УДК 004.45: 004.62
DOI https://doi.org/10.32782/IT/2024-2-16

Олександр САФАРОВ
кандидат технічних наук, доцент кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0003-1489-2006*
***Scopus Author ID:** 57191867000*

Валерій КОРНІЄНКО
доктор технічних наук, професор, завідувач кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0002-0800-3359*
***Scopus Author ID:** 56446921900*

В'ячеслав ГОРЄВ
кандидат фізико–математичних наук, доцент, завідувач кафедри фізики, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького 19, Дніпро, Україна, 49005
***ORCID:** 0000-0002-9528-9497*
***Scopus-Author ID:** 55047688400*

Вадим МЄШКОВ
аспірант кафедри безпеки інформації та телекомунікацій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, Дніпро, Україна, 49005
***ORCID:** 0000-0001-9873-4712*

Бібліографічний опис статті: Сафаров, О., Корнієнко, В., Горєв, В., Мєшков, В. (2024). Підвищення кібербезпеки електронних комунікаційних систем медичного призначення. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 128–133, doi: https://doi.org/10.32782/IT/2024-2-16

ПІДВИЩЕННЯ КІБЕРБЕЗПЕКИ ЕЛЕКТРОННИХ КОМУНІКАЦІЙНИХ СИСТЕМ МЕДИЧНОГО ПРИЗНАЧЕННЯ

У роботі визначено актуальність розгляду та всебічного аналізу рівня кібербезпеки електронних медичних систем і, перш за все, захисту персональних даних в них. Досліджено потенційні можливості зловмисника та потенційні атаки на ці дані.

Окреслені проблеми вирішуються шляхом використання програмних методів забезпечення безпеки. Як показують результати аналізу, кожен із методів забезпечує безпеку лише окремого аспекту – захист від втручання в код, коректність логіки виконання програмного додатку тощо. Як наслідок, продуктивним бачиться комплексний підхід, який синтезує всі розглянуті методи.

***Метою роботи** є дослідження та аналіз вразливостей персональної інформації в електронних комунікаційних системах медичного призначення та обґрунтування ефективних методів забезпечення кібербезпеки цих систем.*

***Методологія** вирішення поставленої задачі полягає у комплексному та критичному аналізі як існуючих вразливостей, так і методів забезпечення безпеки інформації електронних медичних систем.*

***Наукова новизна.** На основі комплексного критичного аналізу актуальних вразливостей обґрунтовані ефективні методи забезпечення безпеки інформації в сучасних електронних комунікаційних системах медичного призначення.*

***Висновки**. Проведений аналіз загроз безпеці та обґрунтування і використання відповідних методів захисту інформації дозволяють підвищити рівень кібербезпеки електронних комунікаційних систем медичного призначення.*

***Ключові слова:** кібербезпека, електронна комунікаційна система, цифровий медичний пристрій, протокол передачі даних, вразливість, безпека інформації.*

Oleksandr SAFAROV
Candidate of Technical Sciences, Associate Professor of Information Security and Telecommunication Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, safarov o.o@nmu.one
ORCID: *0000-0003-1489-2006*
Scopus Author ID: *57191867000*

Valerii KORNIIENKO
Doctor of Technical Sciences, Professor, Head of Information Security and Telecommunication Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho ave., Ukraine, 49005, korniienko.v.i@nmu.one
ORCID: *0000-0002-0800-3359*
Scopus Author ID: *56446921900*

Vyacheslav GOREV
Candidate of Physical and Mathematical Sciences, Docent, Head of the Department of Physics, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave., Dnipro, Ukraine, 49005, lordjainor@gmail.com
ORCID: *0000-0002-9528-9497*
Scopus-Author ID: *55047688400*

Vadym MIESHKOV
Postgraduate Student at the Department of Information Security and Telecommunications, Dnipro University of Technology, 19 Dmytra Yavornytskoho ave, Dnipro, Ukraine, 49005, mieshkov.v.i@nmu.one
ORCID: *0000-0001-9873-4712*

To cite this article: Safarov, O., Korniienko, V., Gorev, V., Mieshkov, V. (2024). Pidvyshchennia kiberbezpeky elektronnykh komunikatsiinykh system medychnoho pryznachennia [Improving cybersecurity of medical electronic communication systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security,* 2, 128–133, doi: https://doi.org/10.32782/IT/2024-2-16

IMPROVING CYBERSECURITY OF MEDICAL ELECTRONIC COMMUNICATION SYSTEMS

The work determines the relevance of consideration and comprehensive analysis of the level of cyber security of electronic medical systems and, above all, the protection of personal data in them. Potential attacker capabilities and potential attacks on this data are explored.

The outlined problems are solved by using software security methods. As the results of the analysis show, each of the methods ensures the security of only a separate aspect – protection against tampering with the code, correctness of the software application execution logic, etc. As a result, a comprehensive approach that synthesizes all the considered methods is seen as productive.

The aim *is research and analysis of vulnerabilities of personal information in medical electronic communication systems and substantiation of effective methods of ensuring cyber security of these systems.*

The methodology *of the solution to the given task consists in a comprehensive and critical analysis of both existing vulnerabilities and methods of ensuring information security of electronic medical systems.*

Scientific novelty*. On the basis of a complex critical analysis of current vulnerabilities, effective methods of ensuring information security in modern medical electronic communication systems are substantiated.*

Conclusions. *The conducted analysis of security threats and the justification and use of appropriate methods of information protection allow to increase the level of cybersecurity of medical electronic communication systems.*

Key words: *cybersecurity, electronic communication system, digital medical device, data transfer protocol, vulnerability, information security.*

Актуальність проблеми. Розвиток інформаційних технологій передбачає їх проникнення в нові галузі людської діяльності, які раніше не були безпосередньо пов'язані з комп'ютерними системами. У сучасній медичній практиці електронні комунікаційні системи медичного призначення (електронні медичні пристрої) стають все більш поширеним інструментом для діагностики та моніторингу пацієнтів. Разом з розширенням функціональних можливостей подібних пристроїв (таких як запис, і передача даних за допомогою того чи іншого протоколу передачі даних, у тому числі через мережу) виникають нові виклики в області безпеки даних (Azrour, 2021; Metty, 2023).

Вирішення проблем безпеки даних полягає у дослідженні актуальних вразливостей та методів протидії сучасним атакам на дані з метою

створення максимально можливо надійної системи захисту.

Аналіз останніх досліджень і публікацій. Захист персональних даних, з якими в постійному режимі працюють цифрові медичні пристрої є актуальним завданням, оскільки ці дані є конфіденційною інформацією, що охороняється. Таким чином, порушення безпеки такого пристрою може мати серйозні наслідки: витік особистої медичної інформації, хибні діагнози та неправильний вибір протоколу лікування, а також підрив довіри пацієнтів до електронних медичних пристроїв. У цьому контексті забезпечення надійного захисту даних в різноманітних цифрових медичних пристроях стає невід'ємною умовою для успішного впровадження та використання сучасних технологій у медичній практиці.

Проблема захисту даних в електронних комунікаційних системах медичного призначення проявляється тим сильніше, чим більше вони розвиваються. Наприклад, якщо спочатку такий пристрій, як електронний стетоскоп лише записував посилений мікрофоном аудіосигнал аускультації пацієнта, то сучасні моделі крім адаптивної фільтрації сторонніх шумів дозволяють розпізнавати записи та отримувати попередній діагноз в режимі реального часу, а також відправляти самі записи на комп'ютер або інший зв'язаний пристрій за допомогою бездротових протоколів передачі. Інший тип пристрою – апарат штучної вентиляції легень, також пройшов історичний шлях від повністю механічної машини до електронної і більш портативної. Незважаючи на широке поширення та затребуваність, вкрай мала кількість платформ реалізовані з відкритою архітектурою, наприклад The People's Ventilator Project (LaChance, 2023). Такий підхід підвищує доступність подібних систем та динаміку їх розвитку, що особливо актуально через істотні ризики глобальних пандемій. Але чим більшого поширення отримує пристрій, що працює з інформацією, тим вище ймовірність того, що в ньому будуть виявлені проблеми безпеки, тобто зростуть як ризики компрометації персональних медичних даних, так і швидкість реакції спільноти розробників на виявлені канали витоку інформації. Отже, відкритість архітектури є як плюсом, і мінусом системи. Тим не менш, навіть у системах із закритою архітектурою для зберігання та передачі даних практично завжди використовуються вже відомі технології, що добре зарекомендували себе. Для зберігання даних найчастіше обирається той чи інший варіант енергонезалежної пам'яті, а для передачі – відомі протоколи дротової та бездротової передачі. Тому всі сучасні електронні медичні системи мають ті чи інші потенційні канали витоку конфіденційної інформації.

Таким чином, актуальним завданням є аналіз особливостей існуючих проблем безпеки інформації електронних медичних систем та, відповідно, методів забезпечення безпеки цієї інформації.

Мета статті: дослідження та аналіз вразливостей персональної інформації в електронних комунікаційних системах медичного призначення та обґрунтування ефективних методів забезпечення кібербезпеки цих систем.

Виклад основного матеріалу.

Особливості організації роботи з інформацією в електронних комунікаційних системах медичного призначення. Зберігання даних у електронних медичних пристроях є критично важливою та невід'ємною частиною сучасної медичної практики. Логічно, що характеристики інформації, що зберігається, різняться в залежності від типу пристрою, але єдині в одному – ця інформація повинна бути захищена. Практично всі цивілізовані країни так чи інакше законодавчо регулюють правила роботи з медичною інформацією та вимагають дотримання її конфіденційності, розрізняються лише ступінь суворості та конкретні вимоги. Так, у США існує акт (закон) про мобільність та підзвітність медичного страхування (HIPAA) (United States Department of Health and Human Services, 2022), який встановлює стандарти для захисту конфіденційності та безпеки медичної інформації пацієнтів у США. Він вимагає, щоб медична інформація була захищена від несанкціонованого доступу та забезпечує право пацієнтів контролювати свої медичні дані. Загальний регламент захисту даних Європейського Союзу, GDPR (European Parliament and the Council, 2016), встановлює вимоги щодо збору, зберігання та обробки медичних даних, а також забезпечує право на конфіденційність та безпеку персональної інформації. В той час, як HIPAA надає пацієнтам права на контроль та доступ до їх медичних даних без явної згоди на обробку даних, GDPR вимагає явної згоди суб'єкта даних на обробку його персональних даних, включаючи медичні дані. При цьому GDPR передбачає більш високі штрафи за порушення та вимагає обов'язкового повідомлення про порушення безпеки даних.

Безпосередньо самі дані в більшості випадків зберігаються на вбудованій пам'яті пристроїв з можливістю вивантаження їх на зовнішній носій, зв'язаний пристрій або хмарний сервіс. У складних пристроях по типу апаратів штучної вентиляції легень може бути варіант

дублювання, трансляції інтерфейсу програми для віддаленого доступу на сторонній пристрій – у більшості випадків це планшет.

Щодо характеру інформації, то на цифрових медичних пристроях часто зберігається як персональна медична інформація пацієнта, так і допоміжні внутрішні дані, необхідні для забезпечення роботи цих пристроїв. До першої категорії належать персональні дані пацієнта, його медична картка чи історія: діагнози, процедури, результати аналізів тощо. До другої категорії відносяться налаштування та події, що виникають на самому пристрої, а також параметри, що впливають на реалізацію основної функції пристрою: у стетоскопах це може бути тип аускультації та рівень придушення стороннього шуму, а в апаратах штучної вентиляції легень – параметри та режими вентиляції, дані про стан підключеного пацієнта, профілі налаштувань. Звичайно, залежно від конкретного пристрою кількість подібної інформації варіюється, але очевидно, що в обох випадках витік інформації її є загрозою безпеці і може призвести до значних наслідків.

Всі сучасні медичні цифрові прилади у тому чи іншому вигляді мають інтерфейси для введення та виведення даних, оновлення прошивки та програмного забезпечення пристрою та організації доступу для розробників, необхідного для технічного обслуговування. Таким чином, виникає питання про використання протоколів дротового та бездротового зв'язку, які відіграють ключову роль в організації роботи з даними та обміні ними з іншими пристроями. Зважаючи на суттєвий прогрес у стандартизації, а також високу вартість розробки та впровадження власного протоколу, більшість сучасних пристроїв має один або відразу декілька досить поширених стандартних протоколів обміну даними.

З дротових протоколів у цифрових пристроях медичного призначення найчастіше використовуються наступні: Universal Serial Bus (USB), Ethernet (IEEE 802.3) та Recommended Standard 232 (RS-232).

Протокол USB дозволяє як передавати дані, так і подавати живлення на пристрій. Підтримується більшістю існуючих операційних систем та забезпечує можливість швидкого з'єднання з іншими пристроями. Ще однією перевагою даного протоколу його висока сумісність між версіями протоколу, тобто з пристроєм із більш старою версією порту USB можливе повноцінне з'єднання під час використання відповідного кабелю або адаптера.

Протокол Ethernet, переважно застосовується для організації дротового мережевого з'єднання, а в медичних пристроях використовується переважно за тим самим призначенням: забезпечення передачі між медичними пристроями, комп'ютерними терміналами і серверами зберігання даних. Більше того, в сучасних лікарняних закладах найчастіше розгорнуто локальну комп'ютерну мережу, тому використання даного протоколу забезпечує швидке підключення та інтеграцію пристроїв з підтримкою Ethernet до даної мережі.

Протокол RS-232, практично витіснений більш новим протоколом USB у сфері споживчої електроніки, проте, як і раніше, широко застосовується в медичних пристроях. Як і USB, цей протокол простий у використанні підтримується більшістю існуючих операційних систем і не вимагає написання додаткових драйверів. Завдяки тому, що медичне обладнання має куди більший термін служби, ніж споживче, а також через свою простоту і надійність даний протокол все ще популярний серед виробників медичних пристроїв незважаючи на більш низьку швидкість передачі даних.

З актуальних бездротових протоколів слід виділити Bluetooth, Wi-Fi (IEEE 802.11) та Zigbee (IEEE 802.15.4). Для Bluetooth характерна економічність, прагнення мінімально витрачати заряд акумулятора у випадку портативного пристрою, і, як наслідок, обмеженість швидкості та відстані передачі. Крім того, цей протокол переважно використовується для з'єднання лише двох пристроїв. Wi-Fi забезпечують набагато більшу швидкість передачі даних і можливість підключення пристрою до мережі, для медичних приладів це в більшості випадків бездротова мережа медичного закладу, а також можливість організації взаємодії з іншими пристроями, що підключені до цієї ж самої мережі. Протокол Zigbee ще більш економічний, ніж Bluetooth, але й швидкість передачі даних у ньому нижча, проте за допомогою нього можна організувати повноцінні мережі, які будуть співіснувати з каналами Wi-Fi без перешкод.

Вибір протоколу безпосередньо залежить від вимог до конкретного пристрою, в першу чергу таких як швидкість передачі даних, енергоефективність, необхідність підключення до мережі або пов'язаного з пристроєм додатку.

Загрози інформації в електронних комунікаційних системах медичного призначення. Перераховані вище протоколи передачі є основними потенційними каналами витоку інформації з цифрових медичних пристроїв. Саме використовуючи наявні вразливості у цих протоколах, зловмисник може отримати несанкціонований доступ до персональних даних, що зберігаються на пристрої. Використання

навіть захищених і надійних хмарних сервісів не здатне повноцінно усунути цю загрозу, оскільки пристрій залишається вразливим і так чи інакше буде передавати дані в хмару. Крім того, далеко не в кожному медичному приладі раціонально застосовувати хмарні сервіси для роботи з даними: враховуючи високі вимоги до надійності та стабільності роботи цього типу пристроїв для їх коректної роботи був би необхідний постійний, наднадійний та високошвидкісний канал зв'язку з хмарою. Таким чином, має сенс розглядати вразливості персональних даних, які зберігаються у внутрішній пам'яті пристрою і передаються провідним або бездротовим шляхом, а також відповідні можливості зловмисника, що витікають з цих вразливостей.

Вважається, що потенційний зловмисник має наступні можливості для проведення атаки на медичний цифровий пристрій:

1. Наявність фізичного чи віддаленого доступу до середовища, де використовується пристрій.

2. Знання протоколу, що використовується для комунікації з пристроєм.

3. Можливість отримати доступ до каналу комунікації з пристроєм за допомогою сторонніх пристроїв або програм.

4. Можливість видати себе за легального користувача медичного пристрою за допомогою підробки або отримання доступу до облікового запису такого користувача на зв'язаному пристрої (комп'ютерному терміналі, смартфоні тощо) (Newaz, 2021).

До найпоширеніших типів атак можна віднести наступні:

1. Відмова в обслуговуванні (DOS) – це одна з найпопулярніших атак на систему безпеки, яка спрямована на те, щоб завадити законному користувачеві мати авторизований доступ до мережевих ресурсів. Як правило, здійснюється за допомогою флуд-атаки – відправлення безлічі пакетів або повідомлень з метою перевантажити ресурси системи.

2. Повторна атака – досить старий тип атаки, спрямований на захоплення фрагмента даних або навіть усієї сесії обміну даними з метою подальшого використання перехопленої інформації під виглядом легальної. Тобто, по суті, це експлуатація вразливості безпеки, коли дані або їх частина обробляються системою без авторизації.

3. Атака з підбором пароля – зловмисник здійснює прослуховування процесу авторизації легальних пристроїв або користувачів з метою отримати корисну інформацію для того, щоб оптимізувати подальший підбір пароля і, у разі успішного підбору, авторизуватися в системі.

4. Спуфінг-атака – атака, коли незареєстрований користувач завдяки використанню фальсифікованих параметрів змушує сервера авторизувати його, що дозволяє йому діяти в системі надалі, маючи права легального користувача.

5. Інсайдерська атака – тип атаки, який виникає при спробі легального, авторизованого користувача нашкодити системі, навмисно або випадково (Azrour, 2021).

Всі ці атаки можна застосувати і проти цифрових медичних пристроїв і, як показують дослідження (Newaz, 2021), найчастіше метою зловмисника стають неінвазивні терапевтичні медичні пристрої, тобто менш специфічні прилади, які в більшості випадків розташовуються поруч із тілом пацієнта, а чи не вживлюються в нього. Такі пристрої часто мають слабкі механізми аутентифікації та шифрування процесів передачі даних, якщо вони взагалі реалізовані.

Обґрунтування методів забезпечення безпеки інформації в електронних комунікаційних системах медичного призначення. Виходячи з описаних можливостей зловмисника можна виділити наступні методи протидії йому та рішення для забезпечення безпеки персональної інформації на медичних пристроях.

1. Безпечне середовище виконання. Для забезпечення безпеки медичних додатків їх слід запускати у спеціально створеному безпечному для виконуваного коду та завантажуваних даних просторі. Створення такого середовища здійснюється за допомогою так званих віртуальних машин, які надають додатку мережевий інтерфейс, сховище для збереження даних та середовище для виконання коду програми. Таким чином, програми, що працюють на віртуальних машинах, ізольовані одна від одної, що підвищує рівень безпеки, хоча сама система керування середовищем на рівні операційної системи все ж таки може бути скомпрометована.

2. Статичний аналіз. Незважаючи на те, що запуск програми в ізольованому безпечному середовищі в цілому захищає його від вразливостей системи, цей метод практично безсилий у разі, якщо шкідливий код впроваджено в саму програму. Методи статичного аналізу, зокрема методи символьного виконання та аналізу вихідного коду, використовуються щоб охарактеризувати можливу поведінку програми при його виконанні, а також для того, щоб виявити помилки та шкідливий код у вихідному коді додатку. Отже, дані методи передбачають доступ до вихідного коду програми, який далеко не завжди доступний для медичних додатків.

3. Методи динамічного аналізу. Додаток поміщується в тестове середовище та

здійснюється аналіз його поведінки прямо під час виконання. Існують окремі фреймворки, що дозволяють змоделювати безпечну та небезпечну поведінку програми відповідно до зазначених політик безпеки, проте не завжди є можливість проаналізувати увесь спектр можливої поведінки досліджуваного додатку.

4. Формальна верифікація. Методи цього типу використовують чітко сформульовані висловлювання математичної логіки і здійснюють перевірку слідуючи суворим висновкам з цієї логіки. Таким чином, досліджується весь простір станів системи, щоб виявити відповідні параметри безпеки для всіх можливих вхідних даних. Формальна верифікація може бути використана для виявлення тих чи інших вразливостей, які можуть бути наявні у медичних цифрових пристроях і є по суті методом запобігання виникнення потенційних каналів витоку даних (Newaz, 2021).

Висновки з даного дослідження і перспективи подальшої роботи у даному напрямку. Здійснено докладний опис особливостей організації роботи з даними в сучасних **електронних комунікаційних системах медичного призначення** і розглянуто протоколи, що використовуються для цього (як дротові так і бездротові). Виходячи з цього, проаналізовано існуючі загрози безпеці інформації медичних систем та визначені потенційні типи атак на них. Використання обґрунтування в статті методів захисту інформації дозволяють підвищити рівень кібербезпеки електронних комунікаційних систем медичного призначення.

Подальші дослідження мають бути спрямовані на опрацювання та розробку принципово нових методів забезпечення безпеки інформації в медичних системах, у тому числі з використанням інтелектуальних методів обробки інформації.

ЛІТЕРАТУРА:

1. Azrour M., Mabrouki J., Guezzaz A., & Kan-wal A. Internet of Things Security: Challenges and Key Issues. Security and Communication Networks, 2021, vol. 2021, article no. 5533843, pp. 1–11. DOI: 10.1155/2021/5533843

2. Metty P., Maglaras L., Amine Ferrag M., Almomani I. Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 2023, 9, (4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007

3. LaChance J., Schottdorf M., Zajdel TJ., Saunders JL., Dvali S., Marshall C., et al. PVP1–The People's Ventilator Project: A fully open, low-cost, pressure-controlled ventilator research platform compatible with adult and pediatric uses. 2022. PLoS ONE 17(5): e0266810. https://doi.org/10.1371/journal.pone.0266810

4. United States Department of Health and Human Services. The HIPAA Privacy Rule. URL: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) URL: http://data.europa.eu/eli/reg/2016/679/oj

6. Newaz A. I., Sikder A. K., Rahman M. A., Uluagac A. S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2021. 2(3), 1–44.

REFERENCES:

1. Azrour, M., Mabrouki, J., Guezzaz, A. & Kan-wal, A. (2021). Internet of Things Security: Challenges and Key Issues. Security and Communication Networks, 2021, vol. article no. 5533843, pp. 1–11. DOI: 10.1155/2021/5533843.

2. Metty, P., Maglaras, L., Amine Ferrag, M. & Almomani, I. (2023). Digitization of healthcare sector: A study on privacy and security concerns. ICT Express, 9, (4), 571–588. https://doi.org/10.1016/j.icte.2023.02.007.

3. LaChance, J., Schottdorf, M., Zajdel, TJ., Saunders, JL., Dvali, S., Marshall, C, et al. (2022). PVP1–The People's Ventilator Project: A fully open, low-cost, pressure-controlled ventilator research platform compatible with adult and pediatric uses. PLoS ONE 17(5): e0266810. https://doi.org/10.1371/journal.pone.0266810

4. United States Department of Health and Human Services.The HIPAA Privacy Rule. Retrieved from: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) Retrieved from: http://data.europa.eu/eli/reg/2016/679/oj

6. Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Transactions on Computing for Healthcare, 2(3), 1–44.