Технічні науки

УДК 004.62:006.86

**Гулін Іван Леонідович**

*студент*

*Національного технічного університету України*

*«Київський політехнічний інститут імені Ігоря Сікорського»*

# ЕЛЕКТРОНІ МЕДИЧНІ ЗАПИСИ ТА ДЕЦЕНТРАЛІЗАЦІЯ

***Анотація.*** *В статті розглянуті розповсюдженні медичні стандарти збереження, передачі, управління медичної інформації та даних, що пов'язані з охороною здоров'я у програмному забезпеченні, їх переваги та недоліки над паперовими документами, а також перспективи розвитку.*

***Ключові слова:*** *електронний медичний запис, медичні стандарти, безпека, self-sovereign identity.*

**Актуальність теми.** Електронний медичний запис (EHR) - це систематизована колекція медичної інформації пацієнтів, що зберігається у цифровому форматі. Ці записи можна спільно використовувати в різних установах охорони здоров'я. Записи поділяються через мережеві, корпоративні інформаційні системи або інші інформаційні мережі. EHR можуть включати в себе цілий ряд даних, включаючи демографічні дані, історію хвороби, медикаменти та алергію, стан імунізації, результати лабораторних випробувань, рентгенологічні зображення, життєво-важливі ознаки, особисту статистику, такі як вік і вага, та платіжну інформацію [1].

Найпопулярніші стандарти EHR:

Digital Imaging and Communications in Medicine (DICOM) - міжнародний стандарт для представлення та передачі медичних зображень.

ISO - ISO TC 215 надає міжнародні технічні специфікації для EHR.

ISO 18308 описує архітектуру EHR.

Health Level 7 (HL7) – набір міжнародних стандартів для передачі клінічних та адміністративних даних між програмними додатками, що використовуються різними медичними працівниками.

openEHR - це специфікація відкритого стандарту, яка описує управління та зберігання, пошук і обмін медичними даними в електронних медичних документах.

Більш універсальні стандарти, такі як HL7, визначають деяку функціональність, яка допоможе лікарям ефективніше працювати. Деякі з цих функцій включають, але не обмежуються:

- Визначення та інтеграція медичного запису пацієнта.
- Статистика по демографії - збір та підтримка демографічної інформації. Там, де це доречно, дані повинні бути клінічно релевантними, підлягати звітуванню та відстежуватися з плином часу.
- Керування списками проблем – створення та підтримка списків проблем, що стосуються пацієнтів.
- Керування списками медикаментів – створення та підтримка списків медичних препаратів для пацієнтів.
- Керування історією хворого – збір, перегляд та керування медичною, хірургічною, соціальною та сімейною історією, включаючи збір позитивних і негативних історій, повідомлених пацієнтом або наявних у пацієнта в історії хвороби.
- Керування клінічними документами та примітками – створення, додавання, виправляння, аутентифікація та закривання, за потребою, переписану або безпосередньо введену клінічну документацію та примітки.
- Включення клінічної документації з зовнішніх джерел.
- Керування планами догляду за пацієнтами.

- Створення та запис інструкцій для пацієнта.

Створені, у тому числі, як сучасна альтернатива паперовим документам у медичному документообігу, електроні медичні записи мають підвищену прозорість, портативність і доступність, що збільшує легкість використання медичними працівниками даних. Однак, це також полегшує викрадання інформації несанкціонованими особами або недобросовісними користувачами, що призвело до підвищення вимог безпеки до електронних медичних записів, у країнах, де даний вид документообігу є поширеним. Також існує проблема порушень у конфіденційних записах. Занепокоєння з приводу безпеки сприяє тому, що розвиток електронних медичних записів значно сповільнюється.

З іншого боку, рукописні медичні записи можуть бути погано розбірливими, що може сприяти медичним помилкам, а електронні записи можуть допомогти у стандартизації форм, термінології та введення даних. Оцифрування форм полегшує збір даних для епідеміології та клінічних досліджень. Однак стандартизація може створити деякі виклики для місцевої практики [2].

З вищевказаного очевидно, що найбільшим недоліком електронних медичних записів є безпека перед несанкціонованим доступом до особистої інформації пацієнтів. Першопричиною цього можна вважати фактор централізованості даних. З розвитком нових технологій можливо забезпечити розбиття доступу до даних, кожен випадок до відповідної людини, що має право отримати якийсь об'єм інформації. Розвиток децентралізованих систем зберігання даних був спричинений тими самими занепокоєннями у сенсі зловживаннями окремих компаній особистими данин користувачів, які були їм довірені, за вимогами особистостей централізованих систем.

Принцип self-sovereign identity є наслідком розвитку технологій та прагненням спроектувати особисту свободу у цифровому розрізі. Self-

sovereign identity дозволяє довіреним лицям створювати шаблони за допомогою яких користувачі можуть отримувати дані з довірених лиць та демонструвати ці ж дані для отримання іншої інформації (як приклад людина отримує диплом, використовуючи якого отримує роботу як доказ кваліфікації, з роботи отримує довідки платоспроможності, після чого можна отримати кредит в банку тощо).

Якщо казати про self-sovereign identity, то ще немає консенсусу щодо точного визначення цього. Поки що використовують термінологію SSI, як концепцію індивідуумів або організацій, які мають єдине право власності на свої цифрові та аналогові ідентичності, і контролюють, яким чином їхні особисті дані є спільними та використовуються. Це додає рівень безпеки та гнучкості, що дозволяє власникові ідентифікації лише розкривати необхідні дані для будь-якої операції або взаємодії. Оскільки ідентифікація є центральною частиною суспільства, необхідно гарантувати, що користувальницький контроль буде основною основою для створення SSI [3].

Згідно з моделлю самоврядування, особи та організації (власники), які мають один або більше ідентифікаторів (що дозволяє виявити та ідентифікувати суб'єкта), можуть пред'явити претензії, що стосуються цих ідентифікаторів, без необхідності проходити через посередника. Як наслідок, найкращим способом реалізації системи з самостійною ідентичністю буде технологія blockchain, де немає необхідності в посередництві.

Подібно до Інтернету, наша інформація про здоров'я також поширюється в різних силосах. Self Sovereign Identity прагне зробити людей власниками всієї особистої медичної інформації, щоб мати можливість вибирати, кому надати подальший доступ і дозволяючи мати доступ до власної інформації, коли це буде потрібно. У майбутньому це повинно дозволити лікареві або лікарні отримати доступ до користувацьких даних,

коли користувач захоче цього. Цей метод може навіть бути використаний для допомоги у розробці нових лікарських засобів, не ставлячи під загрозу нашу конфіденційність. Смарт-годинники могли б виміряти наш пульс і кров'яний тиск в режимі реального часу, і ми могли б вирішити пожертвувати або продавати цю інформацію в наукових цілях або в обмін на продукти та послуги.

**Література**

1. The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions [Електроний ресурс] / Tracy D. Gunter, Nicolas P. Terry // *2005*. – Режим доступу: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1550638/
2. To Err Is Human: Building a Safer Health System / Linda T. Kohn, Janet M. Corrigan, Molla S. Donaldson // 1999. – С. 177-194.
3. The Inevitable Rise of Self-Sovereign Identity – A white paper from the Sovrin Foundation [Електронний ресурс] / Andrew Tobin, Drummond Reed, Phillip J. Windsley // 2017. – С. 7. – Режим доступу: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf