

ЗАТВЕРДЖЕНО
Наказ Національної служби
здоров'я України
№ _____

ТЕХНІЧНІ ВИМОГИ
до електронної пацієнтської інформаційної системи для її підключення до
центральної бази даних електронної системи охорони здоров'я



СЕД АСКОД Національна служба здоров'я України
ДОКУМЕНТ № 978 від 08.12.2025
Сертифікат 3FAA9288358EC003040000007866330044EAD800
Підписувач Гусак Наталія Борисівна
Дійсний з 13.09.2024 0:00:00 по 12.09.2026 23:59:59

Зміст

1. ЗАГАЛЬНІ ВИМОГИ ДО ПІС	8
2. ЗАГАЛЬНІ ВИМОГИ ДО БЕЗПЕКИ	9
3. ФУНКЦІОНАЛЬНІ ВИМОГИ ДО МОДУЛІВ ПІС	11
3.1. Авторизація ПІС	11
3.2. Авторизація Користувача через АПІС	11
3.3. Авторизація Користувача через КПІС	12
3.4. Реєстрація Користувача через АПІС	13
3.5. Реєстрація Користувача через КПІС	18
3.6. Передача електронних копій оригіналів документів до Системи	22
3.7. Припинення дії токенів	23
3.8. Управління доступами, наданими Користувачем для ПІС	23
3.9. Отримання і перегляд даних запису про пацієнта	24
3.9.1. Загальні вимоги до отримання і перегляду даних запису про пацієнта	24
3.9.2. Перегляд персональних даних пацієнта	24
3.9.3. Отримання інформації щодо статусів верифікації пацієнта	26
3.9.4. Отримання інформації щодо методів автентифікації	31
3.10. Зміна персональних даних пацієнта	32
3.10.1. Загальні вимоги по зміні персональних даних	32
3.10.2. Запити на зміну персональних даних	34
3.10.3. Реєстрація методу автентифікації	34
3.10.4. Оновлення методу автентифікації	35
3.11. Управління Деклараціями	35
3.11.1. Подання Декларації	35
3.11.2. Отримання та перегляд Запитів на реєстрацію запису про Декларацію	39
3.11.3. Перегляд Декларацій	39
3.11.4. Припинення Декларації	40
3.12. Робота із переліками, довідниками та класифікаторами	41
3.12.1. Загальні вимоги до отримання довідників та відомостей реєстрів	41
3.12.2. Вимоги до отримання переліків з реєстрів Системи	41
3.12.3. Вимоги до отримання інформації з адресного компоненту Системи	42

Терміни та визначення

Терміни, що використовуються, та їх значення наведені у таблиці нижче.

Термін	Значення
АПС	Авторизована ПС, яка функціонує на Єдиному державному вебпорталі електронних послуг, зокрема із використанням мобільного додатка Порталу Дія (Дія)
Декларація	Декларація про вибір лікаря, який надає первинну медичну допомогу
ДРАЦСГ	Державний реєстр актів цивільного стану громадян
ДРФО	Державний реєстр фізичних осіб платників податків
ЕП	Кваліфікований електронний підпис або удосконалений електронний підпис, що базується на кваліфікованому сертифікаті електронного підпису, відповідно до Закону України "Про електронну ідентифікацію та електронні довірчі послуги"
ЕСОЗ	Електронна система охорони здоров'я
ЄДДР	Єдиний державний демографічний реєстр
ЄДР	Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань
Законний представник	Особа, яка має право виконувати дії в Системі від імені іншого пацієнта
Клієнт	Набір дозволів верхнього рівня, що визначають тип системи, яка забезпечує використання функціональних можливостей Системи Користувачами
КМУ	Кабінет Міністрів України
Користувач	Користувач Системи з роллю "PATIENT"
КПС	Кваліфікована ПС
Метод автентифікації	Спосіб автентифікації пацієнта, інформація про який зберігається в записі про нього в реєстрі пацієнтів Системи

Термін	Значення
МНП	Місце надання послуг, місце провадження господарської діяльності
МОЗ	Міністерство охорони здоров'я України
НСЗУ	Національна служба здоров'я України
НЦУ	Національний центр оперативно-технічного управління мережами телекомунікацій
ПІС	Електронна медична інформаційна система, яка забезпечує використання функціональних можливостей Системи Користувачем з роллю "PATIENT"
ПМГ	Програма державних фінансових гарантій медичного обслуговування населення (програма медичних гарантій)
ПМД	Первинна медична допомога
Політика конфіденційності	Документ (політика конфіденційності, повідомлення про обробку персональних даних тощо), що зокрема містить інформацію про те, як та які персональні дані користувача збираються, зберігаються, обробляються та передаються ПІС, а також про мету, обсяг, умови використання таких даних та права користувача щодо їх захисту
РНОКПП	Реєстраційний номер облікової картки платника податків
Роль	Набір дозволів, що визначають, які дії Користувач може виконувати і до якої функціональності має доступ в Системі
СГУСОЗ	Суб'єкт господарювання у сфері охорони здоров'я
Сервіс авторизації системи	"Auth UI" користувацький інтерфейс, через який здійснюється ідентифікація та авторизація Користувача в Системі. Веб-сторінка авторизації, яка надходить з ресурсу https://pis-auth.ehealth.gov.ua/
Система	Центральна база даних електронної системи охорони здоров'я
Скоуп	"Score", одиниця обліку прав доступу Користувача, яка визначає обсяг функціональних можливостей Користувача, які він може використовувати у Системі

Термін	Значення
Технічні вимоги	Технічні вимоги до електронної пацієнтської інформаційної системи для її підключення до центральної бази даних електронної системи охорони здоров'я
Токен	Електронний ключ, який використовується для безпечної автентифікації та підтвердження особи Користувача Системи
УНЗР	Унікальний номер запису в Єдиному державному демографічному реєстрі
Access token	Тимчасовий Токен, що видається Системою після успішної авторизації Користувача. Використовується ПІС для доступу до API
API	"Application Programming Interface", відкритий прикладний програмний інтерфейс Системи
API-key	Ключ, що надається ПІС для автентифікації при використанні API
BOM	"Byte-order mark", спеціальний символ на початку текстового файлу, який вказує на порядок байтів і кодування
CSP	"Content Security Policy", механізм безпеки веб-додатків, що дозволяє обмежувати ресурси, які можуть завантажуватися на веб-сторінці, запобігаючи атакам типу XSS
DSA	"Digital Signature Algorithm", алгоритм для створення цифрових підписів, який забезпечує автентичність та цілісність повідомлень
ECC	"Elliptic Curve Cryptography", метод шифрування, що використовує властивості еліптичних кривих для забезпечення безпеки даних
ECDSA	"Elliptic Curve Digital Signature Algorithm", алгоритм цифрового підпису, що використовує еліптичну криву для забезпечення автентичності та цілісності даних
Grant code	Одноразовий код, що видається Системою після надання Користувачем згоди на доступ до його даних.

Термін	Значення
	Використовується ПІС для отримання токена доступу ("Access token") та оновлення доступу ("Refresh token")
HSTS	"HTTP Strict Transport Security", політика безпеки, яка змушує браузері завжди використовувати захищене з'єднання (HTTPS) для доступу до веб-сайту
HTTPOnly	Прапор безпеки в cookie, який запобігає доступу до cookie через JavaScript, забезпечуючи додатковий захист від атак типу XSS
JWT	"JSON Web Token", стандартизований формат токена доступу, який використовується для безпечного обміну інформацією між сторонами у вигляді підписаного JSON-об'єкта
LFI	"Local File Inclusion", процес включення файлів, які вже локально присутні на сервері, через експлуатацію вразливих процедур включення, реалізованих як мобільний додаток ПІС
NIST	"National Institute of Standards and Technology", агентство США, яке розробляє стандарти та технології в галузі науки і технологій, зокрема в сфері криптографії
OTP	"One-time password", тимчасовий пароль, який дійсний тільки для одного сеансу або транзакції
Refresh token	Тимчасовий Токен, що видається Системою після успішної авторизації Користувача, який дозволяє ПІС від імені Користувача отримати новий Access token
RFI	"Remote File Inclusion", процес включення віддалених файлів через експлуатацію вразливих процедур включення, реалізованих як мобільний додаток ПІС
RSA	"Rivest-Shamir-Adleman", алгоритм асиметричного шифрування, який використовує пару ключів (публічний і приватний) для шифрування та підпису даних
SameSite	Атрибут cookie, який обмежує надсилання cookie разом із запитом між різними сайтами, знижуючи ризик CSRF-атак

Термін	Значення
Secure	Прапор безпеки в cookie, який дозволяє передавати cookie лише через захищене з'єднання HTTPS, що запобігає перехопленню даних через незашифровані канали
SQL	"Structured query language", мова для здійснення запитів, внесення змін та керування реляційними базами даних
SSL	"Secure Sockets Layer", протокол безпеки, який забезпечує шифрування даних між веб-сервером і браузером, забезпечуючи безпечну передачу інформації
TLS	"Transport Layer Security", криптографічний протокол, який забезпечує безпечну передачу даних в Інтернеті, шляхом шифрування, автентифікації сторін і забезпечення цілісності даних
URL	"Uniform Resource Locator", стандартизована адреса ресурсу в інтернеті
UTC	"Universal Time Coordinated", всесвітній координований час
XSS	"Cross-Site Scripting", вразливість веб-додатків, що дозволяє зловмисникам вставляти шкідливий скрипт на веб-сторінки, які відображаються користувачам

1. ЗАГАЛЬНІ ВИМОГИ ДО ПІС

- 1.1. ПІС забезпечує можливість обміну даними з Системою через API.
- 1.2. При відображенні інформації та документів, отриманих із Системи, ПІС забороняється вносити до них зміни, що викривляють їх суть.

1.3. Загальні системні вимоги:

- 1.3.1. параметр ПІС "redirect_uri" має містити відповідний URL з чинним сертифікатом TLS, де доменом буде тільки такий домен, де ПІС здатна опрацювати запити та відповіді від Системи;
- 1.3.2. ПІС повинна використовувати інтервал таймауту очікування не менше 60 секунд на будь-які синхронні запити до Системи, крім випадків коли відповідь від Системи була отримана раніше;
- 1.3.3. в разі створення ідентифікатору запису на стороні ПІС для використання його в методах API Системи, остання повинна забезпечити кодування UUID згідно стандарту RFC4122 першої версії (мітка часу та апаратний ідентифікатор).
- 1.3.4. версії служб, що працюють на відкритих портах ПІС, не повинні мати експлойтів, зазначених в базі даних exploit-db (www.exploit-db.com).

1.4. Загальні вимоги до безпеки:

- 1.4.1. для забезпечення доступу Користувачу до Системи, ПІС повинна використовувати Access token згідно із специфікацією API, контролювати дані про дату валідності Access token (параметр "expires_at") та, у разі закінчення дії, оновлювати його за Refresh token (метод API "Renew access token using refresh token");
 - 1.4.1.1. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 1.4.2. ПІС для мобільного додатку повинна зберігати Access token і Refresh token на стороні клієнта у безпечний спосіб, а саме: токени повинні зберігатися у захищених сховищах, які забезпечують шифрування та обмеження доступу;
- 1.4.3. у запитах на гарантування обсягу автентифікації Користувачів, ПІС передає не більший ніж визначений специфікацією Системи обсяг Скоупів, який необхідний Користувачу для подальшої роботи із Системою.

1.5. Загальні вимоги до інтерфейсів:

- 1.5.1. ПІС забезпечує можливість внесення інформації до Системи через свій інтерфейс українською мовою. У випадках, коли використання літер українського алфавіту призводить до спотворення інформації, можуть використовуватися латинські літери та спеціальні символи, зокрема для запису адрес електронної пошти;
- 1.5.2. на стороні КПІС заборонено використовувати проміжні інтерфейси авторизації Користувачів до Системи, окрім Сервісу авторизації системи;

- 1.5.3. інтерфейс Користувача ПС повинен відповідати вимогам ДСТУ EN 301 549:2022 (EN 301 549 V3.2.1 (2021–03), IDT) "Інформаційні технології. Вимоги щодо доступності продуктів та послуг ІКТ";
- 1.5.4. у разі отримання помилки від Системи (неправильність введення даних Користувачами, авторизація тощо) та на підставі виконання Користувачем визначених дій та/або значень параметрів Системи, ПС відображає Користувачам інформаційні повідомлення у текстовому вигляді, українською мовою. Якщо текст інформаційних повідомлень визначено цими Технічними вимогами або Додатком 1 до цих Технічних вимог, то ПС інформує користувача використовуючи такий текст.
- 1.5.5. у разі необхідності внесення Користувачем інформації про дату та час, ПС передає в Систему таку інформацію за UTC.
- 1.6. ПС повинна надавати функціональну можливість засвідчення даних, що вносяться до Системи Користувачами виключно за допомогою ЕП, в якому наявні атрибути certificate-values та revocation-values, які свідчать про CAdES-X Long формат довгострокового розширеного підпису ЕП;
 - 1.6.1. для методів АРІ, які вимагають накладення ЕП, у ПС має бути забезпечена можливість накладення ЕП без переходу на зовнішні ресурси (за виключенням, якщо такий перехід необхідний для використання засобу ЕП, який використовується Користувачем);
 - 1.6.2. для методів АРІ, які вимагають накладення ЕП, підписаний контент має передаватися до Системи в закодованому вигляді у форматі BASE64;
 - 1.6.3. ПС повинна перевіряти контент, закодований в BASE64 до накладання ЕП та, в разі наявності, видаляти символ Юнікоду з кодом U+FEFF ("нерозривний пробіл нульової ширини", або BOM) для уникнення проблем з подальшою обробкою закодованої інформації.
- 1.7. ПС дозволяється предзаповнювати дані пацієнта при його реєстрації в Системі та/або оновленні даних про себе з можливістю редагування таких відомостей (крім випадків, передбачених цими Технічними вимогами);
 - 1.7.1. АПС може забороняти редагування таких даних Користувачем, якщо такі відомості отримані з державних реєстрів, що є першоджерелом відповідної інформації (ЄДДР, ДРФО, ДРАЦС, ЄДР).

2. ЗАГАЛЬНІ ВИМОГИ ДО БЕЗПЕКИ

- 2.1. ПС повинна використовувати чинний SSL/TLS сертифікат, який відповідає таким криптографічним стандартам: ECC (ECDSA P-256, P-384) або RSA (з довжиною ключа не менше 2048 біт);
- 2.2. ПС повинна бути захищена від SQL-ін'єкцій. Дані, що передаються до ПС не повинні призводити до виконання непередбачених SQL-запитів, модифікації існуючих запитів або виконання додаткових запитів, ініційованих Користувачем;

- 2.3. ПІС повинна бути захищена від XSS-ін'єкцій. Дані, що передаються до ПІС або обробляються на клієнтській стороні не повинні призводити до виконання неавторизованого чи шкідливого коду у контексті веб браузера кінцевого Користувача;
- 2.4. ПІС повинна бути захищена від SSRF-атак. Дані що передаються до ПІС не повинні призводити до формування запитів з боку сервера до внутрішніх або зовнішніх ресурсів, доступ до яких не передбачено бізнес-логікою Системи;
- 2.5. ПІС повинна бути захищена від атак LFI та RFI. Дані що передаються до ПІС не повинні призводити до завантаження, читання, виконання або іншим чином обробки локальних чи віддалених файлів, доступ до яких не передбачено;
- 2.6. ПІС повинна бути захищена від атак, що призводять до виконання довільного коду або системних команд ("Command Execution"). Дані що передаються до ПІС не повинні дозволяти запуск системних команд, а також виконання скриптів або програм на стороні сервера;
- 2.7. ПІС повинна використовувати тільки безпечні способи передачі даних, а саме між ПІС та Користувачем ПІС - протокол TLS версії не нижче 1.2 або інший спосіб, що відповідає вимогам чинного законодавства;
- 2.8. ПІС для веб-застосунку повинна зберігати Access token і Refresh token на стороні клієнта у безпечний спосіб, а саме токени повинні зберігатися лише у cookie з параметрами HttpOnly, Secure та SameSite що унеможливило б доступ до них через JavaScript та передачу через незахищені з'єднання;
- 2.9. Після успішної авторизації в Системі через мобільний додаток ПІС, ПІС має забезпечити обов'язкове встановлення та використання Користувачем локального PIN-коду додатку або біометричної автентифікації ("Face ID", "Touch ID", сканер відбитка пальця, тощо). Застосування таких додаткових вимог є обов'язковим протягом терміну доступу Користувача до отриманих від Системи даних або терміну дії Refresh token.

ПІС має вимагати введення PIN-коду або проходження біометричної автентифікації у разі якщо Користувач:

- не здійснює жодних дій у мобільному додатку (відсутня будь-яка взаємодія з інтерфейсом, зокрема введення даних із клавіатури, переміщення між екранами, натискання (тап) на елементи інтерфейсу, прокручування, жести або інші дії користувача) протягом п'яти хвилин;
- припинив використання додатку (додаток завершив роботу на пристрої Користувача, що включає: самостійне закриття додатку користувачем (через свайп або кнопку "Закрити"), вивантаження додатку з пам'яті ОС (системне закриття через нестачу ресурсів або

тривалу неактивність), вихід користувача через кнопку “Вихід / Logout”, перезапуск пристрою або аварійне завершення додатку).

3. ФУНКЦІОНАЛЬНІ ВИМОГИ ДО МОДУЛІВ ПІС

3.1. Авторизація ПІС

3.1.1. ПІС при роботі з Системою має використовувати дійсний API-key.

3.2. Авторизація Користувача через АПІС

Передумови:

- ПІС має мати успішно протестовану функціональність згідно вимог:
 - п. 3.1 Авторизація;
 - п. 3.12 Робота із переліками, довідниками та класифікаторами.
- Вік Користувача більше 14 років.

3.2.1. АПІС повинна надати Користувачу можливість ознайомитися з політикою конфіденційності ПІС до початку проходження авторизації;

3.2.1.1. АПІС повинна надати можливість Користувачу зберегти політику конфіденційності у форматі текстового файлу;

3.2.1.2. АПІС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача з положеннями політики конфіденційності АПІС (окрема дія Користувача в інтерфейсі ПІС);

3.2.2. АПІС повинна надати Користувачу можливість ознайомитися з переліком Скоупів, які будуть запитані для авторизації в Системі;

3.2.2.1. АПІС повинна відобразити Користувачеві форму наступного змісту:

[ПІБ Користувача],
щоб авторизуватися в Електронній системі охорони здоров'я, ви маєте погодити надання прав на виконання дій в системі через [Назва АПІС].
Ви надаєте доступ для таких функцій:
[перелік Скоупів, визначений згідно Специфікації Системи]

3.2.2.2. АПІС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача на надання ПІС Скоупів (окрема дія Користувача в інтерфейсі ПІС);

3.2.2.3. у випадку відхилення Користувачем надання Скоупів АПІС повинна припинити авторизацію та повернути Користувача на початок процесу авторизації;

3.2.3. АПІС має отримати JWT для авторизації (метод API "Get nonce");

3.2.3.1. у випадку отримання помилки від Системи АПІС повинна зупинити процес авторизації та обробити помилку згідно Додатку 1. "Таблиця обробки помилок";

- 3.2.4. АПС має сформувати дані для авторизації і перелік Скоупів для підпису ЕП згідно специфікації методу і забезпечити Користувачу можливість накласти ЕП на пакет даних (метод API "TRUSTED PIS. Patient sign-in");
- 3.2.5. АПС повинна передати підписані дані до Системи (метод API "TRUSTED PIS. Patient sign-in");
 - 3.2.5.1. у разі успішної авторизації, АПС повинна зберегти отриманий від Системи Access token і Refresh token;
 - 3.2.5.2. у разі отримання помилки від Системи АПС повинна зупинити процес авторизації та обробити помилку згідно Додатку 1. "Таблиця обробки помилок".

3.3. Авторизація Користувача через КПС

Передумови:

- ПС має мати успішно протестовану функціональність згідно вимог:
 - п. 3.1 Авторизація;
 - п. 3.12 Робота із переліками, довідниками та класифікаторами.
 - Вік Користувача більше 14 років.
- 3.3.1. КПС повинна надати Користувачу можливість ознайомитися з політикою конфіденційності ПС до початку проходження авторизації;
 - 3.3.1.1. КПС повинна надати можливість Користувачу зберегти політику конфіденційності у форматі текстового файлу;
 - 3.3.1.2. КПС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача з положеннями політики конфіденційності КПС (окрема дія Користувача в інтерфейсі ПС);
 - 3.3.2. КПС має отримати JWT для авторизації (метод API "Get nonce");
 - 3.3.2.1. у випадку отримання помилки від Системи КПС повинна зупинити процес авторизації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
 - 3.3.3. КПС повинна надати Користувачу можливість підписати ЕП дані для авторизації (отримані за допомогою API "Get nonce");
 - 3.3.4. КПС повинна перенаправити Користувача на веб-сторінку сервісу авторизації, передавши підписані дані до Системи (метод API "PIS. Patient sign-in");
 - 3.3.4.1. у разі отримання помилки Системи КПС повинна зупинити процес авторизації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
 - 3.3.5. за результатами роботи Користувача з сервісом авторизації Системи, у разі погодження Користувачем Скоупів, КПС повинна отримати від Системи "grant code";
 - 3.3.5.1. у разі відмови Користувача від надання КПС Скоупів завершити процес авторизації;

- 3.3.6. КПС має сформувавати запит на отримання токена доступу ("access token") та токена оновлення доступу ("refresh token") з використанням "grant code" (метод API Системи "Exchange OAuth Code Grant to Access Token");
- 3.3.6.1. у разі отримання помилки Системи КПС повинна зупинити процес авторизації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.4. Реєстрація Користувача через АПС

Передумови:

- ППС має мати успішно протестовану функціональність згідно вимог:
 - п. 3.1 Авторизація;
 - п. 3.2 Авторизація Користувача через АПС;
 - п. 3.12 Робота із переліками, довідниками та класифікаторами.
- Вік Користувача більше 14 років.
- Користувач має РНОКПП

- 3.4.1. АПС має надати Користувачу можливість ознайомитися з політикою конфіденційності АПС;
- 3.4.1.1. АПС повинна надати можливість Користувачу зберегти політику конфіденційності у форматі текстового файлу;
- 3.4.1.2. АПС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача з положеннями політики конфіденційності АПС (окрема дія Користувача в інтерфейсі ППС);
- 3.4.2. АПС повинна надати Користувачу можливість ознайомитися з формою надання АПС переліку Скоупів, усі чи частину яких буде надано Користувачем для ППС у разі успішного проходження реєстрації;
- 3.4.2.1. АПС повинна відобразити Користувачеві форму наступного змісту:

[ПІБ Користувача],
щоб успішно авторизуватися в Електронній системі охорони здоров'я, ви маєте погодити надання прав на виконання дій в системі через [Назва АПС].
Ви надаєте доступ для таких функцій:
[перелік Скоупів, визначений згідно Специфікації Системи]

- 3.4.2.2. АПС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача на надання ППС Скоупів (окрема дія Користувача в інтерфейсі ППС);
- 3.4.2.3. у випадку відхилення Користувачем надання Скоупів АПС повинна зупинити процес реєстрації та повернути Користувача на початок процесу реєстрації;

- 3.4.3. АПС має отримати JWT для авторизації (метод API "Get nonce");
- 3.4.3.1. у випадку отримання помилки від Системи АПС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 3.4.4. АПС повинна відобразити форму для реєстрації Користувача після отримання даних для авторизації від Системи;
- 3.4.5. АПС повинна заповнити форму для реєстрації відомостями одержаними з державних реєстрів (ЄДДР, ДРФО, ДРАЦС, ЄДР) без можливості їх редагування Користувачем згідно наступних вимог:
- 3.4.5.1. ім'я (параметр "first_name") - обов'язково;
- 3.4.5.2. прізвище (параметр "last_name") - обов'язково;
- 3.4.5.3. по батькові (параметр "second_name");
- 3.4.5.4. дата народження (параметр "birth_date"), яка заповнюється в форматі "ДД.ММ.РРРР" - обов'язково;
- 3.4.5.5. країна народження (параметр "birth_country"), яка заповнюється Користувачем значенням ("value") згідно з довідником "COUNTRY" та, у разі відсутності необхідного значення, довільним значенням - обов'язково;
- 3.4.5.6. місце народження (параметр "birth_settlement") - обов'язково;
- 3.4.5.7. стать (параметр "gender") згідно з довідником "GENDER"- обов'язково;
- 3.4.5.8. РНОКПП (параметр "tax_id"), має відповідати формату "[^][0-9]{10}\$";
- 3.4.5.9. документ пацієнта, що посвідчує особу (масив "documents") - обов'язково один і тільки один документ, зокрема:
- a. тип документа (параметр "type"), одне зі значень довідника "DOCUMENT_TYPE", дозволених конфігураційним параметром "PIS_PERSON_REGISTRATION_DOCUMENT_TYPES" - обов'язково один з:
 - i. "PASSPORT";
 - ii. "NATIONAL_ID";
 - iii. "TEMPORARY_PASSPORT";
 - iv. "BIRTH_CERTIFICATE";
 - v. "TEMPORARY_CERTIFICATE";
 - vi. "PERMANENT_RESIDENCE_PERMIT";
 - vii. "REFUGEE_CERTIFICATE";
 - viii. "COMPLEMENTARY_PROTECTION_CERTIFICATE";
 - ix. "BIRTH_CERTIFICATE_FOREIGN";
 - b. серію (за наявності) та номер документа (параметр "number") з урахуванням формату, визначеного специфікацією Системи - обов'язково;

- c. дата видачі (параметр "issued_at") - обов'язково, дата видачі повинна бути меншою ніж поточна дата, дата видачі повинна бути більшою ніж дата народження Користувача;
 - d. дійсний до (параметр "expiration_date");
 - e. орган яким виданий (параметр "issued_by");
- 3.4.5.10. документ пацієнта, що посвідчує дієздатність (масив "documents") - для Користувачів, чий вік більше або дорівнює значенню конфігураційного параметра "no_self_registration_age", але менше значення конфігураційного параметра "person_full_legal_capacity_age", АПІС повинна додати у масив "documents" обов'язково один і тільки один документ, зокрема:
 - a. тип документа (параметр "type"), одне зі значень довідника "DOCUMENT_TYPE", дозволених конфігураційним параметром "PIS_PERSON_LEGAL_CAPACITY_DOCUMENT_TYPES" - обов'язково;
 - b. серію (за наявності) та номер документа (параметр "number") з урахуванням формату, визначеного специфікацією Системи - обов'язково;
 - c. дата видачі (параметр "issued_at") - обов'язково, дата видачі повинна бути меншою ніж поточна дата, дата видачі повинна бути більшою ніж дата народження Користувача;
 - d. дійсний до (параметр "expiration_date")- дата закінчення дії повинна більшою ніж поточна дата;
 - e. орган яким виданий (параметр "issued_by");
- 3.4.5.11. УНЗР (параметр "unzr"), має відповідати формату: "[0-9]{8}-[0-9]{5}\$" - АПІС повинна заповнити УНЗР відомостями отриманими з ЄДДР;
- 3.4.6. Користувач повинен мати можливість заповнити та/або змінити попередньо заповнені дані для реєстрації згідно наступних вимог:
 - 3.4.6.1. кодове слово (параметр "secret"), відповідно формату "[A-Za-zA-Яа-яҐґїіІіЄє0-9]{6,20}\$" - обов'язково;
 - 3.4.6.2. адреси пацієнта (масив параметрів "addresses") - обов'язково, Користувач повинен обов'язково вказати адресу фактичного місця проживання;
 - a. тип адреси (параметр "type"), згідно з довідником "ADDRESS_TYPE", значення "RESIDENCE" - обов'язково;
 - b. країна (параметр "country"), згідно з довідником "COUNTRY" - обов'язково;
 - c. область (параметр "area") - обов'язково;
 - d. район області (параметр "region");
 - e. населений пункт (параметр "settlement") - обов'язково;
 - f. тип населеного пункту - (параметр "settlement_type"), згідно з довідником "SETTLEMENT_TYPE" - обов'язково;

- g. тип вулиці - (параметр "street_type"), згідно з довідником "STREET_TYPE";
 - h. назва вулиці (параметр "street");
 - i. будинок (параметр "building");
 - j. квартира (параметр "apartment");
 - k. поштовий індекс (параметр "zip");
- 3.4.6.3. контактний телефон Користувача (масив об'єктів "phones"):
- a. тип телефону (параметр "phones_type"), згідно з довідником "PHONE_TYPE" - обов'язково;
 - b. номер телефону в форматі " $^{\backslash}+38[0-9]\{10\}\$"$ (параметр "phones_number") - обов'язково;
- 3.4.6.4. метод автентифікації (об'єкт "authentication_methods") - обов'язково:
- a. тип (параметр "type"), згідно з довідником "AUTHENTICATION_METHOD", значення "OTP" - обов'язково;
 - b. номер мобільного телефону, в форматі " $^{\backslash}+38[0-9]\{10\}\$"$ (параметр "phone_number") - обов'язково;
- 3.4.6.5. електронна пошта (параметр "email"), домен якої не міститься в переліку заборонених (заблокованих) визначених відповідними розпорядженнями НЦУ - опційно;
- 3.4.6.6. бажаний спосіб зв'язку (параметр "preferred_way_communication") - обов'язково, параметр повинен відповідати одному з допустимих значень:
- a. електронна пошта (значення "email");
 - b. телефон (значення "phone");
- 3.4.6.7. дані особи для екстреного зв'язку (об'єкт "emergency_contact") - обов'язково:
- a. ім'я (параметр "first_name") - обов'язково;
 - b. прізвище (параметр "last_name") - обов'язково;
 - c. по батькові (параметр "second_name");
 - d. телефони контакту для екстреного зв'язку (масив об'єктів "emergency_contact.phones"):
- i. тип телефону (параметр "phones_type"), згідно з довідником "PHONE_TYPE" - обов'язково;
 - ii. номер в форматі " $^{\backslash}+38[0-9]\{10\}\$"$ (параметр "number") - обов'язково;
- 3.4.7. АПС повинна надати Користувачу можливість підписати дані для реєстрації за допомогою ЕП;
- 3.4.8. АПС повинна ініціювати верифікацію номера телефону, вказаного в якості методу автентифікації пацієнта (метод API "Verify phone number");
- 3.4.8.1. якщо у відповідь на запит в параметрі "phone verification result" отримано значення "OTP sent", АПС повинна відобразити

Користувачу поле для введення коду верифікації у форматі " $\backslash d\{4\}\$$ ";

- 3.4.8.1.1. після введення Користувачем в інтерфейсі АПІС отриманого коду для верифікації номера телефона, АПІС має додати одноразовий пароль до попередньо підписаних даних для реєстрації;
- 3.4.8.2. якщо у відповідь на запит в параметрі "phone verification result" отримано значення "Verified", верифікація номера телефона не потрібна, АПІС не повинна відображати Користувачу поле для введення коду верифікації;
- 3.4.8.3. у випадку отримання помилки від Системи АПІС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 3.4.9. АПІС має передати реєстраційні дані Користувача до Системи (метод API "TRUSTED PIS. Patient sign-up");
- 3.4.9.1. у разі успішного отримання токенів АПІС має повідомити Користувача про успішне завершення реєстрації та авторизації;
- 3.4.9.2. якщо в процесі реєстрації пацієнта:
 - в масиві "person.documents" присутній документ з типом "PERMANENT_RESIDENCE_PERMIT",
 - або вік Користувача більше або дорівнює значенню конфігураційного параметра "no_self_registration_age", але менше значення конфігураційного параметра "person_full_legal_capacity_age", та в "person.documents" міститься документ з типом, що відповідає конфігураційному параметру: "PIS_PERSON_LEGAL_CAPACITY_DOCUMENT_TYPES",

АПІС повинна забезпечити можливість завантажити електронні копії оригіналів документів відповідно до вимог п.3.6.

- 3.4.9.3. у разі отримання помилки Системи АПІС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок.
- 3.4.9.4. АПІС має скерувати Користувача (з можливістю перейти до його використання) на електронний кабінет пацієнта ЦБД ЕСОЗ для здійснення реєстрації у разі якщо Користувач:
 - не може використати ЕП в АПІС;
 - має документ, відомості про який неможливо отримати з державних реєстрів;
 - має документ, який потребує завантаження електронної копії оригіналу документу відповідно до специфікації Системи.

3.5. Реєстрація Користувача через КПІС

Передумови:

- ПІС має мати успішно протестовану функціональність згідно вимог:

- п. 3.1 Авторизація;
 - п. 3.3 Авторизація Користувача через КПС;
 - п. 3.12 Робота із переліками, довідниками та класифікаторами.
 - Вік Користувача більше 14 років.
- 3.5.1. КПС має надати Користувачу можливість ознайомитися з політикою конфіденційності КПС;
- 3.5.1.1. КПС повинна надати можливість Користувачу зберегти політику конфіденційності у форматі текстового файлу;
- 3.5.1.2. КПС повинна надати можливість Користувачу продовжити роботу з Системою лише після явної згоди Користувача з положеннями політики конфіденційності КПС (окрема дія Користувача в інтерфейсі ПС);
- 3.5.2. КПС має отримати JWT для авторизації (метод API "Get nonce");
- 3.5.2.1. у випадку отримання помилки від Системи КПС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 3.5.3. КПС повинна відобразити форму для реєстрації Користувача після отримання даних для авторизації від Системи;
- 3.5.4. Користувач повинен мати можливість заповнити та/або змінити попередньо заповнені дані для реєстрації згідно з наступними вимогами:
- 3.5.4.1. ім'я (параметр "first_name") - обов'язково;
- 3.5.4.2. прізвище (параметр "last_name") - обов'язково;
- 3.5.4.3. по батькові (параметр "second_name");
- 3.5.4.4. дата народження (параметр "birth_date"), яка заповнюється в форматі "ДД.ММ.РРРР" - обов'язково;
- 3.5.4.5. країна народження (параметр "birth_country"), яка заповнюється Користувачем значенням ("value") згідно з довідником "COUNTRY" та, у разі відсутності необхідного значення, довільним значенням - обов'язково;
- 3.5.4.6. місце народження (параметр "birth_settlement") - обов'язково;
- 3.5.4.7. стать (параметр "gender") згідно з довідником "GENDER"- обов'язково;
- 3.5.4.8. електронна пошта (параметр "email"), домен якої не міститься в переліку заборонених (заблокованих) визначених відповідними розпорядженнями НЦУ;
- 3.5.4.9. відмітка про відмову РНОКПП (параметр "no_tax_id");
- 3.5.4.10. РНОКПП (параметр "tax_id"), має відповідати формату "[0-9]{10}\$";
- 3.5.4.11. кодове слово (параметр "secret") відповідно формату "[A-Za-zA-Яа-яҐґїіЛіЄє0-9]{6,20}\$" - обов'язково;
- 3.5.4.12. документ пацієнта, що посвідчує особу (масив "documents") - обов'язково один і тільки один документ, зокрема:

- a. тип документа (параметр "type"), одне зі значень довідника "DOCUMENT_TYPE", дозволених конфігураційним параметром "PIS_PERSON_REGISTRATION_DOCUMENT_TYPES" - обов'язково;
 - b. серію (за наявності) та номер документа (параметр "number") - обов'язково;
 - i. зазначається користувачем та передається до системи з урахуванням формату, визначеного специфікацією системи;
 - c. дата видачі (параметр "issued_at") - обов'язково зазначається, дата видачі повинна бути меншою ніж поточна дата, дата видачі повинна бути більшою ніж дата народження Користувача;
 - d. дійсний до (параметр "expiration_date");
 - e. орган яким виданий (параметр "issued_by");
- 3.5.4.13. документ пацієнта, що посвідчує дієздатність (масив "documents") - для Користувачів, чий вік більше або дорівнює значенню конфігураційного параметра "no_self_registration_age", але менше значення конфігураційного параметра "person_full_legal_capacity_age", КПІС повинна додати у масив "documents" обов'язково один і тільки один документ, зокрема:
- a. тип документа (параметр "type"), одне зі значень довідника "DOCUMENT_TYPE", дозволених конфігураційним параметром "PIS_PERSON_LEGAL_CAPACITY_DOCUMENT_TYPES" - обов'язково;
 - b. серію (за наявності) та номер документа (параметр "number") - обов'язково;
 - i. зазначається користувачем та передається до системи з урахуванням формату, визначеного специфікацією системи;
 - c. дата видачі (параметр "issued_at") - обов'язково зазначається, дата видачі повинна бути меншою ніж поточна дата, дата видачі повинна бути більшою ніж дата народження Користувача;
 - d. дійсний до (параметр "expiration_date")- дата закінчення дії повинна більшою ніж поточна дата;
 - e. орган яким виданий (параметр "issued_by");
- 3.5.4.14. УНЗР (параметр "unzr"), має відповідати формату: "[^][0-9]{8}-[0-9]{5}\$" ;
- 3.5.4.15. адреси пацієнта (масив параметрів "addresses") - обов'язково, Користувач повинен обов'язково вказати адресу фактичного місця проживання;

- a. тип адреси - (параметр "type"), згідно з довідником "ADDRESS_TYPE", значення "RESIDENCE" - обов'язково;
 - b. країна - (параметр "country"), згідно з довідником "COUNTRY" - обов'язково;
 - c. область - (параметр "area") - обов'язково;
 - d. район області - (параметр "region");
 - e. населений пункт - (параметр "settlement") - обов'язково;
 - f. тип населеного пункту - (параметр "settlement_type"), згідно з довідником "SETTLEMENT_TYPE" - обов'язково;
 - g. тип вулиці - (параметр "street_type"), згідно з довідником "STREET_TYPE";
 - h. назва вулиці - (параметр "street");
 - i. будинок - (параметр "building");
 - j. квартира - (параметр "apartment");
 - k. поштовий індекс - (параметр "zip");
- 3.5.4.16. контактний телефон Користувача (масив об'єктів "phones"):
- a. тип телефону (параметр "phones_type"), згідно з довідником "PHONE_TYPE" - обов'язково;
 - b. номер телефону в форматі " $^{\backslash}\backslash+38[0-9]\{10\}\$"$ (параметр "phones_number") - обов'язково;
- 3.5.4.17. метод автентифікації (об'єкт "authentication_methods") - обов'язково:
- a. тип (параметр "type"), згідно з довідником "AUTHENTICATION_METHOD" - обов'язково;
 - b. номер мобільного телефону, що належить оператору в Україні, в форматі " $^{\backslash}\backslash+38[0-9]\{10\}\$"$ (параметр "phone_number") - обов'язково;
- 3.5.4.18. бажаний спосіб зв'язку (параметр "preferred_way_communication")— обов'язково, параметр повинен відповідати одному з допустимих значень:
- c. електронна пошта (значення "email");
 - d. телефон (значення "phone");
- 3.5.4.19. дані особи для екстреного зв'язку (об'єкт "emergency_contact") - обов'язково:
- a. ім'я (параметр "first_name") - обов'язково;
 - b. прізвище (параметр "last_name") - обов'язково;
 - c. по батькові (параметр "second_name");
 - d. телефон контакту для екстреного зв'язку (масив об'єктів "emergency_contact.phones"):
 - i. тип телефону (параметр "phones_type"), згідно з довідником "PHONE_TYPE" - обов'язково;
 - ii. номер телефону (параметр "number" в форматі " $^{\backslash}\backslash+38[0-9]\{10\}\$"$) - обов'язково;
- 3.5.5. КПС повинна надати Користувачу можливість підписати дані для реєстрації за допомогою ЕП без переходу на зовнішні ресурси (за

- виключенням, якщо такий перехід необхідний для використання ЕП, який використовується Користувачем);
- 3.5.6. після підписання Користувачем даних для реєстрації за допомогою ЕП, КПС має передати підписані дані до Системи, у випадку позитивної відповіді, КПС повинна відобразити веб-частину сервісу авторизації Системи (метод API "PIS. Patient sign-up");
- 3.5.6.1. у разі отримання помилки Системи КПС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 3.5.7. За результатами роботи Користувача з Сервісом авторизації Системи, у разі погодження Користувачем Скоупів, КПС повинна отримати від Системи Grant code;
- 3.5.7.1. у разі відмови Користувача від надання КПС Скоупів завершити процес реєстрації;
- 3.5.8. КПС має сформувавати запит на отримання Access token і Refresh token з використанням Grant code (метод API "Exchange OAuth Code Grant to Access Token")
- 3.5.8.1. у разі успішного отримання токенів, КПС має повідомити Користувача про успішне завершення реєстрації та авторизації;
- 3.5.8.2. якщо в процесі реєстрації пацієнта:
- в масиві "person.documents" присутній документ з типом "PERMANENT_RESIDENCE_PERMIT",
 - або вік Користувача більше або дорівнює значенню конфігураційного параметра "no_self_registration_age", але менше значення конфігураційного параметра "person_full_legal_capacity_age", та в "person.documents" міститься документ з типом, що відповідає конфігураційному параметру: "PIS_PERSON_LEGAL_CAPACITY_DOCUMENT_TYPES",
- КПС повинна:
- 3.5.8.2.1. відобразити користувачу повідомлення
- Завантажте копії ваших документів. До завантаження документів можливості особистого кабінету пацієнта будуть обмежені.
- 3.5.8.2.2. забезпечити можливість завантажити електронні копії оригіналів документів відповідно до вимог п.3.6.
- 3.5.8.3. у разі отримання помилки Системи КПС повинна зупинити процес реєстрації та обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.6. Передача електронних копій оригіналів документів до Системи

Передумови:

- ПС має мати успішно протестовану функціональність згідно з вимогами:

- п. 3.1 Авторизація;
- п. 3.3 Авторизація Користувача через АПС;
- п. 3.4 Реєстрація Користувача через АПС;
- п. 3.12 Робота із переліками, довідниками та класифікаторами;

АБО

- п. 3.1 Авторизація;
- п. 3.3 Авторизація Користувача через КПС;
- п. 3.4 Реєстрація Користувача через КПС;
- п. 3.12 Робота із переліками, довідниками та класифікаторами.

3.6.1. ПС повинна забезпечити передачу в ЦБД ЕСОЗ електронних копій оригіналів документів, за відповідним посиланням, з використанням методу API "PIS. Initialize Person documents upload", завантажувальні файли повинні відповідати наступним вимогам:

1. тип файлу:

- a. ".pdf";
- b. ".jpg";
- c. ".png";
- d. ".bmp";

2. об'єм файлу:

- a. до 20 мб;

3. назва файлу:

- a. може вміщати в себе: від А до Я; Ї І Є в обох регістрах, від 0 до 9;
- b. не може вміщати в себе: ЪЪЭЁыьъё@%&\$^#;

3.6.1.1. у випадку отримання помилки від Системи ПС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок;

3.6.2. ПС має передати електронні копії оригіналів документів пацієнта до Системи з використанням методу API "PIS. Complete Person documents upload".

3.6.2.1. у випадку отримання помилки від Системи ПС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.7. Припинення дії токенів

Передумови:

- Користувач авторизований у ПС та має дійсний Access token

3.7.1. ПС повинна надати Користувачу можливість самостійно ініціювати припинення дії Access token та Refresh token (метод API "Logout");

3.7.1.1. у випадку отримання помилки від Системи ПС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.8. Управління доступами, наданими Користувачем для ПС

Передумови:

- Користувач авторизований у ПІС та має дійсний Access token;
- 3.8.1. ПІС повинна надати Користувачу можливість переглянути перелік ПІС, яким пацієнт надав доступ до інформації про себе (метод API "PIS. Get Approvals (apps)");
- 3.8.1.1. ПІС повинна обов'язково відобразити Користувачу наступні атрибути відповіді методу API "PIS. Get Approvals (apps)":
1. назва клієнта (параметр "client_name");
 2. перелік Скоупів (параметр "scope") відображати "description" відповідно до довідника "SCOPES";
 3. дата створення (параметр "created_at");
- 3.8.1.2. крім обов'язкових атрибутів, Користувач повинен мати можливість переглянути інші параметри, отримані ПІС у відповіді на виклик відповідного методу API.
- 3.8.1.3. у разі отримання помилки Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок;
- 3.8.2. ПІС повинна надати Користувачу можливість (після перегляду переліку ПІС, яким було надано Скоупи) ініціювати припинення доступу, вибраного Користувачем (метод API "PIS. Delete approval (apps)");
- 3.8.2.1. якщо Користувач ініціює відкликання доступу для тієї ПІС, через яку він вчиняє цю дію, ПІС повинна відобразити попередження, що доступ до функціональності Системи через цю ПІС буде припинено. Для продовження роботи буде потрібно повторно авторизуватися. Після підтвердження Користувачем ПІС повинна виконати процедуру виходу з інтерфейсу ("Logout") відповідно до вимог п.3.7;
- 3.8.2.2. якщо було відкликано доступ для іншої ПІС, ПІС повинна оновити та відобразити Користувачеві актуальний перелік ПІС, яким було надано Скоупи (метод API "PIS. Get Approvals (apps)");
- 3.8.2.3. у разі отримання помилки Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.9. Отримання і перегляд даних запису про пацієнта

- 3.9.1. **Загальні вимоги до отримання і перегляду даних запису про пацієнта**
- 3.9.1.1. ПІС повинна забезпечити за запитом Користувача отримання та відображення відомостей про нього, які містяться в Системі, за допомогою методів:
1. "PIS.Get Person details";
 2. "PIS.Get Person authentication methods";
 3. "PIS.Get Person verification details".

3.9.2. Перегляд персональних даних пацієнта

3.9.2.1. ПІС повинна обов'язково відобразити всі наступні атрибути даних пацієнта.

Атрибути даних пацієнта мають бути заповнені даними відповіді Системи (метод API "PIS. Get Person details") за їх наявності а за їх відсутності у відповіді Системи – відображені порожніми, а саме:

3.9.2.1.1. персональні дані:

1. ім'я (параметр "first_name");
2. прізвище (параметр "last_name") ;
3. по батькові (параметр "second_name");
4. дата народження (параметр "birth_date") в форматі "ДД.ММ.РРРР";
5. стать (параметр "gender") значення "value" згідно з довідником "GENDER";
6. країна народження (параметр "birth_country"), значення "value" згідно з довідником "COUNTRY" ;
7. місце народження (параметр "birth_settlement");
8. РНОКПП (параметр "tax_id");
9. інформація про відмову від присвоєння РНОКПП (параметр "no_tax_id");
10. УНЗР (параметр "unzr");
11. кодове слово (параметр "secret");

3.9.2.1.2. адресні дані (масив параметрів "addresses"), а саме:

1. у разі якщо з Системи повернулась інформація про адреси ПІС повинна вивести інформацію з наступною деталізацією:
 - a. тип адреси (параметр "type"), значення "value" з довідника ADDRESS_TYPE;
 - b. країна (параметр "country"), значення "value" згідно з довідником "COUNTRY";
 - c. область (параметр "area");
 - d. район області (параметр "region");
 - e. населений пункт (параметр "settlement");
 - f. тип населеного пункту (параметр "settlement_type"), значення "value" згідно з довідником "SETTLEMENT_TYPE";
 - g. тип вулиці (параметр "street_type"), значення "value" згідно з довідником "STREET_TYPE";
 - h. назва вулиці (параметр "street");
 - i. будинок (параметр "building");
 - j. квартира (параметр "apartment");
 - k. поштовий індекс (параметр "zip");
2. у разі якщо у відповіді Системи не повернулась інформація про адресу фактичного місця проживання (параметр

"type"=RESIDENCE) та Користувач має відповідні дозволи на редагування персональних даних, ПІС має вивести додаткове повідомлення:

Вам необхідно вказати адресу фактичного місця проживання

- 3.9.2.1.3. документи (масив "documents") мають бути згруповані за категоріями "посвідчення особи" та "про набуття цивільної дієздатності" з наступною деталізацією:
1. тип документа (параметр "type");
 2. серію (за наявності) та номер документа (параметр "number");
 3. дата видачі (параметр "issued_at") в форматі "ДД.ММ.РРРР";
 4. дійсний до (параметр "expiration_date") в форматі "ДД.ММ.РРРР";
 5. орган яким виданий (параметр "issued_by");
- 3.9.2.1.4. контактні дані пацієнта, а саме
1. контактний телефон Користувача (масив об'єктів "phones"):
 - a. тип телефону (параметр "type"), згідно з довідником PHONE_TYPE;
 - b. номер телефону (параметр "number");
- 3.9.2.1.5. бажаний спосіб зв'язку (параметр "preferred_way_communication"):
1. електронна пошта (значення "email");
 2. телефон (значення "phone");
- 3.9.2.1.6. дані пацієнта для екстреного зв'язку (об'єкт "emergency_contact"):
1. ім'я (параметр "first_name");
 2. прізвище (параметр "last_name");
 3. по батькові (параметр "second_name");
 4. телефони контакту для екстреного зв'язку (масив об'єктів "emergency_contact.phones"):
 - a. тип телефону (параметр "phones.type");
 - b. номер (параметр "number");
- 3.9.2.2. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.
- 3.9.3. Отримання інформації щодо статусів верифікації пацієнта**
- 3.9.3.1. ПІС повинна за запитом Користувача отримати і відобразити інформацію про його статуси верифікації виключно за визначеними напрямками верифікації відповідно до специфікації Системи (метод API "PIS. Get Person verification details"), а саме виключно:
- 3.9.3.2. статус верифікації пацієнта в ДРФО
1. статус верифікації (параметр details.drfo.verification_status);
 2. причину верифікації (параметр details.drfo.verification_reason);
 3. додаткову інформацію залежно від статусу

a. якщо `"details.drfo.verification_status"` = `"VERIFICATION_NEEDED"`

Ваші персональні дані потребують перевірки в реєстрі Державної податкової служби

b. якщо `"details.drfo.verification_status"` = `"IN_REVIEW"`

Ваші персональні дані в процесі перевірки в реєстрі Державної податкової служби

c. якщо `"details.drfo.verification_status"` = `"VERIFIED"`

Ваші персональні дані підтверджені в реєстрі Державної податкової служби

d. якщо `"details.drfo.verification_status"` = `"VERIFICATION_NOT_NEEDED"`

Ваші персональні дані не потребують верифікації з реєстром Державної податкової служби

e. якщо `"details.drfo.verification_status"` = `"NOT_VERIFIED"`

Зверніть увагу, РНОКПП, дата народження або ПІБ, внесені до системи, не відповідають даним в державному реєстрі Державної податкової служби.

Вам необхідно звірити дані про себе в Реєстрі пацієнтів (ПІБ, дату народження, РНОКПП).

Якщо дані в Реєстрі пацієнтів співпадають з даними у ваших документах - це може означати наявність розбіжностей в реєстрі Державної податкової служби. У такому випадку потрібно звернутися до Державної податкової служби.

У разі невідповідності даних в Реєстрі пацієнтів - необхідно внести зміни та пересвідчитись, що дані в Реєстрі пацієнтів оновлені.

Якщо ви відмовилися від отримання РНОКПП (наявна відмітка в паспорті або довідка) необхідно додатково перевірити та оновити відомості про документ.

3.9.3.3. статус верифікації наявності Актового запису про смерть пацієнта в ДРАЦСГ відображається Користувачу за наявності у відповіді `"details.dracs_death.verification_status"` = `"NOT_VERIFIED"`:

1. статус верифікації (параметр `details.dracs_death.verification_status`);

2. причину верифікації (параметр details.dracs_death.verification_reason);
3. коментар (параметр "details.dracs_death.verification_comment");
4. додаткове повідомлення:

За вашими персональними даними в Державному реєстрі актів цивільного стану громадян знайдено відомості щодо ймовірної реєстрації смерті. Для зміни статусу верифікації зверніться до лікаря, якому подано декларацію або створіть контекстне звернення через портал підтримки НСЗУ за посиланням [url переходу на створення запиту з відповідною категорією].

3.9.3.4. статус верифікації свідоцтва про народження пацієнта в Державному реєстрі актів цивільного стану громадян:

1. статус верифікації (параметр "details.dracs_birth.verification_status");
2. причину верифікації (параметр "details.dracs_birth.verification_reason");
3. коментар, у випадку статусу верифікації "NOT_VERIFIED" (параметр "details.dracs_birth.verification_comment");
4. додаткову інформацію залежно від статусу
 - a. якщо "details.dracs_birth.verification_status" = "VERIFICATION_NEEDED"

Ваші персональні дані потребують перевірки в Державному реєстрі актів цивільного стану громадян

b. якщо "details.dracs_birth.verification_status" = "IN_REVIEW"

Ваші персональні дані в процесі перевірки в Державному реєстрі актів цивільного стану громадян

c. якщо "details.dracs_birth.verification_status" = VERIFIED

Ваші персональні дані підтвержені в Державному реєстрі актів цивільного стану громадян

d. якщо "details.dracs_birth.verification_status" = NOT_VERIFIED

Ваші ПІБ, дата народження, серія та номер свідоцтва про народження не відповідають даним в Державному реєстрі актів цивільного стану громадян.

Необхідно перевірити актуальність даних. У разі неспівпадіння даних в Реєстрі пацієнтів та документах – необхідно внести зміни в запис про пацієнта.

У разі співпадіння ваших даних в Реєстрі пацієнтів з

даними документів – є розбіжності в Державному реєстрі актів цивільного стану громадян.

Щодо оновлення даних в Реєстрі пацієнтів (звернувшись до вашого сімейного лікаря чи Національної служби здоров'я України) чи Державного реєстру актів цивільного стану громадян звертаються ваші батьки (законні представники).

- 3.9.3.4.1. статус верифікації свідоцтва про народження пацієнта в ДРАЦСГ не повинен відображатись якщо:
- a. "details.dracs_birth_verification_status" = "VERIFICATION_NOT_NEEDED");
 - b. користувачу на момент отримання статусу виповнилось <person_full_legal_capacity_age> років;
- 3.9.3.5. статус ручної верифікації співробітником НСЗУ
1. статус верифікації (параметр "details.nhs_verification_status");
 2. причину верифікації (параметр "details.nhs_verification_reason");
 3. додаткову інформацію залежно від статусу
 - a. якщо "details.nhs_verification_status" = "VERIFICATION_NEEDED"

Ваші персональні дані потребують перевірки Національною службою здоров'я України
 - b. якщо "details.nhs_verification_status" = "VERIFICATION_NOT_NEEDED"

Ваші персональні дані не потребують перевірки Національною службою здоров'я України
 - c. якщо "details.nhs_verification_status" = "IN_REVIEW"

Ваші персональні дані перевіряються Національною службою здоров'я України
 - d. якщо "details.nhs_verification_status" = "VERIFIED"

Ваші персональні дані успішно перевірені Національною службою здоров'я України
 - e. якщо "details.nhs_verification_status" = "NOT_VERIFIED" та "person_verification_details.nhs_verification_reason" не "DOCUMENTS_TRIGGERED"

Ваші персональні дані не верифіковано працівником

Національної служби здоров'я України по причині –
{details.nhs.verification_comment}.

f. якщо "details.nhs.verification_status" = "NOT_VERIFIED" та
"person_verification.details.nhs.verification_reason" =
"DOCUMENTS_TRIGGERED",

- ПІС повинна забезпечити можливість передати в ЦБД
ЕСОЗ електронні копії оригіналів документів,
відповідно до вимог п.3.6

- КПІС повинна відобразити користувачу повідомлення

Завантажте копії ваших документів. До завантаження
документів можливості особистого кабінету пацієнта
будуть обмежені.

- АПІС у разі неможливості передачі електронних копій
оригіналів документів повинна скерувати Користувача
(з можливістю перейти до його використання) на
електронний кабінет пацієнта ЦБД ЕСОЗ

3.9.3.6. статус верифікації УНЗР

1. статус верифікації (параметр "details.unzr.verification_status");

2. причину статусу верифікації (параметр
"details.unzr.verification_reason");

3. додаткову інформацію залежно від статусу:

a. якщо "details.unzr.verification_status" =
"VERIFICATION NEEDED"

Ваші персональні дані потребують перевірки в Єдиному
державному демографічному реєстрі

b. якщо "details.unzr.verification_status" =
"VERIFICATION NOT NEEDED"

Ваші персональні дані не потребують перевірки в Єдиному
державному демографічному реєстрі

c. якщо "details.unzr.verification_status" = "IN_REVIEW"

Ваші персональні дані в процесі перевірки в Єдиному
державному демографічному реєстрі

d. якщо "details.unzr.verification_status" = "VERIFIED"

Ваші персональні дані підтвержені в Єдиному державному

демографічному реєстрі

e. якщо "details.unzr.verification_status" = "NOT VERIFIED"

Відомості про унікальний номер запису в реєстрі (УНЗР) не відповідають даним в Єдиному державному демографічному реєстрі.

Перевірте відомості про ПІБ та дату народження в Реєстрі пацієнтів та додайте відомості про УНЗР з свідоцтва про народження, ID-картки або закордонного паспорта. Якщо ви оновили дані, але після їх перевірки Системою вони знову не верифіковані – зверніться до Державної міграційної служби України для уточнення своїх даних в ЄДДР.

Якщо у вас немає УНЗР, а відомості про нього були внесені до Реєстру пацієнтів помилково – оновіть дані, залишивши УНЗР порожнім.

3.9.3.7. статус верифікації дійсності паспорта в ДМС

1. статус верифікації (параметр "details.dms_passport.verification_status");
2. причину статусу верифікації (параметр "details.dms_passport.verification_reason");
3. додаткову інформацію, залежно від статусу:
 - a. якщо "details.dms_passport.verification_status" = "VERIFICATION NEEDED"

Зазначений в Реєстрі пацієнтів паспорт потребує перевірки в Державній міграційній службі

- b. якщо "details.dms_passport.verification_status" = "VERIFICATION NOT NEEDED"

У вас відсутні документи для перевірки в Державній міграційній службі

c. якщо "details.dms_passport.verification_status" = "IN REVIEW"

Зазначений в Реєстрі пацієнтів паспорт в процесі перевірки в Державній міграційній службі

d. якщо "details.dms_passport.verification_status" = "VERIFIED"

Зазначений в Реєстрі пацієнтів паспорт дійсний за даними Державної міграційної служби

е. якщо `"details.dms_passport_verification_status"` = `"NOT_VERIFIED"`

Зазначений в Реєстрі пацієнтів паспорт – недійсний за даними Державної міграційної служби

Звірте дані Реєстру пацієнтів з дійсним паспортом. У разі неспівпадіння даних в Реєстрі пацієнтів та документах – оновіть дані. Якщо помилки відсутні – зверніться до Державної міграційної служби України.

- 3.9.3.8. загальний статус пацієнта (параметр `"verification_status"`) не відображається в інтерфейсі ПІС;
- 3.9.3.9. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.9.4. Отримання інформації щодо методів автентифікації

- 3.9.4.1. ПІС повинна за запитом Користувача отримати і відобразити інформацію про його методи автентифікації отриманні від Системи (метод API `"PIS.Get Person authentication methods"`), а саме:
 1. тип (параметр `"type"`);
 2. номеру телефону для автентифікації (параметр `"phone_number"`) - обов'язково для методу автентифікації ("ОТР");
 3. назви методу автентифікації, за яким пацієнт може ідентифікувати метод авторизації (параметр `"alias"`) - за наявності для методу автентифікації ("ОТР");
 4. дата введення в дію методу автентифікації (параметр `"started_at"`) - за наявності;
 5. ПІС повинен надати можливість вивести інші відомості про пацієнта, отриманих у відповіді API, за запитом Користувача.
- 3.9.4.2. у разі, якщо з Системи не повертається інформація про активні методи автентифікації (у пацієнта відсутні або скинуті методи автентифікації), та Користувач має відповідні дозволи на редагування персональних даних Користувачу необхідно відобразити повідомлення:

Необхідно внести новий метод автентифікації! Це допоможе забезпечити зручність отримання електронних медичних сервісів та вищий контроль Вами доступу до інформації про Вас.

- 3.9.4.3. у разі якщо у Користувача наявний метод автентифікації з типом "OFFLINE" - необхідно відобразити повідомлення:

Додайте новий метод автентифікації з використанням номеру телефону.
 Це допоможе забезпечити зручність отримання електронних медичних сервісів та вищий контроль Вами доступу до інформації про Вас.

- 3.9.4.4. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.10. Зміна персональних даних пацієнта

3.10.1. Загальні вимоги по зміні персональних даних

- 3.10.1.1. ПІС має надати можливість Користувачу оновлювати свої дані у разі необхідності внесення змін (метод API "PIS. Initialize Update Person details" або "TRUSTED PIS. Initialize Update Person details"), окрім:
1. РНОКПП, якщо він був заповнений раніше;
 2. УНЗР, з урахуванням наступних особливостей:
 - a. КПІС не повинна надавати можливість оновлювати значення, якщо воно було заповнено раніше;
 - b. АПІС має надавати можливість оновлювати значення за умови неможливості його редагування Користувачем;
- 3.10.1.2. у разі якщо відповідь API "PIS. Initialize Update Person details" містить відповідне посилання (параметр "urgent.url") ПІС повинна забезпечити передачу Користувачем електронних копій оригіналів документів з урахуванням вимог п.3.6;
- 3.10.1.2.1. у разі неможливості передачі електронних копій оригіналів документів АПІС повинна скерувати Користувача (з можливістю перейти до його використання) на електронний кабінет пацієнта ЦБД ЕСОЗ;
- 3.10.1.3. ПІС має забезпечити можливість завантаження електронних копій оригіналів документів відповідно до типу документу, отриманого у відповіді API "PIS. Initialize Update Person details" (масив "person.documents") для кожного отриманого посилання (параметр "urgent.url") відповідно до вимог п.3.6.1;
- 3.10.1.3.1. ПІС має забезпечити передачу даних документу, що вимагаються конфігурацією "PIS_PERSON_LEGAL_CAPACITY_DOCUMENT_TYPES" для Користувачів з віком де глобальний параметр дорівнює "no_self_registration_age", але менший за глобальний параметр "person_full_legal_capacity_age";

- 3.10.1.4. у разі якщо Користувач підтверджує внесені зміни, ПІС повинен надати можливість Користувачу підписати дані запиту на зміну персональних даних, за допомогою ЕП;
- 3.10.1.5. перед підписанням даних запиту на зміну персональних даних ПІС повинен, за умови наявності Запиту на реєстрацію запису про Декларацію в статусі "NEW" або "APPROVED", вивести Користувачу попереджувальне повідомлення:

Після збереження змінених персональних даних, наявні Запити на реєстрацію запису про Декларацію будуть анульовані. Подана Декларація залишиться чинною.

- 3.10.1.6. після підписання Користувачем змінених даних за допомогою ЕП, ПІС повинна виконати запит API "PIS. Complete Update Person details", передавши повний набір змінених даних із накладеним ЕП;
 - 3.10.1.6.1. у разі відсутності помилок ПІС має вивести повідомлення про успішну зміну персональних даних Користувача;
 - 3.10.1.6.2. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.
- 3.10.1.7. у разі якщо процес зміни персональних даних був перерваний, ПІС повинен надати можливість Користувачу відновити процес з того етапу, на якому сталося переривання, за умови що запит на зміну персональних даних вже був успішно переданий на момент переривання. Для цього ПІС повинна:
 - 3.10.1.7.1. отримати незавершений (статус "NEW") запит на зміну персональних даних з використанням методу "PIS. Get Person request list";
 - 3.10.1.7.2. отримати його деталі з використанням методу "PIS. Get Person request details";
 - 3.10.1.7.3. якщо переривання відбулося до завантаження документів - надати можливість дозавантаження документів із значенням "is_uploaded" = "false" (метод API "PIS. Get Person request details");
 - 3.10.1.7.4. надати можливість Користувачу переглянути раніше внесені дані в інтерфейсі ПІС в рамках процесу;
 - 3.10.1.7.5. надати можливість продовжити процес відповідно до п.3.10.1.1.

3.10.2. Запити на зміну персональних даних

- 3.10.2.1. ПІС повинна забезпечити можливість Користувачу переглянути список запитів на зміну персональних даних (метод API "PIS. Get Person request list"), а саме
 1. статус (параметр "status");
 2. хто вніс зміни (параметр "channel");

3. дата створення запиту на зміну (параметр "inserted_at") в форматі "ДД.ММ.РРРР";
4. ПІС повинен надати можливість вивести інші відомості про пацієнта, отриманих у відповіді API, за запитом Користувача;
- 3.10.2.2. ПІС повинна забезпечити можливість Користувачу переглянути деталі кожного окремого запиту (метод API "PIS. Get Person request details");
 - 3.10.2.2.1. ПІС повинна забезпечити можливість Користувачу переглянути електронну форму (параметр "content") за умови, що у відповіді методу API "PIS. Get Person request list" на попередньому кроці повернулись дані Користувача (параметр "person").
- 3.10.2.3. ПІС повинна надати можливість Користувачу скасовувати запит на зміну персональних даних у статусі "NEW" або "APPROVED" (метод API "PIS. Reject Person request").
- 3.10.2.4. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.10.3. Реєстрація методу автентифікації

Передумови:

- ПІС повинна забезпечити Користувачу можливість отримати перелік методів автентифікації згідно з вимогами п.3.9.4;
- 3.10.3.1. ПІС не повинна надавати можливість створити метод автентифікації іншого типу окрім "OTP";
 - 3.10.3.2. ПІС повинна надати можливість Користувачу створити (метод API "PIS. Create Person authentication method request") метод автентифікації з типом "OTP", шляхом заповнення Користувачем:
 1. номеру телефону (в форматі визначеному в Специфікації);
 2. назву методу автентифікації, за яким пацієнт може ідентифікувати метод авторизації ("alias");
 - 3.10.3.3. у разі, якщо за результатами виконання запиту до Системи верифікація номера телефону не потрібна, ПІС має повідомити Користувача про успішне створення методу автентифікації;
 - 3.10.3.4. у разі, якщо за результатами виконання запиту до Системи верифікація номера телефону потрібна, ПІС повинна відобразити Користувачу поле для введення одноразового пароля (в форматі визначеному в Специфікації);
 - 3.10.3.4.1. у разі якщо Користувач не отримав верифікаційний код або термін його дії вичерпано, ПІС повинна забезпечити можливість Користувачу повторно отримати верифікаційний код (метод API "PIS. Resend authorization OTP for authentication method request");
 - 3.10.3.5. ПІС повинна надати Користувачу можливість підтвердити запит на створення методу автентифікації в передачею верифікаційного коду (метод API "PIS. Approve Person authentication method request");

- 3.10.3.5.1. якщо метод автентифікації створено, ПІС має повідомити Користувача про успішне створення методу автентифікації;
- 3.10.3.5.2. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.10.4. Оновлення методу автентифікації

Передумови:

- ПІС повинна забезпечити Користувачу можливість отримати перелік методів автентифікації згідно з вимогами п.3.9.4;

- 3.10.4.1. у разі якщо у Користувача наявний активний метод автентифікації з типом "ОТР", ПІС повинна забезпечити можливість оновлення назви методу автентифікації, за яким пацієнт може ідентифікувати метод авторизації (параметр "alias") (метод API "PIS. Update Person authentication method");
 - 3.10.4.1.1. якщо метод автентифікації оновлено, ПІС має відобразити Користувачу оновлені відомості про метод автентифікації (нове значення параметра "alias");
 - 3.10.4.1.2. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.11. Управління Деклараціями

3.11.1. Подання Декларації

- 3.11.1.1. ПІС повинна надати Користувачу можливість ініціювати процес подання Декларації незалежно від наявності поданої раніше Декларації;
- 3.11.1.2. Для можливості створити Запит на реєстрацію запису про Декларацію ПІС, на основі відомостей реєстрів Системи, отриманих згідно вимог п.3.12, повинна надати Користувачу зокрема, але не виключно, наступні варіанти (фільтри) пошуку надавача медичних послуг та лікаря:
 1. ПІБ лікаря (параметр "first_name", параметр "last_name", параметр "second_name");
 2. спеціальністю лікаря (параметр "speciality");
 3. статтю лікаря (параметр "gender");
 4. ознакою досягнення ліміту кількості Декларацій у лікаря;
 5. назвою СГуСОЗ (параметр "legal_entity.name");
 6. назвою МНП (параметр "name");
 7. адресою МНП (параметр "addresses");
 8. ознакою наявності або відсутності МНП у договорі СГуСОЗ щодо надання послуг за ПМГ.

- 3.11.1.3. в результаті пошуку Користувач має мати змогу ознайомитись зокрема з наступною інформацією:
1. назва СГуСОЗ (параметр "legal_entity.name")
 2. назва МНП (параметр "name");
 3. адреса МНП (параметр "addresses");
 4. ПІБ лікаря(параметр "first_name", параметр "last_name", параметр "second_name");
 5. спеціальність (параметр "speciality");
 6. кількість поданих Декларацій (параметр "declarations_count");
 - а. у разі перевищення ліміту Декларацій ("declarations_limit"- "declarations_count"<=0) ПІС має відобразити інформацію про це Користувачу;
 7. ознакою наявності або відсутності МНП у договорі СГуСОЗ щодо надання послуг за ПМГ;
- 3.11.1.3.1. у разі вибору Користувачем в результатах пошуку СГуСОЗ, ПІС повинна відобразити перелік МНП цього СГуСОЗ;
- 3.11.1.3.2. у разі вибору Користувачем в результатах пошуку МНП, ПІС повинна відобразити перелік лікарів, що є співробітниками даного МНП;
- 3.11.1.4. ПІС повинна відображати Користувачу тільки лікарів, основна спеціальність (параметр "speciality" за умови "speciality_officio"="true") яких:
1. "FAMILY DOCTOR";
 2. "THERAPIST" - для пацієнтів, вік яких більший або дорівнює 18 рокам (значення конфігураційного параметру "adult_age" відповідно специфікації Системи);
 3. "PEDIATRICIAN" - для пацієнтів, молодших за 18 років (значення конфігураційного параметру "adult_age" відповідно специфікації Системи);
- 3.11.1.5. ПІС повинна надавати Користувачу можливість переглянути такі дані про лікаря:
1. ПІБ (параметри "first_name", "last_name", "second_name" за наявності);
 2. стать (параметр "gender") значення "value" згідно з довідником "GENDER";
 3. спеціальності (параметр "specialities") значення "value" згідно з довідником "SPECIALITY_TYPE";
 4. вік (розрахункове значення на основі параметру "year_of_birth");
 5. освітні дані, а саме:
 - а. ступінь (параметр "educations.degree") - значення "value" згідно з довідником "EDUCATION_DEGREE";
 - б. спеціальність (параметр "educations.speciality") - значення "value" згідно з довідником "SPECIALITY_TYPE";
 6. кваліфікації, а саме:

- a. тип (параметр "qualifications.type") - значення "value" згідно з довідником "QUALIFICATION_TYPE";
 - b. спеціальність (параметр "qualifications.speciality") - значення "value" згідно з довідником "SPECIALITY_TYPE";
7. ПІС повинен надати можливість вивести інші відомості про лікаря, отриманих у відповіді API, за запитом Користувача.
- 3.11.1.6. при виборі Користувачем лікаря, у якого перевищено ліміт поданих Декларацій, ПІС має вивести попереджувальне повідомлення про перевищення ліміту та потребу очікування погодження такого Запиту лікарем (не більше ніж 7 календарних днів) та ймовірність її відхилення;
- 3.11.1.7. при відсутності обраного Користувачем МНП у договорі СГуСОЗ щодо надання послуг за ПМГ, ПІС має вивести попереджувальне повідомлення:

Щоб отримувати медичні послуги безоплатно за Програмою медичних гарантій, оберіть заклад, який має договір з НСЗУ.

Обраний вами медичний заклад не має договору з НСЗУ або це місце надання послуг не входить до такого договору. Через це держава не зможе оплачувати надані вам послуги первинної медичної допомоги за декларацією.

Радимо сконтактувати з закладом та уточнити, чи можна подати декларацію саме тут.

- 3.11.1.8. після заповнення Запиту на реєстрацію запису про Декларацію ПІС повинна дозволити Користувачу передати дані до Системи (метод API "PIS. Create Declaration Request");
- 3.11.1.8.1. у разі успішності виконання запиту ПІС повинна відобразити Користувачу заповнену Системою форму Декларації, отриману у відповіді (параметр "content");
 - 3.11.1.8.2. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.
- 3.11.1.9. Користувач повинен мати можливість підписати за допомогою ЕП дані, повернуті для підпису Системою у відповіді методу API "PIS. Create Declaration Request", без переходу на зовнішні ресурси, з можливістю використання інтегрованих засобів підпису за виключенням, якщо такий перехід необхідний для використання ЕП, який використовується Користувачем. Для передавання підписаних даних ПІС повинна використовувати метод API "PIS. Sign Declaration request";

- 3.11.1.10. ПІС повинен виводити попереджувальне повідомлення перед підписанням Декларації якщо до ліміту Декларацій лікаря залишається менше 20 ($0 < \text{"declarations_limit"} - \text{"declarations_count"} < 20$);
- 3.11.1.11. ПІС має проінформувати Користувача про результат виконання запиту методу API "PIS. Sign Declaration request" залежно від статусу, який отримує запит;
- 3.11.1.11.1. у випадку, коли запит отримує статус "Підтверджений" ("APPROVED"), ПІС повинна відобразити Користувачу повідомлення:
- Обраний Вами лікар вже має рекомендовану кількість пацієнтів.
Ми надіслали лікарю Вашу декларацію на погодження. Це займе до 7 календарних днів.
- 3.11.1.11.2. у випадку, коли запит отримує статус "Підписаний" ("SIGNED"), ПІС повинна зчитати зміну статусу запиту на подання Декларації відобразити Користувачу повідомлення:
- Вітаємо з вибором лікаря!
Декларацію № {declaration_number} лікарю {ПІБ лікаря} успішно подано.
- 3.11.1.12. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.
- 3.11.1.13. у разі якщо процес створення Запиту на реєстрацію запису про Декларацію був перерваний, ПІС повинна надати можливість Користувачу відновити процес з того етапу, на якому сталося переривання, за умови що запит вже був успішно переданий на момент переривання. Для цього ПІС повинна:
- 3.11.1.13.1. отримати незавершений (статус "NEW") Запит на реєстрацію запису про Декларацію з використанням методу "PIS. Get Declaration requests";
- 3.11.1.13.2. отримати його деталі з використанням методу "PIS. Get Declaration request details";
- 3.11.1.13.3. надати можливість Користувачу переглянути форму Декларації згідно специфікації Системи, з можливістю завантаження у PDF форматі (*.pdf);
- 3.11.1.13.4. надати можливість виконати дії пп.3.11.1.7-3.11.1.11.

3.11.2. Отримання та перегляд Запитів на реєстрацію запису про Декларацію

- 3.11.2.1. ПІС повинна отримати і відобразити Користувачу перелік поданих ним Запитів на реєстрацію запису про Декларацію (метод API Системи "PIS. Get Declaration requests"). Атрибути відповіді методу API "PIS. Get Declaration requests", які повинні бути відображені ПІС:
1. статус (параметр "status");
 2. номер Декларації (параметр "declaration_number");
 3. ПІС повинен надати можливість вивести інші відомості про пацієнта, отриманих у відповіді API, за запитом Користувача.
- 3.11.2.2. Користувач повинен мати можливість переглянути деталі вибраного Запиту на реєстрацію запису про Декларацію (метод API "PIS. Get Declaration request details");
- 3.11.2.2.1. для перегляду деталей вибраного запиту, ПІС повинна дати можливість Користувачу отримати електронну форму Декларації згідно специфікації Системи (параметр "content"), з можливістю завантаження у PDF форматі (*.pdf), за умови, що у відповіді методу API "PIS. Get Declaration requests" повернулись дані Користувача (параметр "person");
- 3.11.2.3. Користувач після отримання попередження про незворотність дії, повинен мати можливість відхилити Запит на реєстрацію запису про Декларацію, що знаходиться у статусі "NEW" або "APPROVED" (метод API "PIS. Reject Declaration request");
- 3.11.2.4. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.11.3. Перегляд Декларацій

- 3.11.3.1. ПІС повинна отримати і відобразити Користувачу перелік поданих поданим ним Декларацій (метод API "PIS. Get declarations"), а саме:
- 3.11.3.1.1. атрибути відповіді методу API "PIS. Get Declarations", які обов'язково повинні бути відображені ПІС:
1. статус (параметр "status");
 2. номер Декларації (параметр "declaration_number");
 3. дійсна з (параметр "start_date");
- 3.11.3.1.2. у разі якщо статус Декларація неактивна (статус не відповідає "ACTIVE") додатково мають бути відображені:
1. дійсна до (параметр "updated_at");
 2. причина зміни статусу (параметр "reason");
 3. опис причини зміни статусу (параметр "reason_description");
- 3.11.3.2. ПІС повинна забезпечити відображення Декларацій за статусом ("status") в окремих блоках:
1. Декларація у статусі "ACTIVE";
 2. Декларації в усіх інших статусах;

- 3.11.3.2.1. у випадку відсутності Декларації у статусі "ACTIVE", ПІС повинна запропонувати Користувачу подати Декларацію.
- 3.11.3.3. ПІС повинна надати Користувачу можливість отримати детальну інформацію про Декларацію (метод API "PIS. Get Declaration details") у вигляді електронної форми відповідно до специфікації Системи (параметр "content"), яка була підписана, з можливістю завантаження у PDF форматі (*.pdf).
- 3.11.3.4. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.11.4. Припинення Декларації

- 3.11.4.1. ПІС повинна надавати Користувач можливість розірвати Декларацію тільки в статусі "active";
- 3.11.4.2. ПІС повинна надати Користувачу можливість внести причину припинення Декларації ("reason_description");
- 3.11.4.3. перед підтвердженням припинення Декларації, ПІС має відобразити інформаційне повідомлення з можливістю підтвердити або скасувати дію припинення:

Увага!

Припинення дії Декларації є незворотною дією. Ви впевнені?

- 3.11.4.4. у разі підтвердження виконання операції Користувачем, ПІС виконує запит на припинення Декларації (метод API "PIS. Terminate declaration");
- 3.11.4.5. у разі відміни виконання операції Користувач повертається до попереднього етапу;
- 3.11.4.6. у випадку отримання помилки від Системи ПІС повинна обробити помилку згідно з Додатком 1. Таблиця обробки помилок.

3.12. Робота із переліками, довідниками та класифікаторами

3.12.1. Загальні вимоги до отримання довідників та відомостей реєстрів

- 3.12.1.1. ПІС повинна забезпечити Користувачу відображення актуальних значень довідників та класифікаторів Системи, для можливості використання Користувачем, шляхом їх отримання не частіше ніж 1 раз на 4 години та не рідше ніж 1 раз на добу (метод API "Get dictionaries v2");

3.12.2. Вимоги до отримання переліків з реєстрів Системи

- 3.12.2.1. ПІС повинна забезпечити оновлення актуальних переліків з реєстрів Системи для можливості використання Користувачем не частіше ніж 1 раз на 4 години та не рідше ніж 1 раз на добу згідно відповідних методів API.

- 3.12.2.2. Отримання реєстрової інформації про лікарів
 - 3.12.2.2.1. для отримання медичних спеціалістів ("parties"), що зареєстровані в Системі та мають активний запис про медичного працівника з типом "DOCTOR", з метою надання відомостей Користувачу для подання Декларації, ПІС повинна використовувати метод API "Get parties (Bulk data export)";
 - 3.12.2.2.2. для отримання всіх працівників ("employees"), що зареєстровані в Системі та мають активний запис про медичного працівника з типом "DOCTOR") з метою надання відомостей Користувачу для подання Декларації, ПІС повинна використовувати метод API "Get employees (Bulk data export)".
 - 3.12.2.2.3. для отримання всіх ролей співробітників ("employee roles") що зареєстровані в Системі та мають активний запис про медичного працівника з типом "DOCTOR" з метою надання відомостей Користувачу для подання Декларації, ПІС повинна використовувати метод API "Get employee roles (Bulk data export)".
- 3.12.2.3. Отримання реєстрової інформації про МНП
 - 3.12.2.3.1. для отримання всіх МНП ("divisions") СГуСОЗ з Системи, ПІС повинна використовувати метод API "Get divisions (Bulk data export)".
- 3.12.2.4. Отримання реєстрової інформації про СГуСОЗ
 - 3.12.2.4.1. для отримання всіх СГуСОЗ ("legal_entities") з Системи, ПІС повинна використовувати метод API "Get legal entities (Bulk data export)".
- 3.12.2.5. Отримання реєстрової інформації про медичні послуги
 - 3.12.2.5.1. для отримання всіх медичних послуг ("healthcare services") з Системи, ПІС повинна використовувати метод API "Get healthcare services (Bulk data export)".
- 3.12.2.6. Отримання інформації, щодо обсягу Декларацій лікаря
 - 3.12.2.6.1. для отримання кількості поданих Декларацій та рекомендованого обсягу практики для такого спеціаліста, використовується метод API "Get declarations limit and declarations count per practitioner".
- 3.12.2.7. Отримання інформації про наявність МНП у договорі СГуСОЗ щодо надання послуг за ПМГ
 - 3.12.2.7.1. для отримання переліку МНП, що включені до договору з НСЗУ і супутньої інформації щодо договорів, використовується метод API "Contract Divisions (Bulk export)".
- 3.12.3. **Вимоги до отримання інформації з адресного компоненту Системи**
 - 3.12.3.1. ПІС повинна забезпечити оновлення актуальних даних інформації з адресного компоненту Системи для можливості використання Користувачем не частіше ніж 1 раз на 4 години та не рідше ніж 1 раз на добу згідно відповідних методів API;

- 3.12.3.2. для отримання переліку областей відповідно до параметрів пошуку, ПІС повинна використовувати метод API "List of Regions By Search Params";
- 3.12.3.3. для отримання переліку районів, які входять в область, ПІС повинна використовувати метод API "Districts by Region";
- 3.12.3.4. для отримання переліку населених пунктів, ПІС повинна:
 - 3.12.3.4.1. використовувати метод API "Settlements by districts" для отримання переліку населених пунктів які входять до району;
 - 3.12.3.4.2. використовувати метод API "List of Cities By Search Params" для отримання переліку населених пунктів відповідно до параметрів пошуку;
- 3.12.3.5. для отримання переліку вулиць, відповідно до параметрів пошуку, ПІС може використовувати метод API "List of Streets by Search Params".

Директор
електронної системи охорони здоров'я

департаменту

розвитку
Дмитро ЧЕРНИШ