

Для того, щоб бути впевненими в безпеці власних даних, пацієнти мають право знати, які та скільки даних збираються, з якою метою та як вони будуть використовуватися. Саме тому правила конфіденційності мають бути добре пояснені, формалізовані, а потім поширені між усіма залученими сторонами. Розміщення даних (марне об'єктне сховище) є ще одним фактором, що впливає на конфіденційність інформації про пацієнтів.

Існує багато засобів, якими постачальники медичних послуг можуть гарантувати, що захищена інформація про здоров'я пацієнта залишається належним чином захищеною, особливо щодо електронного зберігання та передачі даних про стан пацієнта. Стандартні процедури включають маскуванню даних (заміна значень конфіденційних даних зміненими значеннями, які, незважаючи на це, зберігають корисність набору даних як довідкового джерела), шифрування (еквівалент блокування даних у сховищі та запобігання доступу до них без необхідного цифрового ключа чи сертифіката) та деідентифікацію. Шифрування є більш корисним при захисті даних під час передачі, тоді як маскуванню даних – під час обміну даними із зовнішньою організацією. Інтернет-зв'язок можна захистити за допомогою таких протоколів, як Secure Socket Layer (SSL) і Transport Layer Security (TLS). Точки доступу Wi-Fi можна захистити за допомогою віртуальних приватних мереж (VPN) для захисту даних. Проте, складність питання захисту персональних даних пацієнта полягає також у тому, що сьогодні низка законодавчих норм не вимагає захисту всієї інформації про пацієнта. Якщо медична інформація надто захищена, це може перешкодити потоку інформації, необхідної для ефективного лікування та медичних втручань.

Висновки: Використання електронних баз даних охорони здоров'я останнім часом зросло в геометричній прогресії, що полегшило можливість ділитися інформацією про пацієнта та отримувати доступ до неї. Зі зростанням попиту зберігання, пошуку та передачі, отримання інформації в галузі охорони здоров'я сьогодні потребує більшої безпеки для захисту даних. Одним із способів організації та зберігання інформації в є стек, як різновид структури даних. Впровадження надійного захисту та конфіденційності на всіх рівнях основного стеку є єдиним перспективним підходом для захисту даних в охороні здоров'я.

Ключові слова: конфіденційність пацієнта, захист даних про здоров'я,