulowania skierowania) i SGZ (dla zdarzeń medycznych i indeksów elektronicznej dokumentacji medycznej) udostępnią administratorowi P1 funkcjonalności zarządzania mechanizmem brakowania dokumentów i metadanymi gromadzonych w P1. Administrator SAA, będzie miał możliwość:

- wskazania dokumentów podlegających brakowaniu wraz z metadanymi, także przez określenia ich zbioru przez wskazanie okresu z którego pochodzą,
- uruchomienia/wstrzymania/ponowienia/anulowania brakowania,
- monitorowania procesu brakowaniu,
- prezentacji listy identyfikatorów dokumentów podlegających brakowaniu oraz informacji dla których zakończyło się ono niepowodzeniem , w przypadku wystąpienia niepowodzenia brakowania.

9.2 Zakres danych

Zakres danych parametrów globalnych obejmuje w szczególności:

- Identyfikator
- Wersja
- Nazwa
- Data obowiązywania
- Status (aktywny/nieaktywny)
- Autor utworzenia/modyfikacji parametru
- Data i czas utworzenia/modyfikacji parametru
- Informacje o obsługiwanej wersji parametru w poszczególnych podsystemach
- Wartość parametru – tekst, liczba, plik XML

Zakres danych dla archiwizacji obejmuje w szczególności:

- Nazwa archiwum
- Data i czas utworzenia
- Dokumenty
- Metadane dokumentów



- Informacja o wyniku archiwizacji:
 - Identyfikator dokumentu
 - Informacja o wyniku archiwizacji dokumentu

Zakres danych informacji o wyniku brakowania obejmuje w szczególności:

- Identyfikator dokumentu
- Informacja o wyniku brakowania dokumentu.

10 OBSZAR AUDYTU

10.1 Opis usług biznesowych obszaru

10.1.1 Kolekcja logów

Podsystem SAU będzie posiadał funkcjonalności umożliwiające kolekcjonowanie 3 rodzajów logów:

- dotyczących udostępniania danych osobowych (logi UDO), zawierających w szczególności informacje wymagane art. 34 ustawy o systemie informacji w ochronie zdrowia oraz zapewniających spełnienie wymagań regulowanych ustawą o ochronie danych osobowych art. 32 i 33,
- zawierających informacje audytowe (logi audytu) umożliwiające skorelowanie zdarzeń technicznych z uruchomieniami usług biznesowych,
- zawierających dane techniczne (logi techniczne) generowane przez oprogramowanie oraz sprzęt.

Z uwagi na różny charakter logów możliwe są różne sposoby ich kolekcji. W przypadku logów UDO oraz audytu zakłada się kolekcję pasywną (tzn. podsystemy P1 będą przekazywały logi do SAU). W przypadku logów technicznych dopuszcza się dodatkowo kolekcję aktywną (przy pomocy agentów instalowanych na komponentach generujących logi).

10.1.2 Udostępnianie logów

Przewiduje się 3 sposoby udostępniania logów. Podstawowym sposobem jest narzędzie klasy SIEM (pozostające częścią SAU), które umożliwiać będzie korelację wszystkich kategorii logów generowanych przez System P1. Głównym celem korelacji będzie wykrycie powiązania między akcją biznesową a zdarzeniami natury technicznej wykrytej na niższych poziomach.

Jako przykład można tu podać ruch wykryty na routerze brzegowym. Audytor będzie mieć możliwość przeprowadzenia korelacji logów routera z odpowiednim logiem audytu (najprawdopodobniej wykorzystując do tego logi poszczególnych serwerów uczestniczących w komunikacji). Brak takiego powiązania będzie oznaczał dla audytora incydent bezpieczeństwa związany z prawdopodobnym nieautoryzowanym wykorzystaniem systemu.

Jako narzędzie wspomagające dostępny będzie interfejs graficzny umożliwiający audytorowi przeglądanie i korelację wyłącznie logów audytu i UDO. Dopuszcza się w tym przypadku zastosowanie innych narzędzi korelacyjnych niż narzędzie klasy SIEM.

10.1.3 Archiwizacja logów

System P1 będzie posiadał narzędzie umożliwiające archiwizację logów UDO na zewnętrznych nośnikach. Dopuszcza się w tym miejscu wykorzystanie gotowych narzędzi dedykowanych do

tego celu. Wymagane jest jednocześnie aby administrator miał możliwość odszukania logów dotyczących konkretnej osoby, a czynność ta była skutecznie wspierana przez system.

10.1.4 Generowanie raportu z udostępnianych danych osobowych usługobiorcy

Zgodnie z art. 34 ustawy o systemie informacji w ochronie zdrowia System P1 będzie obsługiwał funkcjonalności udostępniania raportu z udostępniania danych osobowych.

Usługobiorcy, w podsystemie IKP, udostępniona zostanie funkcjonalność umożliwiająca złożenie wniosku o raport za dany okres. Wniosek będzie przekazywany, z pośrednictwem SUS, do podsystemu SAU i tam składowany. Podsystem SAU generował będzie odpowiedni raport i wysyłał go na adres e-mail zdefiniowany dla konta usługobiorcy.

Jednocześnie udostępniona będzie możliwość ręcznego wygenerowania raportu przez administratora w przypadku, w którym usługobiorca złożył wniosek w postaci papierowej.

Interfejs graficzny będzie umożliwiał administratorowi również ustalenie momentu, od którego przetwarzane są w systemie dane osobowe danego usługobiorcy na podstawie danych z CWUb, SGR, SGR, SGZ oraz SAZ.

10.2 Zakres danych

Dane wspólne dla logu audytu i logu udostępniania danych osobowych to m.in.:

- informacje o użytkowniku,
- informacje o systemie użytkownika,
- informacje o podmiocie, w kontekście którego działa użytkownik,
- informacje o ścieżce wywołań wewnątrz Systemu P1,
- informacje o danych będących przedmiotem zdarzenia.

Log audytu służy do analizy zdarzeń komunikacyjnych w systemie P1, w tym kolejności ich występowania, w zakresie m.in. wywołań usług, przyjmowania komunikatów zewnętrznych, faktu poprawności lub błędów zakończonego przetwarzania tych komunikatów. Log audytu nie może zawierać żadnych danych medycznych, musi natomiast posiadać wbudowane mechanizmy konfiguracyjne, np. ustalenie dla danego podsystemu czy logowane mają być wszystkie przypadki, czy tylko związane z błędami przetwarzania danych.

Dane zawarte w logu udostępniania danych osobowych są przedmiotem regulacji prawnych, m.in. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz art. 34 ustawy o systemie informacji w ochronie zdrowia i wynikającego z niego rozporządzenia. Jednocześnie w ramach logów UDO musi być przechowywana informacja o dacie rozpoczęcia przetwarzania danych osobowych.



Zakres danych logów urządzeń wynika ze specyfiki tych urządzeń. Zakres danych logu oprogramowania powinien być zgodny z typowym zakresem logów realizowanych przez biblioteki konkretnego rozwiązania technicznego, z zastosowaniem m.in. rozróżnienia konfigurowalnych poziomów logowania, kodu podsystemu zapisującego log, opcjonalnych parametrów kontekstu logowania, referencji do miejsca wywołania operacji logowania w kodzie oprogramowania, a także treści logu, której zawartość powinna w sposób wystarczający i jednocześnie minimalny opisywać logowane zdarzenie.



11 OBSZAR RECEPT

11.1 Opis usług biznesowych obszaru

11.1.1 Tworzenie i zapis recepty

Realizowane jest przez utworzenie i podpisanie elektronicznego dokumentu recepty przez pracownika medycznego oraz przesłanie do P1. W systemie obowiązuje zasada umieszczania tylko jednego produktu leczniczego na dokumencie recepty, natomiast zapewniona zostanie możliwość zapisania jednocześnie wielu recept. Wszystkie recepty dla tego samego usługobiorcy przekazywane do systemu P1 w ramach pojedynczego komunikatu zostaną połączone w pakiet. Podpisane recepty są przysyłane poprzez SUS do weryfikacji w podsystemie SWD, a następnie depersonalizowane i zapisywane z wynikami weryfikacji w podsystemie SGR. Przy zapisie w systemie tworzone są dane dostępne do pakietu recept oraz poszczególnych dokumentów recept, które zostaną zwrócone wystawcy dokumentu na potrzeby przekazania tych danych usługobiorcy. Dane dostępne do dokumentów umożliwiają dostęp do recept, w celu ich realizacji.

11.1.1.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA to usługa będzie dodatkowo zapewniała systemowe uzupełnianie recepty o przechowywane w P1 dane pracownika medycznego, usługodawcy, usługobiorcy oraz unikalny numer dokumentu nadany w podsystemie SGR. W systemie AUA będzie możliwość złożenie jednego podpisu pod wieloma dokumentami recept, w celu skrócenia czasu potrzebnego do ich wystawiania.

11.1.1.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem recepty zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru recepty generowanego w systemie usługodawcy odpowiada usługodawca.

11.1.2 Przekazanie usługobiorcy informacji o receptach w pakiecie, w tym kodów dostępowych

Po zapisaniu recept w P1 informacja o receptach w pakiecie, zawierająca też kody dostępne jest automatycznie przekazywana do usługobiorcy za pośrednictwem poczty elektronicznej oraz wiadomości tekstową na numer telefonu, w przypadku, gdy usługobiorca zdefiniuje takie kanały komunikacyjne, wykorzystując do tego aplikację IKP. Jeżeli usługobiorca nie posiada konta w aplikacji IKP lub za jej pomocą nie przekazał do P1 danych kontaktowych jedynym źródłem informacji o receptach i danych dostępowych dla pacjenta jest wydruk informacji o receptach w pakiecie realizowany przez aplikację AUA lub system usługodawcy.

11.1.3 Anulowanie recepty

Pracownik medyczny, który wystawił receptę ma możliwość jej anulowania, jeżeli nie została zrealizowana. Anulowanie recepty jest czynnością polegającą na utworzeniu i podpisaniu dokumentu anulowania oraz przesłaniu do P1. Podpisany dokument anulowania jest weryfikowany w podsystemie SWD, a następnie depersonalizowany i zapisywany z wynikami weryfikacji w podsystemie SGR. Jeżeli przedmiotem anulowania mają być wszystkie recepty z pakietu, należy anulować każdy z dokumentów niezależnie.

11.1.3.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA to usługa będzie dodatkowo zapewniała systemowe uzupełnianie dokumentu anulowania o dane zawarte w receptce, która będzie przedmiotem anulowania oraz unikalny numer dokumentu anulowania nadany w podsystemie SGR.

11.1.3.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem dokumentu anulowania recepty zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru dokumentu anulowania recepty generowanego w systemie usługodawcy odpowiada usługodawca.

11.1.4 Wystawianie recepty farmaceutycznej

Kierownik apteki tworzy w systemie aptecznym i podpisuje receptę farmaceutyczną, a następnie przesyła do systemu P1 wraz z dokumentem realizacji. Dokumenty przesłane poprzez SUS zostają poddane weryfikacji w podsystemie SWD, a następnie są depersonalizowane i zapisywane w podsystemie SGR. Wynik operacji zostaje zwrócony do systemu usługodawcy, jednakże w przeciwieństwie do pozostałych recept nie są tworzone dane dostępne do dokumentu recepty.

11.1.5 Anulowanie recepty farmaceutycznej

Pracownik apteki chcąc anulować wystawioną receptę farmaceutyczną przesyła z własnego systemu do P1 dokument anulowania recepty farmaceutycznej wraz z korektą dokumentu realizacji. Zostaną wówczas zweryfikowane w podsystemie SWD, a następnie zdepersonalizowane i zapisane w podsystemie SGR.

11.1.6 Realizacja recept

Pracownicy aptek otrzymują od usługobiorcy dane dostępne umożliwiające pobranie z systemu P1 receptę lub pakiet recept w celu wydania produktów leczniczych. W związku z występowaniem jednego produktu leczniczego na jednej receptce możliwa jest realizacja poszczególnych recept z pakietu w różnych aptekach. Jeżeli wydane zostaną produkty lecznicze farmaceuta przesyła dokument realizacji recepty do systemu P1. Następnie poprzez SUS zostanie przekazany do SWD w celu weryfikacji, a następnie zostanie zdepersonalizowany oraz zapisany w SGR.

11.1.7 Zablokowanie recepty

Pracownik apteki w przypadku zaistnienia okoliczności, które definiują akty prawne (art. 96 ust. 5 ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne) będzie miał możliwość zmiany statusu recepty na zablokowaną oraz dodania informacji będącej podstawą odmowy wydania produktu leczniczego. Żądanie zmiany statusu zostanie przekazane z systemu usługodawcy za pośrednictwem SUS do SGR, który zmieni status recepty i zapisze dane z nim związane. Jeżeli przedmiotem zablokowania mają być wszystkie recepty z pakietu, należy zablokować każdy z dokumentów niezależnie.

11.1.8 Odblokowanie recepty

Pracownik medyczny, który wystawił receptę oraz pracownik apteki, który zablokował receptę ma możliwość jej odblokowania poprzez zmianę statusu w przypadku jej zablokowania. Żądanie zmiany jest przekazywane do podsystemu SGR, który dokonuje zmiany statusu recepty.

11.1.8.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie żądania o dane zawarte w receptie, która będzie przedmiotem odblokowania.

11.1.8.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane zostaną wypełnione po stronie systemu usługodawcy

11.1.9 Korekta realizacji recepty

Pracownik apteki, w przypadku błędnego przesłania informacji o realizacji recepty, ma możliwość korekty dokumentu realizacji, która polega na przesłaniu nowej wersji dokumentu realizacji do P1. Przekazany poprzez SUS dokument zostanie zweryfikowany przez podsystem SWD, a następnie zdepersonalizowany i zapisany w podsystemie SGR.

11.1.9.1 Przeglądanie recept przez pracownika usługodawcy

Pracownik medyczny korzysta z funkcjonalności wyszukiwania i pobrania dokumentów recept oraz w razie potrzeby dokumentów anulowania, po pobraniu ich z podsystemu SGR w sytuacjach, gdy pracownik medyczny:

- jest autorem dokumentu,
- dysponował danymi dostępowymi do dokumentu recepty przekazanymi przez usługobiorcę,
- otrzymał uprawnienia nadane przez usługobiorcę (preautoryzacja) do recept ,

Autor dokumentu recepty będzie również mógł pobrać dane dostępne celem ewentualnego ich wydruku w postaci informacji o receptach w pakiecie.

11.1.9.2 Kontekst AUA

System AUA po wyszukaniu i pobraniu recept wyświetla je użytkownikowi oraz umożliwia inicjowanie funkcjonalności obszaru związanego z obsługą recept.

11.1.9.3 Przeglądanie recept przez pracownika apteki

Pracownicy aptek wykorzystujący własne systemy będą mogli korzystać z funkcjonalności wyszukiwania i pobierania recept oraz dokumentów realizacji z P1. Zapytania zostaną przekazane poprzez SUS do podsystemu SGR, który udostępni:

- dokumenty recept na podstawie przekazanych danych dostępowych, w szczególności w celu ich realizacji;
- dokumenty recept, anulowania i realizacji, jeżeli recepty zostały zrealizowane w aptece, która realizuje wyszukiwanie.

11.1.10 Przeglądanie recept przez usługobiorcę

Usługobiorca ma możliwość w aplikacji IKP wyszukiwać i przeglądać zapisane w podsystemie SGR dokumenty recept wraz z danymi dostępowymi do recept oraz powiązane z receptami dokumenty anulowania i realizacji.

11.1.11 Weryfikacja dokumentu recepty

System P1 umożliwia aplikacji AUA, jak również systemom zewnętrznym, przeprowadzenie weryfikacji dokumentu recepty w trakcie ich wystawiania (przed przesłaniem do zapisania w P1) przekazując do podsystemu SWD, który następnie zwraca wyniki weryfikacji.

11.2 Zakres danych

11.2.1 Dokument recepty i dokument anulowania recepty

Zakres danych dokumentu recepty i dokumentu anulowania recepty, w tym model danych, sposób wyświetlania i zakres danych wyświetlanych, zdefiniowano w ramach Polskiej Implementacji Krajowej HL7 CDA dostępnej na stronie CSIOZ.

11.2.2 Informacja o receptach w pakiecie

Zakres danych informacji o recepcie zdefiniowano w art. 96b ust. 1. Ustawy z dnia 6 września 2001 r. Prawo farmaceutyczne, przy czym w Systemie P1 są one grupowane w informację o receptach w pakiecie. Inicjalne wersje modelu danych XSD i sposobu ich wyświetlania XSLT udostępni.

11.2.3 Dokument realizacji recepty

Zakres danych dokumentu realizacji recepty obejmuje w szczególności:

- dane dotyczące wydanego leku:
 - nazwa w przypadku leków gotowych,
 - identyfikator leku oraz identyfikator opakowania w przypadku leków gotowych, a w przypadku leków recepturowych numer leku nadany przez aptekę,
 - ilość wydanych opakowań lub ilość leku recepturowego wraz z jednostką miary;
 - numer serii,
 - wielkość opakowania,
 - dawka,
 - postać,
 - data ważności,
 - zrealizowana receptura w przypadku leków recepturowych;
- dane dotyczące rozliczeń:
 - taksa laborum w przypadku leków recepturowych,
 - identyfikator płatnika, z którym apteka posiada umowę,
 - kod kraju płatnika gdy refundacja wynika z przepisów o koordynacji,
 - kod uprawnienia dodatkowego istotnego z punktu widzenia refundacji,
 - kod rodzaju odpłatności,
 - limit urzędowy,
 - kwota podlegająca refundacji,
 - wartość wydanego leku,
 - wysokość zapłaty usługobiorcy;
- dane dotyczące realizacji:
 - identyfikator dokumentu realizacji,
 - identyfikator realizowanej recepty,
 - data i czas realizacji, ewentualnie przyjęcia do realizacji recepty na lek recepturowy,
 - czas zestawienia leku w przypadku leków recepturowych,
 - dane pacjenta,

- dane realizatora i apteki,
 - identyfikator korygowanego dokumentu realizacji oraz numer wersji i numer zbioru wersji, jeżeli dotyczy,
 - dane osoby odbierającej lek,
 - adnotacje farmaceuty,
 - rodzaj realizacji (częściowa, wycofująca lub zamykająca),
 - tryb realizacji (zwykła lub farmaceutyczna);
- podpis.

Inicjalne wersje modelu danych XSD i sposobu ich wyświetlania XSLT udostępni CSIOZ.

11.2.4 Dane dotyczące recepty i dokumentów realizacji tej recepty

Zapis recepty i jej realizacji w podsystemie SGR wymaga zapisu w relacyjnej bazie danych SGR części danych odczytanych z dokumentów XML, a także utrzymywania informacji dodatkowych, celem umożliwienia m.in.:

- wyszukiwania recept i dokumentów ich realizacji;
- prezentacji list będących wynikami takiego wyszukiwania, w tym ich sortowania;
- prezentacji danych szczegółowych recepty i jej kolejnych realizacji niezależnie od wizualizacji samych dokumentów;
- realizacji recept;
- przekazywania, wraz z receptą i jej realizacjami danych o tych dokumentach do hurtowni danych.

Dane dotyczące recepty muszą zawierać w szczególności:

- identyfikator recepty,
- dane dostępowe (kod i klucz recepty oraz klucz pakietu recept),
- tytuł recepty,
- wartości klasyfikatorów recepty:
 - rodzaj leku z wartościami G - gotowy i R – recepturowy,
 - kategoria dostępności leku z wartościami Rp, Rpw i Rpz,
 - tryb wystawienia recepty z wartościami Z - zwykła, F - farmaceutyczna, P - pielęgniarska, PZ - pielęgniarska na zlecenie lekarza,
 - tryb realizacji recepty z wartościami Z-zwykły, I-import docelowy;

- identyfikator depersonalizacji lub pseudonim usługobiorcy, podlegające personalizacji przy odczycie danych o recepcie,
- datę wystawienia recepty,
- data „realizacji od dnia”,
- informację o pilności (cito),
- dane wystawcy recepty,
- dane usługodawcy, u którego wystawiono receptę,
- identyfikator płatnika z recepty,
- kod odpłatności,
- kody uprawnień pacjenta,
- oznaczenie „nie zamieniać”,
- identyfikator leku lub produktu lub substancji,
- nazwę leku,
- przepisaną ilość leku,
- historię statusu recepty wraz z datą każdej zmiany i uzasadnieniem zablokowania (jeżeli zasadne), danymi osoby zmieniającej oraz danymi usługodawcy, w kontekście którego osoba zmieniająca występuje,
- wyniki weryfikacji dokumentu recepty,
- zdepersonalizowany dokument anulowania recepty, jeżeli dotyczy;

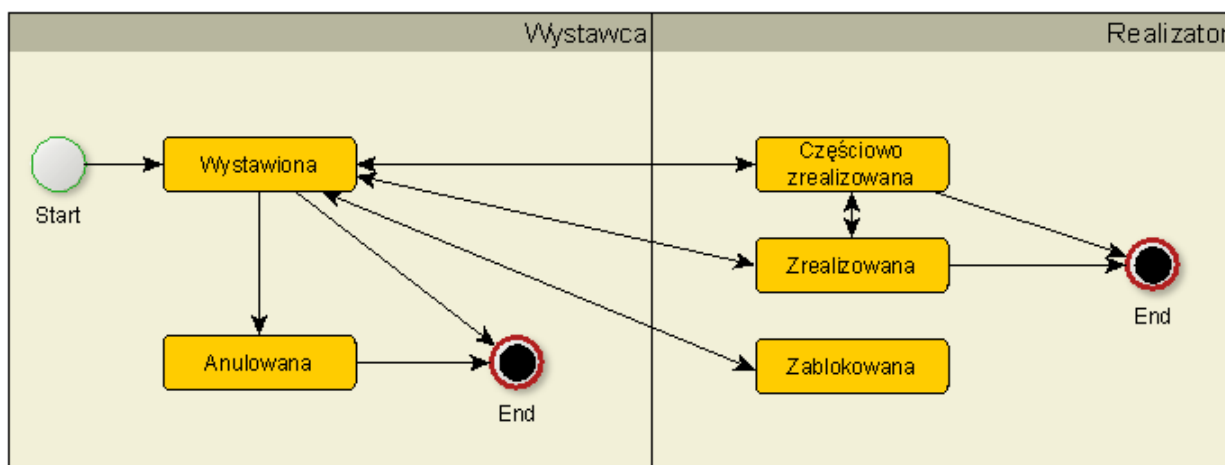
Dane dotyczące realizacji recepty muszą zawierać dla każdej z realizacji w szczególności:

- identyfikator dokumentu realizacji,
- wersję i identyfikator zbioru wersji,
- identyfikator depersonalizacji lub pseudonim usługobiorcy, podlegające personalizacji przy odczycie danych o realizacji recepty,
- identyfikator zrealizowanej recepty,
- datę realizacji recepty,
- dane realizatora recepty,
- dane apteki, w której zrealizowano receptę,
- identyfikator płatnika związanego z apteką,

- informację o wydaniu innego leku niż wskazany na receptce (np. zamiennik),
- dane wydanego leku, w tym identyfikator wydanego leku lub produktu,
- dane dotyczące płatności i refundacji,
- historię statusu dokumentu realizacji recepty wraz z datą każdej zmiany i danymi osoby zmieniającej oraz danymi apteki, w kontekście której osoba zmieniająca występuje,
- rodzaj realizacji (częściowa, wycofująca lub zamykająca), poprzez oznaczenie której pracownik apteki modyfikuje status recepty,
- tryb realizacji (zwykła lub farmaceutyczna).

11.2.5 Dokument recepty

Dopuszcza się następujące wartości statusu dokumentów recepty lekarskiej i pielęgniarskiej:



- Wystawiona – stan obowiązujący od momentu poprawnego zapisania dokumentu recepty w SGR do momentu wykonania choćby częściowej realizacji albo anulowania go przez wystawcę. Stan ten oznacza jednocześnie, że recepta nie została zrealizowana, a więc może być ostatecznym stanem recepty, jeżeli ta nie zostanie zrealizowana. Recepta w tym stanie może zostać zrealizowana przez dowolną aptekę, w której pacjent będzie realizował receptę.
- Anulowana – stan obowiązujący od momentu poprawnego zapisania dokumentu anulowania recepty w SGR. Jest to stan ostateczny.
- Zablokowana – stan obowiązujący od momentu przekazania do SGR żądania zmiany statusu na zablokowana wraz z powodem zmiany. Stan ten może być ostatecznym stanem recepty, jeżeli ta nie zostanie odblokowana. Recepta w tym stanie nie może zostać zrealizowana przez żadną z aptek.

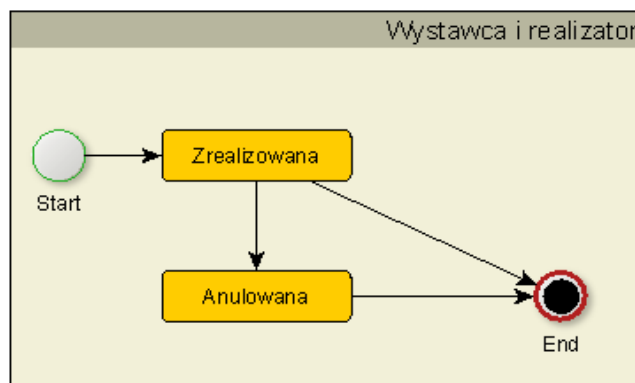
- Częściowo zrealizowana – stan obowiązujący od momentu przekazania do SGR pierwszego dokumentu realizacji recepty w rodzaju „częściowa”. W przypadku recepty o tym statusie realizator może, poprzez przekazanie kolejnego dokumentu realizacji recepty, wykonać jedną z operacji:
 - zmianę statusu recepty na „zrealizowana”, gdy sama realizacja jest rodzaju „zamykająca”;
 - pozostawienie statusu recepty w stanie „częściowo zrealizowana” gdy sama realizacja jest rodzaju „częściowa”;
 - zmianę statusu recepty na „wystawiona”, a więc wycofanie się z przetwarzania tej recepty, gdy sama realizacja jest rodzaju „wycofująca”, korygując ilość wydanego produktu leczniczego do zera.

Stan „częściowo zrealizowana” może być stanem ostatecznym, o ile pacjent nie zdecyduje się na kolejną realizację tej recepty lub pracownik apteki nie wycofa się z tej realizacji.

- Zrealizowana – stan obowiązujący od momentu przekazania do SGR dokumentu realizacji recepty w rodzaju „zamykająca”. Jest to stan ostateczny, o ile realizator nie przekaże korekty własnego dokumentu realizacji recepty zmieniającej status recepty.

11.2.6 Dokument recepty farmaceutycznej

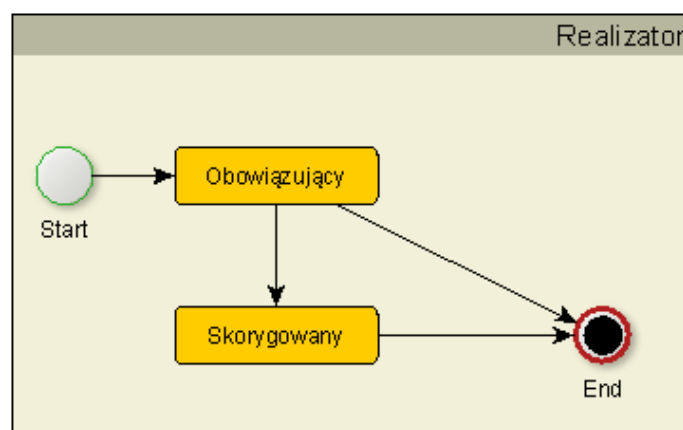
Dopuszcza się następujące wartości statusu dokument recepty farmaceutycznej:



- Zrealizowana – stan obowiązujący od momentu poprawnego zapisania dokumentu recepty farmaceutycznej wraz z dokumentem jej realizacji, obejmującym pełną ilość leku zapisaną w receptce. Jest to stan ostateczny o ile recepta nie zostanie anulowana, wraz z korektą jej realizacji do wartości zero, przez jej wystawcę.
- Anulowana – stan obowiązujący od momentu poprawnego zapisania dokumentu anulowania recepty w SGR wraz z korektą jej realizacji do wartości zero. Jest to stan ostateczny.

11.2.7 Dokument realizacji recepty

Dopuszcza się następujące wartości statusu dokumentu realizacji recepty:



- Obowiązujący – stan obowiązujący od momentu poprawnego zapisania dokumentu realizacji recepty w SGR, do momentu ewentualnego skorygowania go przez wystawcę

nowym dokumentem realizacji. Jest to stan ostateczny, o ile nie zostanie wykonana korekta.

- Skorygowany – stan dotychczas istniejącego dokumentu recepty, ustalany w chwili poprawnego zapisania nowego dokumentu realizacji recepty, w którym wskazano korygowany dokument realizacji recepty. Jest to stan ostateczny.

11.2.8 Wydruki

W AUA wydrukowi podlega dokument recepty, dokument anulowania recepty, informacja o receptach w pakiecie i dokument realizacji recepty. Zakres danych i układ graficzny każdego z wydruków definiowany jest transformatą XSLT służącą do wyświetlania dokumentu, której inicjalną wersję udostępni CSIOZ.

11.2.9 Dane powiadomienia

W wyniku wystawienia pakietu recept (o minimalnej liczności recept równej 1) usługobiorca otrzymuje informację umożliwiającą jego realizację, przy czym poza wydrukiem informacji o receptach w pakiecie informacja taka może zostać przekazana w postaci powiadomienia, którego treść zależy od kanału powiadomień:

- e-mail: tytuł maila brzmi „eZdrowie: informacja o receptach w pakiecie”, zaś treść jest wynikiem transformacji XSLT recept w pakiecie wraz z parametrami do postaci informacji o receptach w pakiecie;
- SMS: „eZdrowie: {kod dostępowy} - kod dostępowy do recept z dnia {data w postaci DD-MM-RR} godz. {czas w postaci GG:MM}, wraz z kodem wymagany identyfikator usługobiorcy, np. numer PESEL”, gdzie w klamrach {} umieszczono wymagane do umieszczenia w treści wartości zmiennych.

12 OBSZAR SKIEROWAŃ

12.1 Opis usług biznesowych obszaru

12.1.1 Utworzenie i zapis elektronicznego skierowania

Realizowane jest przez utworzenie i podpisanie elektronicznego dokumentu skierowania przez pracownika medycznego oraz przesłanie do P1. Podpisane skierowanie jest przesyłane poprzez SUS do weryfikacji w podsystemie SWD, a następnie depersonalizowane i zapisywane z wynikami weryfikacji w podsystemie SGS. Przy zapisie w systemie tworzone są dane dostępne do dokumentu, które zostają zwrócone wystawcy dokumentu na potrzeby przekazania tych danych usługobiorcy.

12.1.1.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie skierowania o zgromadzone w P1 dane pracownika medycznego, usługodawcy, usługobiorcy oraz unikalny numer dokumentu nadany w podsystemie SGS.

12.1.1.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem skierowania zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru skierowania generowanego w systemie usługodawcy odpowiada usługodawca.

12.1.2 Dołączanie elektronicznej dokumentacji medycznej do skierowań

Pracownik medyczny wystawiając skierowanie może dołączyć inne informacje w postaci elektronicznej dokumentacji medycznej w zakresie niezbędnym do udzielenia świadczenia zdrowotnego, którymi w szczególności mogą być wyniki badań lub konsultacji. P1 będzie umożliwiało dołączanie tylko tej dokumentacji medycznej, która została wcześniej zaindeksowana w P1, i która została wskazana w treści dokumentu skierowania. W takiej sytuacji załączana dokumentacja będzie zapisywana wraz z dokumentem skierowania w podsystemie SGS i czasowo tam przechowywana.

12.1.3 Przekazanie usługobiorcy informacji o skierowaniu i kodów dostępowych

Po zapisaniu skierowania w P1 informacja o skierowaniu, zawierająca też kody dostępne, jest automatycznie przekazywana do usługobiorcy za pośrednictwem poczty elektronicznej oraz wiadomością tekstową na numer telefonu, w przypadku, gdy usługobiorca zdefiniuje takie kanały komunikacyjne, wykorzystując do tego aplikację IKP. Jeżeli usługobiorca nie posiada konta w aplikacji IKP lub za jej pomocą nie przekazał do P1 danych kontaktowych, jedynym źródłem informacji o skierowaniu i danych dostępowych dla pacjenta jest wydruk informacji o skierowaniu realizowany przez aplikację AUA lub system usługodawcy.

12.1.4 Anulowanie skierowania

Pracownik medyczny, który wystawił skierowanie ma możliwość jego anulowania. Anulowanie skierowania jest realizowane poprzez utworzenie i podpisanie dokumentu anulowania oraz przesłanie do P1. Podpisany dokument anulowania jest weryfikowany w podsystemie SWD, a następnie depersonalizowany i zapisywany z wynikami weryfikacji w podsystemie SGS.

12.1.4.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie dokumentu anulowania o dane zawarte w skierowaniu, które będzie przedmiotem anulowania oraz unikalny numer dokumentu anulowania nadany w podsystemie SGS.

12.1.4.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem dokumentu anulowania skierowania zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru dokumentu anulowania skierowania generowanego w systemie usługodawcy odpowiada usługodawca.

12.1.5 Przeglądanie skierowania przez pracownika usługodawcy

Pracownik usługodawcy korzysta z funkcjonalności wyszukiwania i prezentacji skierowań oraz dokumentów anulowania po pobraniu ich z podsystemu SGS w sytuacji, gdy jest autorem dokumentu, dysponował danymi dostępowymi do dokumentu skierowania przekazanymi przez usługobiorcę, otrzymał uprawnienia nadane przez usługobiorcę (preautoryzacja) do skierowań.

12.1.5.1 Kontekst AUA

System AUA po wyszukaniu i pobraniu skierowań wyświetla je użytkownikowi, oraz umożliwia inicjowanie pozostałych funkcjonalności obszaru związanych z obsługą skierowań.

12.1.5.2 Kontekst systemu usługodawcy

W przypadku systemów usługodawców prezentacja skierowań będzie realizowana w systemie usługodawcy.

12.1.6 Realizacja skierowania

Realizacja skierowania odbywa się przez zmianę statusu dokumentu (patrz punkt 13.3.3.). Usługodawca w celu realizacji skierowania zarówno z aplikacji AUA jak również z systemu usługodawcy przesyła do podsystemu SGS identyfikator skierowania, docelowy status, identyfikator płatnika, informacje o autorze zmiany statusu oraz usługodawcy realizującym skierowanie. Jeżeli potencjalny realizator odmawia przyjęcia skierowania do realizacji, np. z powodu braku wymaganych załączników bądź opisów merytorycznych, może zapisać w P1 adnotację o powodzie odmowy celem poinformowania wystawcy dokumentu skierowania

o konieczności jego uzupełnienia, tj. anulowania i wystawienia uzupełnionego dokumentu skierowania.

12.1.7 Przeglądanie skierowania przez usługobiorcę

Usługobiorca ma możliwość w aplikacji IKP wyszukiwać i przeglądać zapisane w podsystemie SGS dokumenty skierowań wraz z danymi dostępowymi oraz powiązane z dokumentami skierowań dokumenty anulowania.

12.1.8 Przeglądanie dokumentacji załączonej do skierowania

Pracownicy usługodawcy korzystający z AUA lub systemów zewnętrznych oraz usługobiorcy korzystający z IKP mają możliwość przeglądania dokumentów skierowań, mają możliwość odczytu oraz pobierania dołączonej do skierowania elektronicznej dokumentacji medycznej. Możliwość taka będzie ograniczona czasem przechowywania załączonych dokumentów w systemie SGS. Po tym czasie dokumentacja medyczna pozostanie dostępna wyłącznie w trybie wnioskowania o udostępnienie.

12.1.9 Weryfikacja dokumentu skierowania

System P1 umożliwia aplikacji AUA jak również systemom zewnętrznym przeprowadzenie weryfikacji dokumentu skierowania w trakcie jego wystawiania jeszcze przed wysłaniem dokumentu skierowania do zapisu. Weryfikacja przeprowadzana jest przez podsystem SWD, który następnie zwraca wyniki weryfikacji.

12.1.10 Udostępnianie danych skierowania płatnikowi

Płatnik zyska możliwość dostępu do danych wszystkich zrealizowanych skierowań, które oznaczono jako finansowane przez tego płatnika. Dane podlegające udostępnieniu zostaną pobrane z podsystemu SGS oraz udostępnione usługą na SUS systemowi płatnika.

12.2 Zakres danych

12.2.1 Dokument skierowania i dokument anulowania skierowania

Zakres danych dokumentu skierowania i jego anulowania, w tym model danych, sposób wyświetlania i zakres danych wyświetlanych, zdefiniowano w ramach Polskiej Implementacji Krajowej HL7 CDA dostępnej pod adresem: https://csioz.gov.pl/fileadmin/user_upload/plcda-release-1.1-pl-PL/plcda-html-pl-PL/. Dokument skierowania wraz z jego załącznikami, a więc dokumentami medycznymi (w przypadku ich wystąpienia) wymienionymi w jego treści, stanowi jeden logiczny byt.

12.2.2 Informacja o skierowaniu

Zakres danych informacji o skierowaniu zdefiniowano w art. 59b ust. 1. Ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych. Inicjalne wersje modelu danych XSD i sposobu ich wyświetlania XSLT udostępni CSIOZ.

12.2.3 Dane dotyczące skierowania

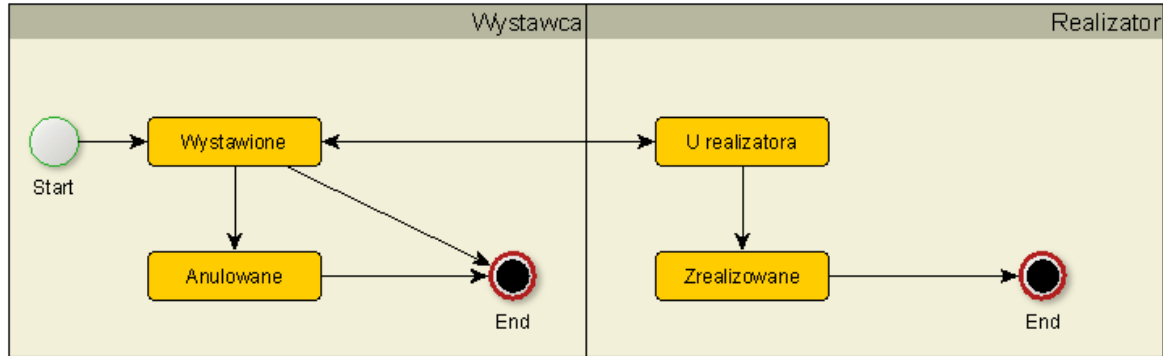
Zapis skierowania w podsystemie SGS wymaga zapisu w relacyjnej bazie danych SGS, a także utrzymywania informacji dodatkowych, celem umożliwienia m.in.:

- wyszukiwania skierowań,
- prezentacji list, będących wynikami takiego wyszukiwania, w tym ich sortowania,
- prezentacji danych szczegółowych skierowania niezależnie od prezentacji treści skierowania,
- poprawnej realizacji skierowania,
- przekazywania, wraz ze skierowaniem, danych o tym skierowaniu do hurtowni danych.

Zestaw danych o skierowaniu musi zawierać w szczególności:

- identyfikator skierowania,
- tytuł i typ skierowania,
- kod i nazwę specjalności komórki organizacyjnej, której dotyczy skierowanie (VIII cz. systemu kodów resortowych),
- identyfikator depersonalizacji lub pseudonim usługobiorcy, podlegające personalizacji przy odczycie danych o skierowaniu,
- datę wystawienia skierowania,
- dane wystawcy skierowania,
- dane usługodawcy,
- historię statusu skierowania wraz z datą każdej zmiany i danymi osoby zmieniającej oraz danymi usługodawcy, w kontekście którego osoba zmieniająca występuje,
- identyfikator płatnika, jeżeli dotyczy,
- wyniki weryfikacji dokumentu skierowania,
- powód odmowy realizacji skierowania, jeżeli dotyczy,
- zdepersonalizowany dokument anulowania skierowania, jeżeli dotyczy,
- identyfikatory i nazwy załączonych dokumentów medycznych.

Dopuszcza się następujące wartości statusu skierowania:



- **Wystawione** – stan obowiązujący od momentu poprawnego zapisania dokumentu skierowania w SGS do momentu przejęcia go przez realizatora albo anulowania go przez wystawcę. Stan ten oznacza jednocześnie, że skierowanie nie zostało zrealizowane, a więc może być ostatecznym stanem skierowania niezrealizowanego. Potencjalny realizator może zapisać przy skierowaniu powód odmowy realizacji skierowania w tym stanie.
- **Anulowane** – stan obowiązujący od momentu poprawnego zapisania dokumentu anulowania skierowania w SGS. Jest to stan ostateczny.
- **U realizatora** – stan obowiązujący od momentu przejęcia skierowania przez realizatora. W przypadku skierowania o tym statusie realizator może wykonać jedną z dwóch operacji:
 - zmianę statusu skierowania na „wystawione”, a więc wycofanie się z przetwarzania tego skierowania, z możliwością zapisania przy skierowaniu powodu odmowy realizacji;
 - zmianę statusu skierowania na „zrealizowane”, a więc uznanie, że świadczenie, na które kierujący wystawił dokument skierowania, zostało wykonane.

Fakt istnienia skierowania usługobiorcy w statusie „u realizatora” oznacza, że w skali kraju żadne inne skierowanie tego pacjenta na to samo świadczenie realizowane ze środków publicznych (art. 20 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych) nie może przyjąć tego statusu. Stan ten nie może być stanem ostatecznym, tzn. jeżeli usługodawca nie zrealizuje świadczenia, musi wycofać je do statusu „wystawione”.

- **Zrealizowane** – stan obowiązujący od momentu zadeklarowania przez usługodawcę, poprzez zmianę statusu skierowania na tę wartość, że wykonano świadczenie, na które wystawca skierowania kierował usługobiorcę. Jest to stan ostateczny.

12.2.4 Wydruki

W IKP i AUA wydrukowi podlega:

- dokument skierowania,
- dokument anulowania skierowania,
- informacja o skierowaniu.

Zakres danych i układ graficzny każdego z wydruków definiowany jest transformatą XSLT służącą do wyświetlania dokumentu, której inicjalną wersję udostępni CSIOZ.

12.2.5 Dane powiadomienia

W wyniku wystawienia skierowania usługobiorca otrzymuje informację umożliwiającą jego realizację i poza wydrukiem informacji o skierowaniu informacja taka może zostać przekazana w postaci powiadomienia, którego treść zależy od kanału powiadomień zdefiniowanego przez usługobiorcę przy wykorzystaniu konta IKP:

- e-mail: tytuł maila brzmi „eZdrowie: informacja o skierowaniu”, zaś treść jest wynikiem transformacji XSLT skierowania do postaci informacji o skierowaniu;
- SMS: „eZdrowie: {kod dostępowy} - kod dostępowy do skierowania z dnia {data w postaci DD-MM-RR} godz. {czas w postaci GG:MM}, wraz z kodem wymagany identyfikator usługobiorcy, np. numer PESEL”, gdzie w klamrach {} umieszczono wymagane do podania w treści wartości zmiennych.

13 OBSZAR ZDARZEŃ MEDYCZNYCH

13.1 Opis usług biznesowych obszaru

13.1.1 Rejestrowanie i zapis zdarzenia medycznego

Usługodawcy, w celu zapewnienia wymiany informacji na potrzeby kontynuacji procesu leczenia, zobowiązani są przekazywać do P1 informacje o udzielonych pacjentom świadczeniach oraz wytworzonej elektronicznej dokumentacji medycznej (EDM). Realizują to poprzez rejestrację zdarzenia medycznego, polegającą na przesłaniu do P1 przez usługodawcę komunikatu o zdarzeniu medycznym oraz indeksach EDM, która powstała w wyniku realizacji tego zdarzenia medycznego. Zdarzenie to wraz z powiązаныmi indeksami EDM traktuje się jako logiczną całość, w związku z czym wszystkie operacje na nim oraz na indeksach traktuje się jako operacje na zdarzeniu medycznym. Informacja o zdarzeniu medycznym może zostać przesłana przez system usługodawcy z udziałem pracownika usługodawcy lub bez jego udziału. Zdarzenia medyczne są przesyłane przez SUS do weryfikacji w podsystemie SWD, następnie depersonalizowane i zapisywane w podsystemie SGZ.

Przyjmuje się, iż każdy indeks EDM musi być zawsze powiązany ze zdarzeniem medycznym. W P1 nie rejestruje się i nie przechowuje się niepowiązanych ze zdarzeniami medycznymi indeksów EDM.

Zapis informacji o zdarzeniu medycznym i indeksie EDM realizowany jest operacją profilu IHE XDS.b "RegisterDocumentSet" oznaczoną w specyfikacji profilu symbolem ITI-42, przy czym w polskiej implementacji standardowy zakres informacyjny zapisu rozszerzono o dane zdarzenia medycznego (patrz punkt Zakres danych dla Obszaru Biznesowego).

13.1.1.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie danych zdarzenia medycznego o zgromadzone w P1 dane pracownika medycznego, usługodawcy, usługobiorcy oraz unikalny numer zdarzenia nadany w podsystemie SGZ, a także podpis Systemu P1.

13.1.1.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że wszystkie wymagane dane, włącznie z numerem zdarzenia zostaną wypełnione po stronie systemu usługodawcy. Za unikalność numeru zdarzenia generowanego w systemie usługodawcy oraz opatrzenie zdarzenia medycznego certyfikatem do uwierzytelnienia danych odpowiada usługodawca.

13.1.2 Modyfikacja i anulowanie zdarzenia medycznego

Pierwotny komunikat o zdarzeniu medycznym, w tym także indeksach EDM, stanowi komplet danych. Każda ingerencja w te dane, w tym modyfikacja lub anulowanie informacji o zdarzeniu lub powiązanych z nim indeksach EDM, uznawana jest za modyfikację całości informacji o zdarzeniu medycznym. Modyfikację realizuje pracownik tego samego usługodawcy, w kontekście którego powstało zdarzenie. Pracownik ten musi podać powód zmiany oraz musi być wskazany w komunikacie jako jej autor. Informacja o modyfikacji lub anulowaniu zdarzenia medycznego zostaje przez SUS przekazana do weryfikacji w SWD, a następnie jest depersonalizowana i zapisywana w SGZ. Przedmiotem anulowania może być zdarzenie medyczne lub pojedyncze indeksy EDM. W pierwszym przypadku efektem anulowania jest anulowanie całego zdarzenia medycznego, w tym z powiązanymi indeksami EDM, jeśli takie indeksy były powiązane ze zdarzeniem. W drugim, przedmiotem anulowania są poszczególne indeksy powiązane ze zmodyfikowanym zdarzeniem medycznym.

Zapis informacji o modyfikacji bądź anulowaniu zdarzenia medycznego lub indeksu EDM realizowany jest operacją profilu IHE XDS.b "UpdateDocumentSet" oznaczoną w specyfikacji profilu symbolem ITI-57.

13.1.2.1 Kontekst AUA

Jeżeli pracownik medyczny korzystać będzie z AUA, to usługa będzie dodatkowo zapewniała systemowe uzupełnianie zdarzenia medycznego o zgromadzone w P1 dane pracownika medycznego oraz dane zawarte w poprzedniej wersji tego zdarzenia.

13.1.2.2 Kontekst systemu usługodawcy

W przypadku wykorzystania systemu usługodawcy zakłada się, że jest on odpowiedzialny za przekazanie kompletu wymaganych danych dla modyfikacji lub anulowania zdarzenia medycznego.

13.1.3 Przeglądanie zdarzeń medycznych i indeksów elektronicznej dokumentacji medycznej przez pracownika usługodawcy

System P1 zapewnia pracownikowi usługodawcy funkcjonalność wyszukiwania i pobierania zdarzeń medycznych z podsystemu SGZ, w szczególności indeksów elektronicznej dokumentacji medycznej w sytuacjach, gdy pracownik usługodawcy:

- jest autorem zdarzenia,
- jest uprawnionym pracownikiem usługodawcy,
- otrzymał uprawnienia od usługobiorcy (preautoryzacja) do zdarzeń medycznych.

Wyszukiwanie i pobranie informacji o zdarzeniu medycznym i indeksie EDM realizowane jest operacją profilu IHE XDS.b "RegistryStoredQuery" oznaczoną w specyfikacji profilu symbolem ITI-18, przy czym w polskiej implementacji standardowy zakres informacyjny wyszukiwania, w tym zestaw predefiniowanych zapytań rozróżnianych identyfikatorem, rozszerzono o obsługę danych zdarzenia medycznego (patrz punkt Zakres danych dla Obszaru Biznesowego).

13.1.4 Przeglądanie zdarzeń medycznych i indeksów elektronicznej dokumentacji medycznej przez usługobiorcę

Usługobiorca ma możliwość w aplikacji IKP wyszukiwać i przeglądać zapisane w podsystemie SGZ zdarzenia medyczne jego dotyczące oraz, do których posiada uprawnienia, oraz powiązane z nimi indeksy elektronicznej dokumentacji medycznej.

Do implementacji usługi biznesowej wykorzystano operację opisaną w poprzednim punkcie.

13.1.5 Weryfikacja zdarzenia medycznego i indeksu elektronicznej dokumentacji medycznej

System P1 umożliwia aplikacji AUA, jak również systemom zewnętrznym, przeprowadzenie weryfikacji informacji o zdarzeniu medycznym i indeksach elektronicznej dokumentacji medycznej przed przekazaniem ich do rejestracji. Weryfikacja jest wykonywana przez podsystem SWD.

Do przeprowadzenia weryfikacji służy dedykowana usługa sieciowa.

13.1.6 Hurtowa zmiana kustosza dokumentów

W ramach zakresu informacyjnego indeksu EDM w P1 przechowywana jest informacja o opiece (kustosz) dokumentu, będąca wskazaniem na usługodawcę, który jest odpowiedzialny za dokument oraz jego przechowywanie i udostępnianie. W sytuacji, gdy zachodzi potrzeba zmiany opiekuna pojedynczego lub wielu dokumentów system P1 zapewnia systemom usługodawców odpowiednią funkcjonalność. Usługodawca odpowiedzialny za przekazanie dokumentów do innego usługodawcy ma możliwość wyselekcjonowania zbioru dokumentów podlegających przekazaniu, a następnie wskazania nowego kustosza dokumentów.

Lista wyselekcjonowanych przez Usługodawcę przekazujących dokumentów wraz ze wskazaniem nowego kustosza zostanie przekazana przez SUS do zapisu w SGZ. Usługodawca, na którego wskazano przypisanie dokumentów (który ma pełnić rolę nowego kustosza dokumentów) przy wykorzystaniu funkcjonalności powiadomień w P1 otrzymuje powiadomienie o tym fakcie.

Usługodawca przejmujący dokumenty będzie miał możliwość pobrania do własnego systemu listy dokumentów oraz zatwierdzenia roli kustosza dla całej listy zbiorczo lub poprzez wskazanie pojedynczych dokumentów z listy. Zatwierdzona przez usługodawcę lista zostanie przekazana przez SUS do SGZ celem zapisu oraz zmiany kustosza dokumentów w indeksach zaaprobowanych przez usługodawcę.

Do przeprowadzenia hurtowej zmiany kustosza dokumentów służą dedykowane usługi sieciowe.

13.1.7 Hurtowa zmiana statusu dostępności dokumentów

W ramach zakresu informacyjnego indeksu EDM w P1 przechowywana jest informacja o statusie dostępności dokumentu, w którego zmianę może być skutkiem np. uruchomienia nowego repozytorium dokumentów medycznych w sytuacji, gdy dokumenty nie były do tej pory przechowywane w dostępnym repozytorium (zmiana wartości statusu z "offline" na "online") lub archiwizacja dokumentów (zmiana wartości z "online" na "offline").

Zmiana statusu dostępności dokumentów medycznych kustosza będzie mogła być realizowana przez system usługodawcy w sposób hurtowy, tj. pojedynczym wywołaniem operacji zmiany statusu dla listy indeksów tego kustosza, a więc bez kontekstu pacjenta.

Do przeprowadzenia hurtowej zmiany statusu dostępności dokumentów służy dedykowana usługa sieciowa.

13.2 Zakres danych

13.2.1 Komunikat z informacją o zdarzeniu medycznym i indeksie elektronicznej dokumentacji medycznej

Zakres danych komunikatu i sposób jego przesyłania i modyfikacji zdefiniowano w dokumencie „Model transportowy danych o Zdarzeniach Medycznych oraz Indeksie Elektronicznej Dokumentacji Medycznej gromadzonych w systemie P1” dostępnym pod adresem: <https://www.csioz.gov.pl/interoperacyjnosc/interfejsy/>.

13.2.2 Dane dotyczące zdarzenia medycznego i indeksu elektronicznej dokumentacji medycznej

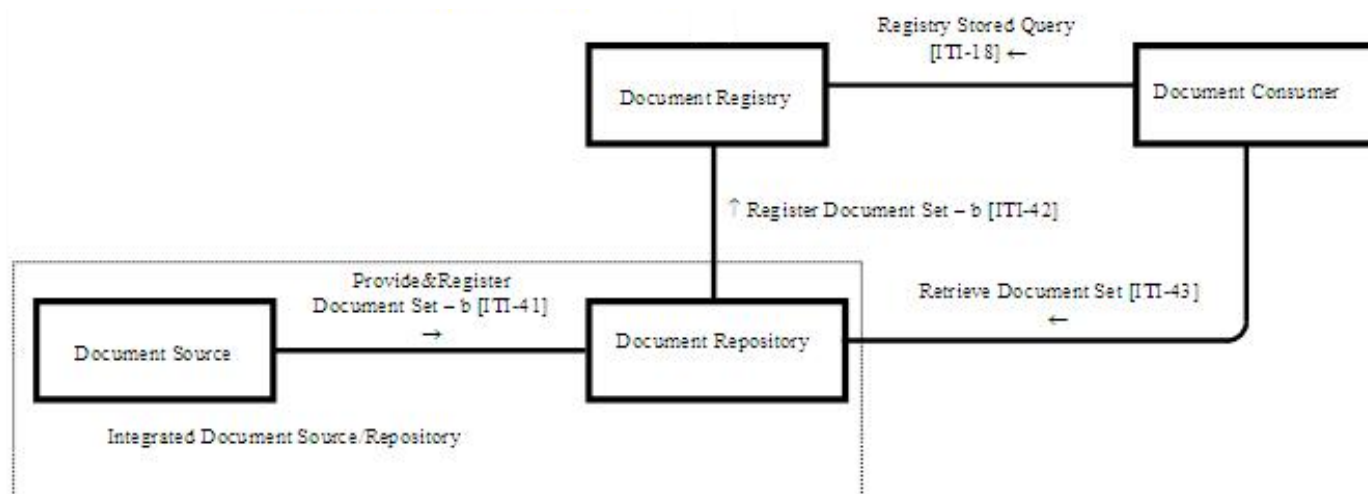
Dane dotyczące zdarzenia medycznego i indeksu elektronicznej dokumentacji medycznej stanowią podzbiór zakresu informacyjnego zawartego w komunikacie o zdarzeniu medycznym.

14 OBSZAR WYMIANA DOKUMENTACJI MEDYCZNEJ

14.1 Opis przyjętego rozwiązania

Wymiana elektronicznej dokumentacji wykorzystująca dedykowane wsparcie Systemu P1 będzie oparta o implementację profilu IHE XDS.b, a w przypadku dokumentów obrazowych IHE XDS-I.b.

Zostało przyjęte, że w polskim systemie ochrony zdrowia dokumenty medyczne udostępniane są elektronicznie w sposób identyczny w każdym przypadku, tj. poprzez jedną standardową operację typu WebService, a dostępność dokumentu w tym trybie oznaczana jest w indeksie tego dokumentu zapisanym w P1 - przewidziany do tego atrybut będzie przyjmował wartość „online”. Niedostępność dokumentu w trybie online, a więc dostępność tylko w ramach odbioru osobistego, oznaczana będzie w tym samym miejscu - zgodnie ze standardem wartością „offline”.



Rysunek 1. Podstawowy diagram transakcji IHE XDS.b

Na diagramie w prostokątnych blokach przedstawiono następujących aktorów, biorących udział w wymianie dokumentów medycznych (opisane strzałki oznaczają kierunek wykonania transakcji, tj. wywołania operacji WebService):

- Document Source – źródło dokumentów, tj. system usługodawcy, w ramach którego dokumenty wystawiono;
- Document Repository – repozytorium dokumentów, przy czym objęcie dodatkową ramką aktora wraz z Document Source oznacza, że repozytorium jest z punktu widzenia P1 zintegrowane z usługodawcą wystawiającym dokument i to niezależnie czy ten usługodawca wykorzystuje do prowadzenia repozytorium własny system informatyczny, system regionalny, czy też komercyjny system zewnętrzny. Do zapisu dokumentów do repozytorium służy operacja „Provide&RegisterDocumentSet” oznaczona w specyfikacji profilu symbolem ITI-41, jednak z punktu widzenia P1, komunikacja pomiędzy źródłem dokumentu a repozytorium nie będzie specyfikowana, gdyż nie dotyczy Systemu P1 (jest to operacja wewnętrzna usługodawcy i jego repozytorium);
- Document Registry – **rejestr dokumentów prowadzony w P1**, jedna z funkcjonalności Systemu P1. Do zaindeksowania dokumentu w P1 służy operacja zapisu indeksów (rozszerzona o dane zdarzenia medycznego) „RegisterDocumentSet” oznaczona w specyfikacji profilu symbolem ITI-42;
- Document Consumer – system pracownika usługodawcy wyszukującego i pobierającego dokumenty medyczne. Do wyszukania indeksów w rejestrze służy operacja „RegistryStoredQuery” oznaczona w specyfikacji profilu symbolem ITI-18, przy czym nazwa ta oznacza, że rejestr posiada predefiniowane zapytania rozróżniane identyfikatorem, zawierające z góry określoną liczbę atrybutów wyszukiwania. W wyniku wyszukiwania pracownik usługodawcy otrzymuje indeksy, do których posiada prawo dostępu, wraz z informacją o statusie dostępności poszczególnych dokumentów medycznych. W przypadku indeksów ze statusem dostępności „online” możliwe jest pobranie dokumentu z repozytorium (w przypadku statusu „offline” możliwe jest pobranie jedynie w trybie osobistym, tj. poza wsparciem P1). Do pobrania dokumentów z repozytorium służy operacja „RetrieveDocumentSet” oznaczona w specyfikacji profilu symbolem ITI-43, przy czym jak widać na diagramie wywołanie tej operacji WebServices realizowane jest z pominięciem rejestru dokumentów, a więc z pominięciem P1. Dokumenty pobiera się po ich identyfikatorach;
- DocumentAdministrator – aktor pominięty w powyższym standardowym diagramie, implementowany w systemach źródłowych oraz w systemie zarządzającym rejestrem dokumentów, w tym implementowany w P1. Administrowanie w polskim rozwiązaniu ogranicza się do implementacji operacji „UpdateDocumentSet” oznaczonej w specyfikacji profilu symbolem ITI-57, wywoływanej na danych rejestru celem modyfikacji zawartości indeksu w kontekście jednego pacjenta. Specyfikacja operacji publikowana jest w dokumencie typu Trial Implementation „XSD Metadata Update”.

Zgodnie z przywołanym standardem system implementujący rolę DocumentConsumer będzie mógł po wyszukaniu indeksów w P1, odnośnie których istnieje zgoda pacjenta na dostęp, pobrać zaindeksowane jako dostępne "online" dokumenty medyczne z repozytorium usługodawcy udostępniającego standardową operacją Webservice „RetrieveDocumentSet”. System P1 nie wspiera wymiany dokumentów oznaczonych jako „offline” poza faktem udostępniania indeksu, a więc informacji o ich istnieniu – w takim przypadku wnioskujący musi odebrać dokumenty fizycznie od usługodawcy, tj. w dotychczasowy praktykowany sposób.

1.1.1. Wsparcie Systemu P1 dla wymiany standardowych dokumentów medycznych

Wywołanie operacji wymiany dokumentów medycznych odbywać się będzie poza Systemem P1, nie licząc przypadku wywołania z aplikacji AUA i IKP. W przypadku dokumentów medycznych dostępnych w trybie online (informacja o trybie dostępu znajduje się w indeksie dokumentu medycznego) możliwe jest automatyczne pobranie dokumentu bezpośrednio z jego repozytorium przy zastosowaniu operacji RetrieveDocumentSet profilu IHE XDS.b. W przypadku dokumentów medycznych dostępnych w trybie offline możliwy jest wyłącznie odbiór w sposób praktykowany obecnie, np. osobiście w siedzibie usługodawcy.

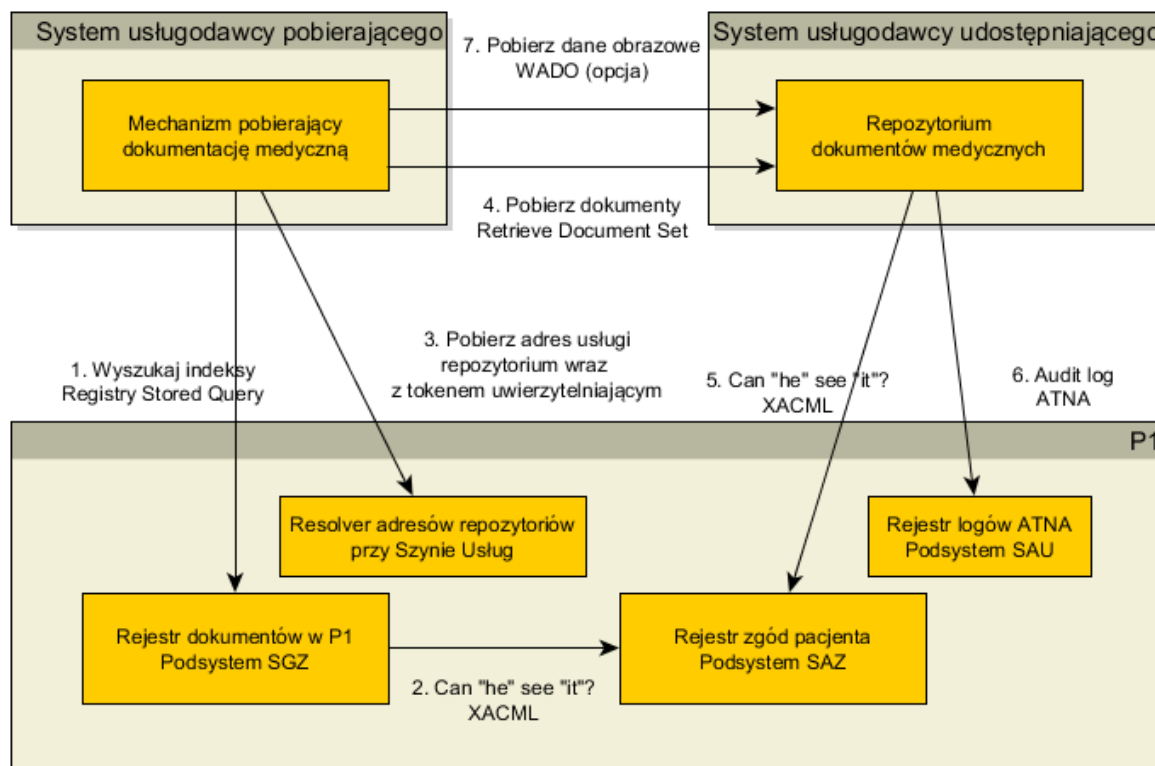
1.1.2. Wsparcie Systemu P1 dla wymiany danych obrazowych

Wymaga się, by System P1 wspierał wymianę danych obrazowych wg profilu IHE XDS-I.b. W ramach tej funkcjonalności dokumentację typu DICOM indeksuje się w postaci dwóch dokumentów – opisowego „diagnostics report” oraz tzw. manifestu. Osoba wyszukująca dokumenty obrazowe może wyszukać sam opis badania diagnostycznego, może też wyszukać sam dokument typu manifest, pobrać ten dokument z repozytorium dokumentów usługodawcy i przy jego pomocy pobierać dokumenty obrazowe z repozytorium dokumentów obrazowych usługodawcy przy wykorzystaniu standardu WADO.

Szczegółowy opis danych stosowanych w indeksie dokumentów obrazowych oraz zasad wykorzystania profilu znajduje się m.in. w specyfikacji profilu IHE RAD http://ihe.net/uploadedFiles/Documents/Radiology/IHE_RAD_TF_Vol3.pdf w rozdziale dotyczącym zapisu danych DICOM do repozytorium dokumentów z uwzględnieniem metadanych (indeksu), które zostaną przekazane do rejestru (rozdział 4.68 Provide and Register Imaging Document Set – MTOM/XOP). Uwzględnienie profilu IHE XDS-I.b w P1 nie wprowadza zmian w zastosowaniu profilu IHE XDS.b w zakresie rejestru dokumentów medycznych, należy jednocześnie zapewnić niesprzeczność implementacji rejestru z profilem IHE XDS-I.b.

1.1.3. Proces wymiany dokumentów medycznych

Na poniższym diagramie przedstawiono implementowane w Polsce poszczególne wywołania transakcji składających się na proces wymiany dokumentów medycznych:



Rysunek 2. Sekwencja wywołań operacji WDM, celem uproszczenia diagramu nie zaznaczono udziału SUS

Ponumerowane wywołania oznaczają kolejno:

1. System usługodawcy występujący w roli pobierającego dokumentację medyczną wywołuje operację standardową IHE XDS.b Registry Stored Query (opisaną jako usługa biznesowa w obszarze zdarzeń medycznych), przekazując parametry zapytania do P1. System ten otrzymuje odpowiedź w postaci indeksów dokumentów medycznych, dopiero po wewnętrznym w P1 wykonaniu operacji 2.
2. Rejestr dokumentów w P1 przed udostępnieniem indeksów weryfikuje w roli elementu PEP standardu XACML, w rejestrze zgód pacjenta czy, i które indeksy dokumentów powinien zwrócić. Rejestr zwraca w ramach odpowiedzi na operację 1 listę indeksów, którą wyszukiwający ma prawo poznać.
3. System usługodawcy występujący w roli pobierającego dokumentację medyczną, posiadając indeksy dokumentów oznaczone jako dostępne "online", rozpoczyna pobieranie tych dokumentów z systemów usługodawców realizujących funkcję repozytoriów tych dokumentów. W tym celu system pobierający dokumentację medyczną może odnaleźć adres operacji WebService standardu IHE XDS.b Retrieve Document Set utrzymywanej przez

usługodawcę wskazanego w indeksie jako kustosz (udostępniający). W ramach tego wywołania P1 nadaje systemowi pobierającemu dokumentację medyczną token (dedykowany dla architektury P1 mechanizm, patrz w dalszej części dokumentu uzasadnienie dla tokena) potwierdzający dla systemu udostępniającego, że system wyszukujący jest systemem zaufanym w środowisku P1.

4. System usługodawcy pobierającego dokumentację medyczną, korzystając z adresu usługi systemu udostępniającego, tj. adresu operacji udostępniania z repozytorium dokumentów, wywołuje tę usługę będącą implementacją standardowej operacji WebService IHE XDS.b Retrieve Document Set. Zanim repozytorium dokumentów zwróci dokumenty, wywołuje operacje 5 i 6.

5. System usługodawcy udostępniającego, tj. repozytorium dokumentów, przed udzieleniem odpowiedzi w operacji 4 musi zweryfikować czy wyszukujący ma prawo otrzymać dokument. W tym celu działa jako element PEP standardu XACML, wykorzystując P1 jako element PDP tego standardu.

6. Po otrzymaniu zgody system usługodawcy udostępniającego wysyła do P1 log UDO komunikatem XML poprzez Syslog over TLS (log, zgodnie z zasadami IHE, może też zostać wysłany możliwie krótko po udzieleniu odpowiedzi w ramach operacji 4, szczególnie gdy rejestr logów ATNA chwilowo nie jest dostępny). Po wykonaniu operacji 5 i 6 system udostępniający odpowiada systemowi pobierającemu dokumentację medyczną przekazując dokumenty bądź odmowę w ramach zakończenia obsługi operacji 4.

7. W przypadku pobierania dokumentu typu manifest standardu DICOM system usługodawcy pobierającego może wykonać przegląd dokumentacji obrazowej wskazanej w pobranym dokumencie przy wykorzystaniu np. standardu WADO. Standard ten nie jest przedmiotem opracowania.

1.1.3.1. Kontekst AUA i IKP

Aplikacje AUA i IKP umożliwiają pobranie dokumentów medycznych dostępnych w trybie online na komputer (dysk twardy) użytkownika aplikacji, przykładowo w przypadku dokumentów XML wymagających dedykowanej transformaty pobranie powinno zakończyć się pobraniem dokumentu z transformatą w postaci archiwum ZIP. Proces pobrania jest podobny do procesu implementowanego w systemach usługodawców - użytkownik AUA lub IKP wyszukuje indeksy, a po ich pobraniu w przypadku indeksów oznaczonych statusem dostępności dokumentu o wartości "online" może kliknąć pobranie tych dokumentów z repozytorium elektronicznego wskazanego w indeksie. AUA i IKP posiadać będzie dostęp do usługi biznesowej wskazującej adres usługi repozytorium i nadającej token uwierzytelniający, a po jej wywołaniu nastąpi wywołanie usługi repozytorium służącej do pobrania dokumentu. Aplikacje AUA i IKP nie wspierają przeglądania dokumentów obrazowych DICOM, choć

umożliwiają pobranie dokumentu opisowego, a także dokumentu typu manifest standardu DICOM.

Aplikacja AUA posiada funkcjonalność zapisu zdarzeń medycznych i indeksów dokumentacji medycznej do P1. Oznaczenie dokumentacji jako dostępnej w trybie "online" może zostać wykonane w AUA wyłącznie, gdy dokumenty wytworzone przez usługodawcę rzeczywiście znajdują się w tego typu dostępnym repozytorium elektronicznej dokumentacji medycznej. AUA nie bierze udziału w procesie udostępniania dokumentacji medycznej, tj. nie implementuje roli systemu usługodawcy udostępniającego.

14.2 Opis usług biznesowych obszaru

14.2.1 Informacja o adresie usługi udostępniania dokumentacji medycznej usługodawcy

System P1 umożliwia zapisanie informacji o adresie usługi WebServices repozytorium wg standardu IHE XDS.b „RetrieveDocumentSet” dla każdego usługodawcy identyfikowanego jego własnym identyfikatorem zapisanym w notacji OID.

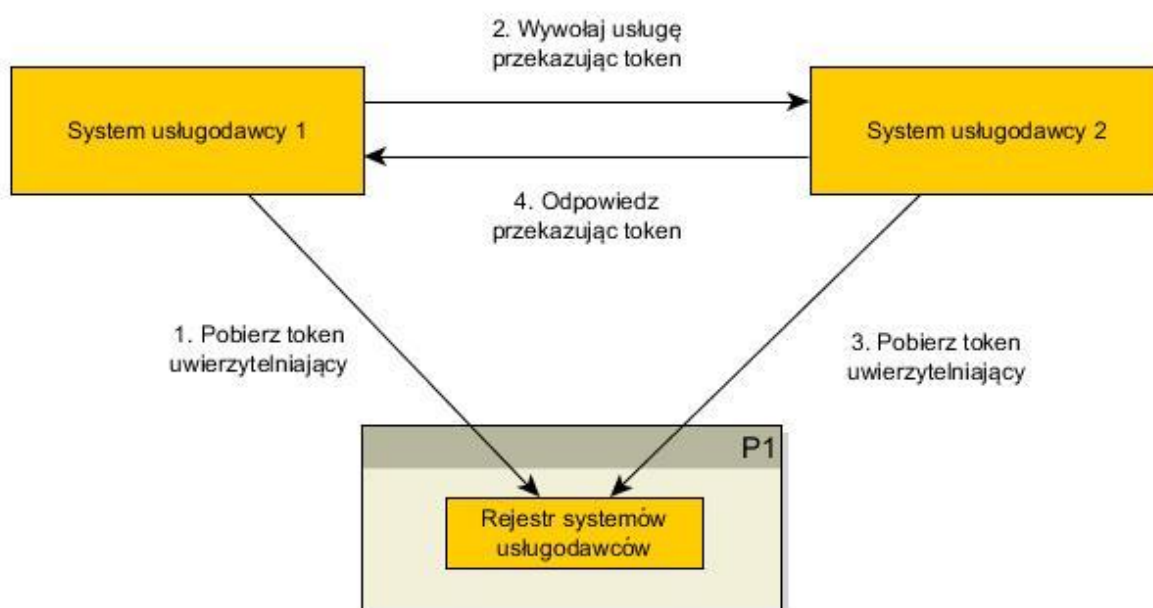
14.2.2 Wydawanie tokenu uwierzytelniającego system usługodawcy w systemie innego usługodawcy

Do Systemu P1 podłączone są wyłącznie zaufane systemy usługodawców, tj. formalnie zgłoszone, posiadające wydany certyfikat X.509 do uwierzytelniania. Systemy te mogą komunikować się ze sobą bezpośrednio, uwierzytelniając się nawzajem z wykorzystaniem posiadanych certyfikatów (protokół challenge-response).

Systemy te mogą też wykorzystywać inne dwustronnie uzgodnione mechanizmy uwierzytelnienia. Przykładowo jeżeli system szpitalny włączony w rozwiązanie regionalne wyszukuje w P1 dokumenty medyczne znajdując w ich indeksach informację, że są one dostępne w systemie innego szpitala włączonego w to samo rozwiązanie regionalne,

a uzgodnionego na poziomie regionalnym, pobranie dokumentów medycznych nie musi angażować mechanizmów uwierzytelniania P1.

Kolejną alternatywą jest możliwość zastosowania Systemu P1 jako zaufanej trzeciej strony, tj. wykorzystania usługi biznesowej wydania tokenu uwierzytelniającego wg schematu przedstawionego na poniższym diagramie:



Rysunek 3. Wydawanie tokenów uwierzytelniających dla dwustronnej weryfikacji tożsamości systemów

W rozwiązaniu tym każda strona weryfikująca token zobowiązana jest do sprawdzenia, czy czas ważności tokenu nie minął oraz czy podpis Systemu P1 pod tokenem jest ważny. Istotne jest szyfrowanie połączenia pomiędzy systemami celem uniknięcia ewentualnego przechwycenia tokenu przez stronę atakującą.

Powyższe dwustronne rozwiązanie może z punktu widzenia systemu usługodawcy zostać uproszczone do jednostronnej weryfikacji tożsamości systemu wywołującego usługę w sytuacji, gdy np. usługa dotyczy pobrania dokumentu medycznego, a więc gdy system usługodawcy wywołującego nie przekazuje do zapisu żadnych danych systemowi usługodawcy udostępniającego.

Implementowana w P1 usługa wydawania tokenu będzie zintegrowana z usługą udzielania informacji o adresie usługi udostępniania dokumentacji medycznej usługodawcy, tj. token powinien zostać wydany w nagłówku SAML komunikatu odpowiedzi na wywołanie operacji pobrania adresu repozytorium dokumentów medycznych.

14.2.3 Weryfikacja uprawnień żądającego udostępnienia dokumentu

Pobranie dokumentu medycznego z systemu usługodawcy musi zostać poprzedzone weryfikacją uprawnień pobierającego. W tym celu System P1 udostępni usługę biznesową zgodną ze standardem XACML, umożliwiającą wywołanie przez system pełniący rolę komponentu PEP (Policy Enforcement Point) operacji komponentu PDP (Policy Decision Point). Szczegóły poszczególnych komponentów znajdują się w opisie standardu XACML, np.: <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>.

14.2.4 Zapis logu z udostępnienia danych osobowych

Udostępnienie dokumentu medycznego z systemu usługodawcy, ale też recepty bądź skierowania z Systemu P1, wymaga odnotowania tzw. logu UDO w podsystemie SAU. Dla systemów usługodawców tworzy się w Systemie P1 dedykowaną usługę do zapisu logu UDO z udostępnienia dokumentu medycznego. Zamawiający wymaga zastosowania profilu IHE ATNA z zakresem danych wymienionym w specyfikacji operacji RetrieveDocumentSet profilu IHE XDS.b.

14.3 Zakres danych

14.3.1 Zakres danych informacji o adresie usługi udostępniania dokumentacji medycznej usługodawcy wraz z wydaniem tokenu

Zakres danych przekazywanych w opisywanej operacji obejmuje adres usługi WebService wraz z tokenem uwierzytelniającym przekazywanym w nagłówku SAML.

14.3.2 Weryfikacja uprawnień żądającego udostępnienia dokumentu

Zakres danych przekazywanych w operacji weryfikacji uprawnień znajduje się w opisie standardu XACML, np.: <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>.

14.3.3 Zapis logu z udostępnienia danych osobowych

Zakres danych komunikatu ATNA dotyczący zapisu logu z udostępnienia dokumentów medycznych zdefiniowano w rozdziale 3.43.6 Security Considerations specyfikacji operacji udostępnienia dokumentów RetrieveDocumentSet profilu IHE XDS.b dostępnej na stronie http://ihe.net/Technical_Frameworks/ w tomie oznaczonym tytułem „ITI TF-2b”.

15 OBSZAR STATYSTYK I ANALIZ

15.1 Opis usług biznesowych obszaru

15.1.1 Zasilenie hurtowni danych na potrzeby analiz i statystyk

System P1 gromadzić będzie szeroki zakres informacji dot. ochrony zdrowia. Wyselekcjonowane, zanonimizowane dane gromadzone w P1 będą wykorzystywane do celów analitycznych na potrzeby wprowadzenia usprawnień w funkcjonowaniu obszaru ochrony zdrowia w kraju. Chcąc zapewnić efektywne wykorzystanie tych danych oraz umożliwić ich analizę podsystem ASR dostarczy funkcjonalność hurtowni danych.

Poza podsystemami P1, źródłami danych dla hurtowni będą również systemy zewnętrzne, takie jak P2, GUS.

15.1.2 Udostępnienie narzędzi klasy Business Intelligence

Dane zgromadzone w hurtowni danych będą udostępniane użytkownikom:

- ASR – na potrzeby prowadzenia analiz, statystyk i raportów,
- HDM – w celu obsługi, analizy i monitorowania wskaźników,
- SWN – w celu wykrywania nadużyć w obszarze ochrony zdrowia.

Podsystem ASR zapewni, aby zakres udostępnianych danych mógł być ograniczony na poziomie data mart, obiektów, faktów i miar.

W zakresie prowadzenia analiz, statystyk i raportów system umożliwi użytkownikom m.in.:

- definiowanie, generowanie, udostępnianie oraz prezentację raportów statycznych i dynamicznych, statystyk i wskaźników,
- generowanie raportów cyklicznych,
- zarządzanie szablonem i formatowaniem raportów i analiz,
- filtrowanie i drążenie danych (przejsście do szczegółowych danych),
- przygotowywanie raportów w oparciu o modele analityczne,
- etapowanie analizy (przygotowanie danych, modelu, zastosowanie modelu przy wykorzystaniu konkretnej metody, ewaluację przeprowadzonej analizy lub zastosowanego modelu),
- tworzenie analiz zaawansowanych – statystycznych, analiz szeregów czasowych oraz prognozowania,
- interpolację brakujących obserwacji,
- wybór próby losowej i przeprowadzenie analizy minimalnej wielkości próby,

- powiadamianie o przekroczeniu wartości wskaźnika przez przekazanie na SUS żądania utworzenia powiadomienia,
- zarządzanie grupą odbiorców powiadomień o przekroczeniu określonych poziomów wskaźników,
- zapisywanie raportów i analiz do pliku w formatach CSV, RTF, PDF, XML.

15.2 Zbiór wymagań

Do implementacji funkcjonalności opisanych w ramach niniejszego obszaru wykorzystane zostaną posiadane przez Zamawiającego narzędzia firmy SAS Institute:

- SAS Enterprise BI Server,
- SAS Enterprise Guide,
- SAS Data Management Standard,
- SAS Enterprise Miner,
- SAS Text Miner,
- SAS Forecast Server,
- Platform Suite for SAS.

15.3 Zakres danych

Zakres danych przetwarzanych w obszarze będzie obejmował w szczególności dane gromadzone w:

- SGZ,
- SGR,
- SGS,
- SRR,
- SRS,
- SAZ,
- SSRMZ,
- RPWDL (P2) w zakresie informacji o łózkach i ubezpieczeniu,
- GUS w zakresie danych demograficznych.

16 OBSZAR PUBLIKACJI TREŚCI

16.1 Opis usług biznesowych obszaru

16.1.1 Publikacja i prezentacja informacji dotyczących ochrony zdrowia

Podsystem PPP zapewni funkcjonalność zarządzania oraz publikacji treści na internetowym portalu edukacyjno-informacyjnym. Portal powinien zapewnić szerokiej grupie odbiorców, m.in. pacjentom, pracownikom medycznym i usługodawcom, przydatne i wartościowe informacje dotyczące ochrony zdrowia. Na portalu będą udostępniane artykuły oraz komunikaty Ministra Zdrowia, wspierające pozostałe działania w realizacji zadania promocji wiedzy w zakresie ochrony zdrowia. Ponadto publikacje będą zawierały informacje dla usługodawców oraz wytwórców oprogramowania na temat systemów informacyjnych, struktur i formatów danych, komunikatów, a także będą dotyczyły aspektów eksploatacyjnych systemów. W tym celu PPP umożliwi publikowanie treści tekstowych oraz multimedialnych takich jak pliki muzyczne, obrazy graficzne i pliki video. Podsystem dostarczy również zestaw narzędzi do zarządzania publikowaną treścią redaktorom oraz narzędzia do zarządzania użytkownikami i uprawnieniami administratorowi systemu.

Wszystkie autoryzowane przez redaktorów treści będą udostępniane każdemu użytkownikowi portalu. W szczególności w celu zapewnienia użytkownikowi szybkiego odnajdywania poszukiwanych informacji portal posiadać będzie mapę strony oraz wyszukiwarkę treści. Użytkownicy portalu zainteresowani nowymi treściami tematycznymi zyskają możliwość po wskazaniu odpowiedniej grupy tematycznej otrzymania e-maila z informacją o zmianie treści lub subskrybować kanał RSS.

16.2 Zakres danych

Dane przetwarzane przez PPP obejmują publikowaną treść tekstowo – multimedialną.

17 TECHNICZNY OBSZAR WERYFIKACJA DANYCH

17.1 Opis usług biznesowych obszaru

17.1.1 Weryfikacja biznesowa danych

Podsystem SWD, aby zapewnić poprawność i zgodność przetwarzania danych w bazach systemu P1 zapewnia weryfikację danych przekazywanych do P1, w szczególności:

- recept,
- realizacji recept,
- anulowania recept,
- skierowań,
- anulowania skierowań,
- zdarzeń medycznych,
- indeksów elektronicznej dokumentacji medycznej.

W tym celu, każdy z dokumentów będzie mógł być weryfikowany pod kątem poprawności struktury dokumentu oraz na zgodność danych w nim zawartych:

- pod względem ich kompletności, tj. czy wszystkie wymagane dane zostały zawarte w dokumencie,
- z wartościami słownikowymi, np. czy rozpoznanie wskazane w zdarzeniu medycznym jest zgodne z obowiązującym słownikiem,
- z rejestrami CWUb, CWUd, CWPM, płatników, leków np. czy podany identyfikator usługobiorcy (PESEL) znajduje się w CWUb,
- z polityką stosowania identyfikatorów, np. stosowanie identyfikatorów zgodnych z OID.

Aby umożliwić weryfikację zgodności ze słownikami i rejestrami SWD będzie komunikował się z gromadzącymi te dane podsystemami odpowiednio SRS i SRR.

Wszystkie przesłane przez podsystem SUS do podsystemu SWD żądania weryfikacji danych powinny w odpowiedzi zwrócić wynik weryfikacji tj.: listę wykrytych błędów i ostrzeżeń. Ostrzeżenia to kategoria, która w przeciwieństwie do błędu pomimo jego wystąpienia umożliwia zapis dokumentu.

17.1.2 Konfiguracja reguł

Podsystem SWD zapewni administratorowi P1 graficzny interfejs umożliwiający:

- dodawanie, modyfikowanie i usuwanie reguł weryfikujących,

- aktywacje i dezaktywacje reguł i zestawów reguł,
- dodawanie i usuwanie do zestawu reguł dla poszczególnych obiektów,
- wskazanie sekwencji i zależności pomiędzy regułami w zestawie,
- dodanie i usunięcie algorytmu według którego działa dana reguła,
- eksportu kodów i opisów błędów.

17.2 Zakres danych

Zakres danych dla obszaru weryfikacji, w tym w szczególności:

- obiekt weryfikacji (zgodnie z rozdziałem. 1.1),
- identyfikator i nazwa reguły,
- wersja reguły,
- status reguły (aktywna/nieaktywna),
- status zestawu (aktywna/nieaktywna),
- identyfikator i nazwa zestawu reguł,
- identyfikator i nazwa algorytmu,
- kod i opis wyniku,
- data i czas weryfikacji.

18 TECHNICZNY OBSZAR SŁOWNIKI

18.1 Opis usług biznesowych obszaru

18.1.1 Zasilanie i aktualizacja słowników

Podsystem ZDP zapewni mechanizm zasilania i aktualizacji słowników, w szczególności ich dodawania, edycji/modyfikowania oraz usuwania. Zasilenie i aktualizacja słowników zostanie zapewniona przez:

- zasilania słowników z pliku w aplikacji ZDP,
- zasilenia realizowanego z zewnętrznego względem P1 systemu – Rejestru Systemów Kodowania (RSK). SUS zapewni możliwość przekazywania słowników pomiędzy RSK a ZDP.

Podsystem ZDP na podstawie przekazanych danych dokona aktualizacji słowników w podsystemie SRS, która skutkować będzie zmianą wersji słownika oraz udostępnieniu informacji o niej pozostałym podsystemom P1.

18.1.2 Udostępnianie słowników

Aby zapewnić spójność danych, w systemie P1 wykorzystuje się dane słownikowe. W tym celu zapewnia się pozostałym podsystemom P1 dostęp do danych słownikowych o charakterze referencyjnym. Podsystem SRS udostępnia słowniki wszystkim podsystemom P1 z wykorzystaniem SUS lub w uzasadnionych przypadkach bez udziału SUS.

18.2 Zakres danych

Każdy ze słowników posiada nazwę i identyfikator OID, a także dane dotyczące wersjonowania, w tym datę obowiązywania wersji słownika. Podstawowa struktura słownika zawiera pozycje, na które składają się w szczególności:

- kod pozycji,
- nazwa pozycji,
- atrybuty pozycji będące mapą nazwa/wartość.

Dodatkowo poszczególne pozycje mogą posiadać relacje między sobą, np. hierarchię, a niektóre ze słowników, niedające się zapisać w postaci hierarchicznych pozycji, wymagają wdrożenia w postaci natywnej, tj. takiej, w jakiej zostały udostępnione przez twórców.

19 TECHNICZNY OBSZAR POWIADOMIEŃ

19.1 Opis usług biznesowych obszaru

19.1.1 Generowanie i przesyłanie powiadomień

System P1 w ramach wsparcia obsługi pozostałych funkcjonalności P1 zapewni mechanizm powiadomień, czyli generowania i przesyłania przez P1 komunikatów o wystąpieniu istotnych dla odbiorców sytuacji biznesowych.

Każdy z podsystemów, który przy realizacji usługi biznesowej lub technicznej powinien wygenerować powiadomienie przekaże żądanie wygenerowania powiadomienia do podsystemu SAA. Następnie SAA przy wykorzystaniu jednego z szablonów zbuduje komunikat powiadomienia, który zostanie uzupełniony o dane przekazane w wywołaniu, a także pozostałe dane pobrane za pośrednictwem SUS m.in. z SAZ w zakresie danych kontaktowych, na które powinny zostać wysłane powiadomienia. Podsystem SAA będzie przekazywał zbudowane powiadomienie odpowiednim kanałem:

- adresatom przez wysłanie SMS,
- adresatom przez wysłanie wiadomości poczty elektronicznej (e-mail).

Poza opisanym powyżej schematem działania usługa powiadomień powinna zapewnić, że dowolny z podsystemów będzie miał możliwość przekazania wszystkich żądanych parametrów powiadomienia do SAA. Będzie miało to istotny wpływ na wydajność np. w kontekście obsługi korespondencji grupowej, tj. list dystrybucyjnych PPP.

19.1.2 Konfigurowanie danych kontaktowych

P1 zapewni każdemu z użytkowników systemu możliwość konfiguracji danych kontaktowych, na które powiadomienia mają być przekazywane. Odpowiednie grupy użytkowników w ramach dedykowanych aplikacji będą dodawać, modyfikować i usuwać dane kontaktowe:

- usługobiorcy - numeru telefonu i adresu e-mail z poziomu aplikacji IKP,
- pracownicy usługodawców (medyczni oraz niemedyczni) posiadający konto w P1 - numeru telefonu i adresu e-mail powiązany z kontekstem usługodawcy, w imieniu którego występuje, z poziomu aplikacji AUA (planowane do realizacji w kolejnych wydaniach),
- administratorom usługodawców - numer telefonu i adres e-mail usługodawcy oraz adres usługi systemu usługodawcy.

19.1.3 Zarządzanie szablonami i powiadomieniami

Podsystem SAA zapewni administratorowi możliwość konfiguracji szablonów powiadomień oraz zarządzanie parametrami powiadomień, w zakresie obejmującym w szczególności:

- tworzenie, modyfikowanie i usuwanie szablonów powiadomień z uwzględnieniem rodzaju kanału na jaki mają zostać przesłane,
- aktywację i dezaktywację powiadomienia,
- konfigurację parametrów związanych z obsługą powiadomień,
- przeglądanie błędów wywołań usług odpowiadających za wysłanie powiadomień.

19.2 Zakres danych

Zakres danych dla powiadomień obejmuje w szczególności:

- nazwa powiadomienia,
- kod sytuacji, której dotyczy powiadomienie,
- aktywowane/dezaktywowane,
- adresaci powiadomienia,
- temat,
- treść,
- załączniki,
- rodzaj powiadomienia,
- nazwa i kod parametru związanego z obsługą powiadomień,
- wartość parametru związanego z obsługą powiadomień.

Lista powiadomień wysyłanych przez P1 (nie obejmuje powiadomień generowanych przez P2) oraz adresatów powinna obejmować w szczególności:

Powiadomienia	Kanał		Adresat									
	sms	e-mail	usługobiorca	małoletni	pełnomocnik	usługodawca	zdefiniowana lista adresatów	Administrator P1	Autor wniosku	Pracownik usługodawcy	Administrator biznesowy	Użytkownik SOW
Wystawienie skierowania	x	x	x	x	x							
Wystawienie recepty	x	x	x	x	x							
Spełnienie kryterium obserwacji wskaźnika	x	x					x					
Potwierdzenie autoryzacji do danych	x		x									
Ustanowienie pełnomocnictwa	x	x			x							
Zgłoszenie błędu		x						x				
Informacje o zmianach w portalu		x					x					
Polecenie artykułu		x					x					
Zapisanie wniosku o założenie konta usługodawcy	x	x							x		x	
Decyzja o rozpatrzeniu wniosku o założenie konta usługodawcy	x	x							x			
Złożenie wniosku o zamknięcie konta usługodawcy	x	x				x						
Wygenerowanie hasła dla administratorów biznesowych i użytkowników SOW	x	x									x	x
Przypisanie pracownika usługodawcy do roli lub poziomu struktury organizacyjnej		x								x		

**CENTRUM SYSTEMÓW INFORMACYJNYCH OCHRONY ZDROWIA**

ul. Stanisława Dubois 5A • 00-184 Warszawa, Polska

tel.: +48 22 597-09-27 • fax: +48 22 597-09-47

biuro@csioz.gov.pl • www.csioz.gov.pl

Skrytka ESP: /csiozgovpl/skrytka

Utworzenie listy dokumentów do przejęcia przez nowego kustosa (opiekuna) EDM		X				X						
Zatwierdzenie listy przez usługodawcę przejmującego EDM		X				X						

