TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology

Britta Sillaots 21204IVCM

Convergence Of Hospital and Consumer Wearables, Their Legal Aspects and Micro Data Sovereignty

Master's thesis

Supervisor: Dr. Matthew James Sorell

Co-Supervisor: Aleksi Oskar Johannes Kajander LL.M

Tallinn 2024

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Meditsiini- ning Tarbijaseadmete Ühildumine, Nende Õiguslikud Aspektid ja Mikro Andmete Suveräänsus

Magistritöö

Juhendaja: Dr. Matthew James Sorell

Kaasjuhendaja: Aleksi Oskar Johannes Kajander LL.M

Tallinn 2024

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Britta Sillaots

12.05.2024

Abstract

Over the past few years, the use of smart wearables has grown. Whether smartwatches are used for a fashion statement or for keeping an eye on everyday activity levels, those devices can be found on almost every person's wrist. The field of wearable devices continues to evolve and integrate into our everyday lives. Many of those devices offer us the opportunity to measure our heart rate, daily steps, temperature, and other important aspects of our health.

The topic of smart wearables and e-health is familiar to the author since their working experience is in the field of medical software.

The aim of the thesis is to explore how the chosen popular smartwatches ecosystem works, what legislation the manufacturers must follow in order for them to categorize the product as a medical device, and how 5G core network could aid in making the connection for sensitive data flow more secure. Using a systematic literature review, the author provides a legislative ecosystem for such cases and explores the use of a 5G core network as a solution for sensitive data transfer.

From the thesis results, it can be concluded that the Estonian legal ecosystem matches the European legislative ecosystem regarding the topic of categorizing medical wearables. 5G core technologies could help with the security of sensitive data transfer by lessening the distance that the data travels with the use of local breakout and network slicing.

The thesis is divided into five chapters (Introduction, Background, Literature, Methodology, Analysis, and Summary).

Keywords: Smart Wearables, 5G, Sensitive Data Flow, Healthcare, Smartwatches, Legal Aspects.

This thesis is written in English and is 58 pages long, including 6 chapters, 5 figures, and 3 tables.

Annotatsioon

Viimastel aastatel on nutikate kantavate seadmete kasutamine kasvanud. Olenemata sellest, kas nutikellasid kasutatakse trendiga kaasaskäimiseks või igapäevase aktiivsuse taseme jälgimiseks, võib neid seadmeid leida peaaegu iga inimese randmelt. Kantavate seadmete valdkond areneb jätkuvalt ja integreerub meie igapäevaellu. Paljud neist seadmetest pakuvad meile võimalust mõõta meie südame löögisagedust, igapäevaseid samme, temperatuuri ja muid meie tervise olulisi aspekte.

Nutikate kantavate seadmete ja e-tervise teema on autorile tuttav, kuna autori töökogemus on meditsiinitarkvara valdkonnast.

Selle töö eesmärk on uurida, kuidas töötab valitud nutikellade ökosüsteem, milliseid seadusandlikke dokumente peavad tootjad järgima, et toode meditsiiniseadmeks liigitada, ja kuidas 5G võiks aidata muuta tundliku andmevoo ühenduse turvalisemaks. Kasutades süstemaatilist kirjanduse analüüsi, autor toob töös välja olulisimad legaalsed dokumendid ning analüüsib, kuidas 5G tehnoloogia võiks aidata tundlike andmete transpordile kaasa .

Töö tulemustest võib järeldada, et Eesti meditsiiniseadmete reeglistik ühtib Euroopa omadega. 5G võib aidata tundlike andmete kaitsele kaasa, vähendades andmete saatmise teekonda.

Käesolev lõputöö on jagatud viieks peatükiks (Sissejuhatus, Taust, Kirjandus, Metoodika, Analüüs ja Kokkuvõte).

Märksõnad: nutikad kantavad seadmed, 5G, tundlik andmevoog, tervishoid, nutikellad, juriidilised aspektid.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 58 leheküljel, 6 peatükki, 5 joonist, 3 tabelit.

List of abbreviations and terms

AFib	Atrial fibrillation
BIA	Bioelectrical impedance analysis
BS	Base Station
BTLE	Bluetooth Low Energy
CDA	Clinical Document Architecture
ECG	Electrocardiography
EU	European Union
FDD	Frequency Division Duplex
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IA	Department of Computer Systems
IoT	Internet of Things
LAN	Local Area Network
LTE	Long-Term Evolution
MDR	Medical Device Regulation
MIMO	Multiple Input Multiple Output
TDD	Time Division Duplex
5G	Fifth Generation

Table of Contents

List of figures

List of tables

1.Introduction

Traditional healthcare systems encounter numerous barriers in chronic disease monitoring, personalized medicine, disease prevention, and early intervention. With the increasing prevalence of chronic diseases among the elderly, continuous monitoring and long-term care are necessary. However, hospitals in resource-limited areas struggle to provide long-term monitoring, which may result in disease progression and significantly impact the patient's quality of life. [1]

In recent years, with the development of the internet, intelligent hardware, and big data, wearable technology has developed rapidly in various fields, such as health care, education and culture, social networking, and the military. Some of these technologies are becoming part of people's daily lives in the form of accessories such as smartwatches. [2]

The use of smart wearables could improve healthcare service quality and offer convenient remote monitoring for both patients and physicians. Between 2019 and 2022, the number of connected wearable devices worldwide increased substantially. In 2022, the number reached to around 1.1 billion, up from 929 million recorded one year before. [3]

Third-generation wearable devices can combine sensors, microprocessors, and wireless modules to continuously sense and monitor various physiological indicators of patients in an intelligent manner while reducing power consumption, improving comfort, and allowing the data to be combined with health information from other channels. [4]

1.1. Motivation

The topic of smart wearables and e-health is familiar to the author since their working experience is in the field of medical software. Smart wearables in the medical context

have not yet seen widespread adoption due to the reservation of the local healthcare sector. It seems inevitable that following the trends from other countries, Estonia will sooner or later follow the trend. Legislative questions could arise with the growing use of smart wearables and seemingly borderless data exchange. When the change happens, it is important to understand the legal ecosystem.

1.2. Research Questions

The aim of the thesis is to explore how smart wearables, such as smartwatches, are used in modern healthcare, how the chosen smartwatches ecosystem works, what legislative documents the manufacturers must follow in order for them to categorize the product as a medical device, and how 5G could aid in making the connection for sensitive data flow more secure.

Research questions consist of two parts: background information and focus questions. The background provides the reader with information about how popular smartwatches' data flow works, what they provide the end user in the sense of sensors and an overview of case studies that have rewarded the manufacturers with medical device classifications. Since the topic of legislation and data flow brings out the problem with smartwatch sensitive data flow, the author includes a case, where sensitive data flow was breached and used against the end users.

Focus questions:

Rq 1. What legislations must manufacturers follow in order to categorize the smart wearable as a medical device in Estonia;

Rq 2. Benefits and risks of using 5G core network as a solution to secure data flow;

- 5G in our context: defining local breakout, software-defined network, network slicing, and what are their roles in the control of the flow of private information;
- Could network slicing support data sovereignty;

1.3. Scope and Goal

The thesis seeks to identify the legal ecosystem in Estonia on the topic of "when consumer wearable wants to be categorized as a medical use device". Since medical devices handle sensitive data, the author explores ways in which 5G, as a core network, could be used to heighten the security of sensitive data transfer.

This thesis focuses on the Estonian legislative system and 5G as a core network. Because Estonia is the frontrunner in digitalization in other government services, the scope was focused on Estonias legal ecosystem.

1.4. Novelty

Previous researches have used more of qualitative research on the topic of how smart wearables are used in healthcare or how 5G is used in healthcare. This thesis differentiates from the existing work with its' focus on the legislative ecosystem combined with the recommendation on how smartwatch manufacturers could improve sensitive data flow with the 5G Core network.

2.Background

The background section covers the topic of different model comparisons in the Apple Watch [5], Samsung [6] Smartwatch, and Fitbit [7]. Apple, Samsung, and Garmin brands were chosen because they are the market leaders in the Smart Watches category in the EU [8]. In the subsections, there is a compact overview of how chosen smartwatches' ecosystems work and where the collected data is processed.

2.1. Apple Watch

This section covers the topic of Apple smart wearable ecosystems. Table 1 shows the different sensors and measurements that Apple Watch models offer to the end user. Figure 1 shows the data flow of collected data.

Table 1. Apple Watch different models comparison. [5]

Model	**Heart Sensor (electrical/optical)**	**GPS**	**Emergency SOS**	**Temperature sensor**
Series 9	yes(both)	yes	yes	yes
Ultra 2	yes(both)	yes	yes	yes
SE	yes(optical)	yes	yes	no
Series 8	yes(both)	yes	yes	yes
Ultra	yes (both)	yes	yes	yes
Series 7	yes(both)	yes	yes	no
Series 6	yes(both)	yes	yes	no
SE (1st gen)	yes(optical)	yes	yes	no
Series 5	yes(both)	yes	yes	no
Series 4	Yes (both)	yes	yes	no
Series 3	yes(optical)	yes	yes	no

Series 2	Yes(optical)	Yes	no	no
Series 1	Yes(optical)	no	no	no

It is stated on the Apple official website that the temperature sensing feature is not intended for medical use. [9] The electrocardiography (ECG) app and irregular rhythm notification require the latest version of watchOS and iOS and are not intended for use by people under 22 years old. The irregular rhythm notification is not designed for people who have been previously diagnosed with atrial fibrillation (AFib).[9]

2.1.1. Apple Smartwatch Data Flow

The health data that the user decides to share will be encrypted and stored by Apple. Apple does not have access to the encryption keys for the stored data, they can not decrypt, view, or otherwise access the health app data. Health app data is stored on a dedicated server so that Apple can share the collected data with user-chosen healthcare organizations. Apple servers are located in the United States, Europe and China, and in development are servers in Denmark and Ireland. The data is sent from the phone only when the device is unlocked and connected to the internet. The data is maintained only for as long as necessary to support the use of this sharing feature, and the data will only be used to enable the sharing feature. Any health data shared in connection with this feature will be encrypted in transit and at rest when stored on Apple servers. [10]

The user's device stores all HealthKit data locally. HealthKit is an Apple framework that is used to access health data. For security, the device encrypts the HealthKit store when the user locks the device. As a result, the app may not be able to read data from the store when it runs in the background. However, the app can still write to the store, even when the phone is locked. HealthKit temporarily caches the data and saves it to the encrypted store as soon as the user unlocks the phone. [11]

Personal data relating to individuals in the European Economic Area, the United Kingdom, and Switzerland is controlled by Apple Distribution International Limited in Ireland. [12]

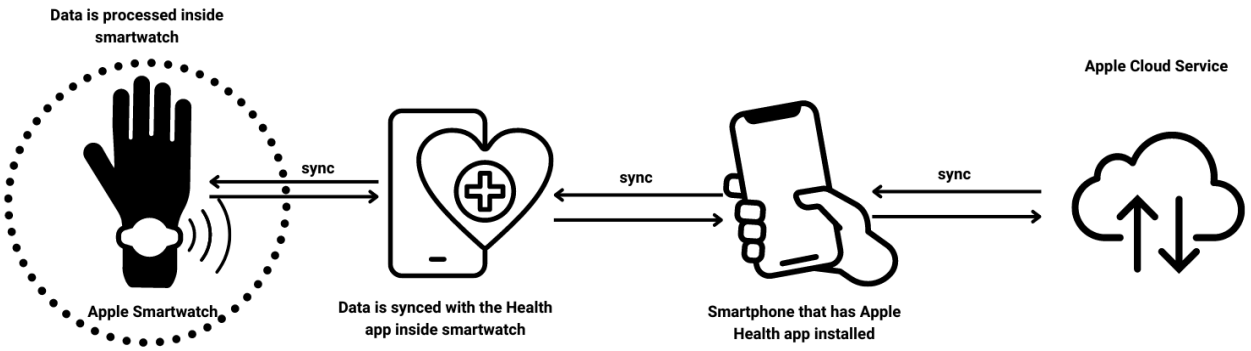

Figure 1: Apple ecosystem [10][11][13]

2.2. Samsung Smartwatch

This section covers the topic of Samsung smart wearable ecosystems. Table 2 shows the different sensors and measurements that Samsung Watch models offer to the end user. Figure 2 shows the data flow of collected data.

Table 2. Samsung Watch different models' comparisons.[14]

Model	**Heart Sensor (Electrical/Optical)**	**Bioelectrical Impedance Analysis Sensor**	**GPS**
Watch4 BT 40mm	yes (both)	yes	yes
Watch4 LTE 40mm	yes (both)	yes	yes
Watch4 BT 44 mm	yes (both)	yes	yes
Watch4 LTE 44mm	yes (both)	yes	yes
Watch4 Classic BT 42mm	yes (both)	yes	yes
Watch4 Classic LTE 42mm	yes (both)	yes	yes
Watch4 Classic BT 46 mm	yes (both)	yes	yes
Watch4 Classic LTE 46mm	yes (both)	yes	yes
Watch5 (44mm) LTE	yes (both)	yes	yes

Watch5 (40mm) BLUETOOTH	yes (both)	yes	yes
Watch5 (40mm) LTE	yes (both)	yes	yes
Watch5 Pro BLUETOOTH	yes (both)	yes	yes
Watch5 Pro LTE	yes (both)	yes	yes
Watch5 (44mm)	yes (both)	yes	yes

Bioelectrical impedance analysis (BIA) is used to analyze human body composition by applying a small alternating current through the body and measuring the impedance.[15] The smaller the electrode of a BIA device, the larger the impedance measurement error due to the contact resistance between the electrode and human skin. [15]

2.2.1. Samsung Smartwatch Data Flow

Users' health data (e.g., weight, blood pressure, body composition) that Samsung Health collects is encrypted, and they are stored with the use of the Knox platform.[16] Data is synchronised and backed up by using the Samsung Cloud. [17] Data that is chosen to be synchronised is automatically sent to Samsung, and Samsung stores them. When the provided services are used, the data that has been collected through them could be sent to the EU, Korea, USA, Switzerland, United Kingdom, Australia, Singapore, India, the Philipines, and Argentina. Data is shared with the countries that the EU General Data Protection Regulation (GDPR) has deemed to be safe. [17]

In addition to the categories of information obtained by Samsung discussed above, their services may generate data automatically when the user uses certain services or may utilize data that the user generates independently (e.g. registering biometric data such as fingerprints to unlock your device). All of this data remains on the device and is not transmitted to Samsung, nor does Samsung obtain or access this data. Samsung does not share this data with third parties. Face-clustering data will remain on the device until the user clears the cache in system settings, resets the device to its factory setting, or deletes the photos from the device. User can delete their registered biometric data at any time in the applicable settings. Because Samsung does not have access to this data, Samsung cannot delete it.[18]

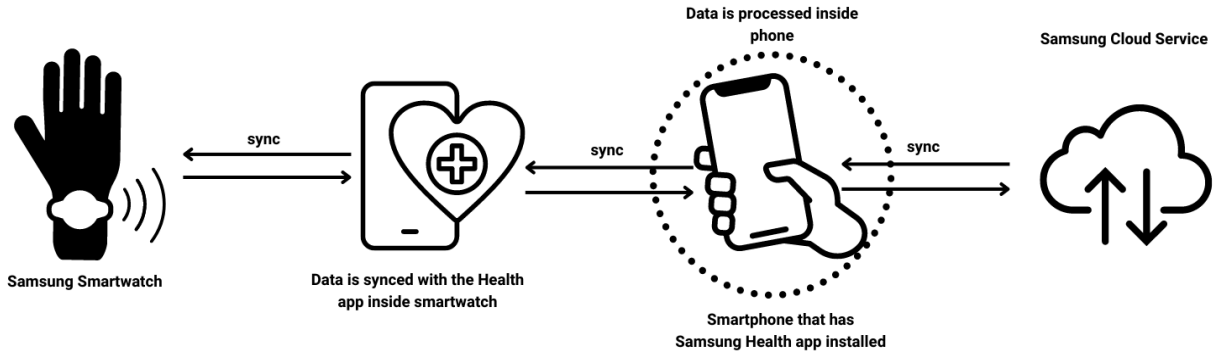

Figure 2: Samsung ecosystem.[16][17] [18]

2.3. Fitbit Smartwatch

This section covers the topic of Fitbit smart wearable ecosystems. Table 3 shows what different sensors and measurements Fitbit models offer to the end user. Figure 3 shows the data flow of collected data.

Table 3. FitBit Watch different models' comparisons [7]

Model	**Heart rate**	**GPS**	**SpO2 (blood oxygen) tracking**	**Skin temperature sensor**	**SOS**
Fitbit Sense 2	yes	yes	yes	yes	no
Google Pixel Watch 2 4G LTE + Bluetooth/Wi Fi	yes	yes	yes	yes	yes
Google Pixel Watch 2 Bluetooth/Wi Fi	yes	yes	yes	yes	yes
Google Pixel Watch 4G LTE + Bluetooth/Wi Fi	yes	yes	yes	no	yes
Google Pixel Watch Bluetooth/Wi Fi	yes	yes	yes	no	yes

Fitbit Versa 4	yes	yes	yes	no	no

There is no information on the official Fitbit page on whether they use optical or electrical sensors to measure heart rate. However, the product description mentions that they use light technology (photoplethysmography), which indicates that they use optical sensors to measure heart rate.[19]

2.3.1. Fitbit Data Flow

Fitbit devices are designed to buffer activity data locally on the device. Occasionally, the user must synchronize their device with the Fitbit service. An app is available to perform the synchronization. During synchronization, the Fitbit application forwards the users' buffered activity data to Fitbit-operated servers over the Internet, where the activity data is stored. The activity data does not stay on the smartphone- user data is fetched from the Fitbit cloud service during each synchronization.[20]
Synchronization between Fitbit devices and smartphones is performed over Bluetooth. In particular, the BTLE [20] (Bluetooth Low Energy) protocol is used. Synchronization between smartphones and the Fitbit service occurs in an encrypted session over the Internet. [20]

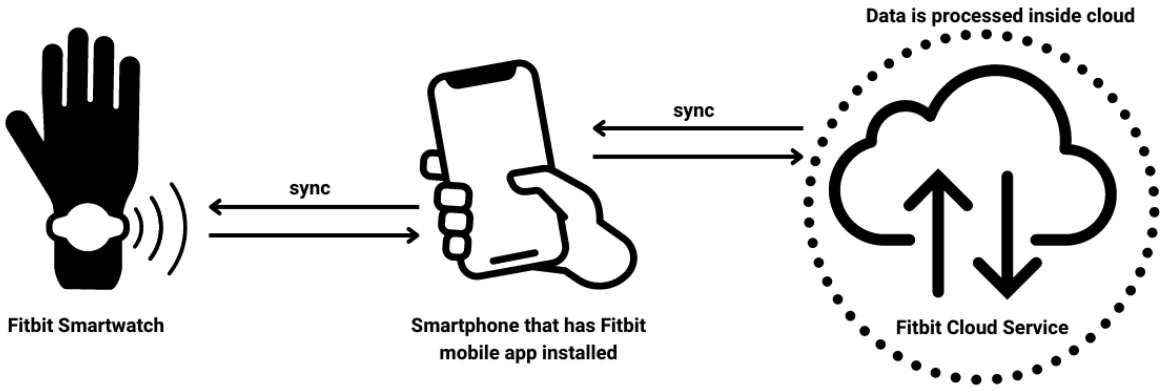

Figure 3: Fitbit ecosystem.[20]

2.4. Clinical Document Architecture (CDA)

The Clinical Document Architecture (CDA) was developed to facilitate the electronic transfer of health information across medical facilities. Medical facilities in the United States, United Kingdom, and Australia widely use CDA. The information is stored and transferred in the XML format. [11] Estonia also uses XML format to exchange data in the X-road service. [21]

Apple Health is compatible with the CDA standard. All CDA documents are stored under Health Records. [11] There is no information on whether or not Samsung Health uses the CDA format to store and exchange data. It is known that data can be imported as CSV files.

A CDA document is entered into Apple Health if you receive the complete file (e.g. from a hospital) and open it with the Apple Health app. It appears that, once registered, CDA documents become part of synchronized data and will be stored in your iCloud account.[11]

CDA documents contain highly sensitive medical information.[11]

3. Literature

Recent studies ([1],[4],[2]) have shown the significant use of smart wearables in the medical context and the use of 5G in the use case of securing private data flow. This section presents prominent papers that discuss the topic of smart wearables in the medical context and 5G use in the medical context.

The thesis includes 53 papers. Papers were selected based on the search strings such as Medical Wearables, Consumer Wearables, Smartwatches, 5G, 5G Core, 5G Radio, Europe Medical Device Legislation, Estonia Medical Device Legislation. The grey literature includes papers from developers' documentation, case studies and government regulations, documentations and standards.

Many of the chosen papers bring out how wearable sensor applications are used in human body systems. “Clinical applications of smart wearable sensors” by Q. Tao et al. [1] categorizes the use of smart wearable sensors by applications according to different diseases. “Wearable Health Devices in Health Care: Narrative Systematic Review” by L. Lu et al, [2] shows the review of 82 papers on the subject of wearable devices in a healthcare context. Use cases, such as chronic disease management, health and safety monitoring, diagnosis and treatment of diseases, and rehabilitation, are categorized as devices. The objective of both of the papers was to show how smart wearables and sensors are used in healthcare. “The Growing Use of Consumer-Grade Medical Devices: Advice for Physicians and Their Patients” by ECRI organization[22] is written as a guidance article for patients and family physicians about consumer-grade products and medical devices. It highlights the use and categorization of the FDA definition and brings out points on why the collected data may be different. “Wrist-wearable bioelectrical impedance analyzer with miniature electrodes for daily obesity management” by M. H. Jung et al[15] provides the reader with a statistical analysis of how wrist wearable sensors could be used for obesity management. The study found that in comparison to commercial use bioelectrical impedance analyzer, the developed

method for using wrist-wearable sensors exceeded the performance of the first device and produced more accurate results.

Smart healthcare is also a relevant topic since it contains the use of smart wearables in the medical context. ”Smart Healthcare: making medical care more intelligent” by S. Tian et al [4] provides a list of different technologies that are being used in the medical context, starting from the algorithms and ending with virtual assistants. “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare” by B. Farahani et al [23] provides a survey of published papers on the topic of Internet of Things (IoT) eHealth and proposes a holistic eHealth ecosystem covering different system layers. Highlighted that the problem is still regarding the topic of scalability and data privacy.

What is uniform in chosen papers and articles is that overall, there is a lot of information about how sensors, smart wearables, smart watches, etc could be used in the medical context; it lacks guidance and uniform regulations. The problematic topic is also the use of smart wearables for remote monitoring and how to keep the data transfer between the patient and the hospital private. The amount of data that travels between the parties is complicated and large, which leads to complications and difficulties in ensuring data integrity and confidentiality. They stated that from a patient's perspective, smart healthcare lacks relevant legal norms, and there are risks with regard to personal information and privacy breaches.

For the technical side of the thesis, the author analysed the developer documentation and website information of the chosen smartwatch brands. Based on the information gathered, the author used Canvas to model the diagrams of how the data flow works on chosen smartwatches.

4. Methodology

A systematic review of existing legal documents regarding consumer wearables and medical devices was conducted to determine the scope of the documents. From the analysed documents, only documents regarding the topic of how consumer devices could be categorized as medical devices and legal documents about sensitive data transfer from smart wearable devices were picked out. Chosen documents were analysed to identify the legal ecosystem that applies to smart wearables and sensitive data flow. Validation comes through working with a co-supervisor to ensure that the legislation exists and is being used in the current legal system. Based on the results from the analysis of legal documents, there could be solutions within 5G architecture that could provide solutions to sensitive data flow and control of the data. The 5G solution validation comes with working and analysing the topic with supervisor.

The search strings used were smart wearables, hospital wearables, consumer wearables, 5G, and legal aspects. Combining those search strings, the literature was chosen. From the chosen literature, the author used the snowballing technique to explore the topic further. The literature that was used had to be written after the year 2010, determination based on the abstract whether the paper was relevant. Search engines such as Google, Google Scholar, IEEE, and Google Books were used. Chosen were the articles that were accessible through TalTech VPN.

Relevant case studies will be covered in the analysis.Relevancy consist of the fact, if the manufacturer was rewarded with a medical device classification from the result of the case study. Apple aFib and Samsung sleep apnea study highlights the use of smartwatch in healthcare. HealthEngine data breach highlights the security risks of not handling sensitive data with proper care.

Definitions that are mentioned throughout the thesis:

1. Medical Device: A medical device can be any instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article intended by the manufacturer to be used, alone or in combination for a medical purpose. [24]
2. Consumer device: Devices that consumers use on their own, can be purchased and is not intended by the manufacturer to be used alone or in combination for a medical purpose.

5. Analysis

In the analysis, the author analyses the legislation that is applicable to the Estonias' case in the topic of sensitive data transfer and consumer wearables being used in medical settings. As shown on figures 1,2 and 3, the data travels between the devices and servers. With that, it is important to know how the legal ecosystem affects the flow of sensitive health data. The author also included, as an example from the other countries' case, the FDA regulation on medical devices.

5.1. Consumer Devices That Have Received Medical Device Classifications and Example of How Medical data is Handled Incorrectly

In this section, the author provides 2 examples on how Apple and Samsung smartwatch manufacturers have received the medical device classification from the FDA/EU MDR or both to their devices. The example about HealthEngine data privacy breach shows how important it is to have regulations and network architecture, that enhance sensitive data security, in use.

5.1.1. Large-Scale Assessment of a Smartwatch to Identify Atrial Fibrillation

The chosen study wanted to discover the detection possibility of AFib with the use of a smartwatch and the included app. The study protocol was approved by the institutional review board at Stanford University and by a central institutional review board. [25] It is also important to note that the study was sponsored by Apple, which owns the data that was collected during the study.

The study recruited 419297 participants to conduct the study, and the recruited participants had to report themselves whether they had a history with AFib or not.

Participants who had been diagnosed with AFib and reported the use of AFib medicine were not included in the study. The study used an Apple iPhone smartphone app to monitor the patients. The participants had to possess an Apple iPhone and Apple Watch, be over the age of 22, and be residents of the United States. In the chosen app, there is an irregular pulse notification, which is an algorithm designed to notify the user if the algorithm identifies possible atrial fibrillation using optical sensors. If the notification is triggered, the researchers initiate a telemedicine visit, and an ECG patch is mailed to the participant. Surveys were administered 90 days after notification of the irregular pulse and at the end of the study.[25] The main objectives were to estimate the proportion of notified participants with atrial fibrillation shown on an ECG patch and the positive predictive value of irregular pulse intervals with a targeted confidence interval width of 0.10. [25]

Over a median of 117 days of monitoring, 2161 participants (0.52%) received notifications of an irregular pulse. Among the 450 participants who returned ECG patches containing data that could be analysed — which had been applied, on average, 13 days after notification — atrial fibrillation was present in 34% (97.5% confidence interval [CI], 29 to 39) overall and in 35% (97.5% CI, 27 to 43) of participants 65 years of age or older. Among participants who were notified of an irregular pulse, the positive predictive value was 0.84 (95% CI, 0.76 to 0.92) for observing atrial fibrillation on the ECG simultaneously with a subsequent irregular pulse notification and 0.71 (97.5% CI, 0.69 to 0.74) for observing atrial fibrillation on the ECG simultaneously with a subsequent irregular tachogram. Of 1376 notified participants who returned a 90-day survey, 57% contacted healthcare providers outside the study. There were no reports of serious app-related adverse events. The probability of receiving an irregular pulse notification was low. Among participants who received notification of an irregular pulse, 34% had atrial fibrillation on subsequent ECG patch readings, and 84% of notifications were concordant with atrial fibrillation.[25]

That study is relevant to the thesis since the results from the study rewarded Apple ECG application with the FDA class II classification on medical devices.

5.1.2. Samsung's Sleep Apnea Feature First of Its Kind got FDA Authorized

Study done by Sara H. Browne, Dr. Florin Vaida, Dr. Anya Umlauf, Jeffrey Kim, Pamela DeYoung, Robert L. Owens in the Journal of Clinical Sleep Medicine, evaluated the accuracy and precision of continuous overnight oxygen saturation (SpO2) measurement by a commercial wrist device (WD) incorporating high-grade sensors, and investigate WD estimation of sleep-disordered breathing by quantifying overnight oxygen desaturation index (ODI) compared to polysomnography (PSG) ODI and apnea-hypopnea index (AHI) with and without sleep questionnaire data, to assess WD ability to detect obstructive sleep apnea (OSA) and determine its severity.[26]

Participants completed sleep questionnaires, had a WD (Samsung Galaxy Watch 4) placed on their wrist, and underwent attending, in-lab overnight PSG (Nihon Kohden) with pulse oximetry probe secured either to a finger or ear lobe. PSG data was scored by a single experienced registered PSG technologist. The 51 participants analyzed had median age of 49 (range 22-78) years, 66.7% were male, with median body mass index (BMI) 28.1 (range 20.1, 47.3) kg/m2 with race/ethnicity distribution of 49.0% Caucasian, 25.5% Hispanic, 9.8% African-American, 9.8% Asian, and 5.9% Middle Eastern. [26]

The WD conducted reliable overnight continuous SpO2 monitoring with RMSE <3% vs PSG. Predictive models of PSG AHI based on WD measurements alone, or plus sleep questionnaires, demonstrated excellent to outstanding discrimination for OSA identification and severity. Longitudinal WD use should be evaluated promptly based on WD potential to improve accessibility and accuracy of OSA testing, as well as support treatment follow-up.[26]

This study is relevant to the thesis since Samsung Sleep Apnea detection got awarded by the FDA with De Novo and class II classification.

The De Novo request provides a marketing pathway to classify novel medical devices for which general controls alone, or general and special controls, provide reasonable assurance of safety and effectiveness for the intended use, but for which there is no

legally marketed predicate device. De Novo classification is a risk-based classification process. [27]

5.1.3. Privacy Breach in the Misuse of Personal Information Used by HealthEngine

The HealthEngine app, marketed as Australia's biggest online doctors appointment booking service, is reported to have used personal information provided by users and forwarded them to third parties who could contact the users as part of their professional services. The most notable recipient of this data is Slater and Gordon, a personal injury firm.[28] It is noted that Health Engine has over 15 million annual users. [29]

HealthEngine has told its investors that it can tailor its advertising to the symptoms of the target group (patients). Even though the firm has said that they only share private information with users' consent, there is no way to opt out of the option of giving out information to third parties. If the user chooses to opt out of that choice, they can no longer use the app. The company's privacy policy makes no mention of sharing the information with third parties for marketing purposes, but the separate "collection statement", which users must accept to use the service and confirm their booking, says HealthEngine shares personal information with a range of third parties.[28]

The documents reveal that HealthEngine has been sending daily lists of prospective clients to third parties of their clients' sensitive health data, such as medical information, as part of a "referral partnership pilot". The documents also reveal that HealthEngine passed on details of an average of 200 clients a month to Slater and Gordon between March and August last year (the year was 2017).

HealthEngine asks users to include details of their symptoms and medical conditions, including whether they have suffered a workplace injury or been in a traffic accident, as part of the process of booking appointments with general physicians, dentists, physiotherapists, optometrists, and other medical practitioners.[28]

When such case happens in the EU, the organization must notify the breach to the supervisory authority without any delay. In Estonia, Andmekaitseinspektsioon (AKI, data protection inspection) has to be informed in such cases. Since the HealthEngine data contained sensitive information, then they should have notified the individuals affected.

5.2. How Would Medical Grade Consumer Wearable Fit Into the Estonian Legal System

In the EU, and according to the Medical Device Regulation (MDR), medical devices are classified according to the risk they pose to patients, with lower-risk devices such as wheelchairs and reading glasses being placed in Class I and higher-risk devices like pacemakers and heart valves allocated to Class III. In the United States, the FDA also uses a risk-based approach to the classification of medical devices, albeit with some differences in device placement. [30] Table 4 shows how the categorizations are matched between the FDA and EU MDR.

<table>
<tr><th>EU MDR</th><th>Examples</th><th>FDA</th><th>Examples</th></tr>
<tr><td>Class I</td><td>Hospital beds, walking aids, stethoscopes, ultrasound gels</td><td>Class I</td><td>Bandages, surgical instruments, wheelchairs</td></tr>
<tr><td>Class IIa</td><td>Syringes, contact lenses, tubes</td><td>Class II</td><td>Computed tomography scanners, infusion pumps</td></tr>
<tr><td>Class IIb</td><td>Blood bags, long term use contact lenses</td><td rowspan="2">Class III</td><td rowspan="2">Pacemakers, deep-brain stimulators</td></tr>
<tr><td>Class III</td><td>IVF or ART products (substance mixtures), needles, heart valve occluders</td></tr>
</table>

Figure 4: EU MDR and FDA examples. [31] [32]

Samsung's Sleep Apnea Feature and Large-Scale Assessment of a Smartwatch to Identify Atrial Fibrillation are the examples on how smartwatch manufacturer got conformity assessment to be categorized as a medical device. In this section, the author highlights the currently in-force legal aspects of the medical device and consumer device regulations, that are needed to be fulfilled before medical classification could be assigned.

5.2.1. Food and Drug Administration (FDA)

The FDA classifications are not applicable in the EU. This is brought in to show the difference between the categorization in the US and EU. Since Apple ECG application is the case study analysed within this thesis, it is important to bring out on what base that classification was received.

For the smart watch or the smart watch application to receive the classification of a medical device in the US, they have to clear the FDA assessment. Apple ECG conducted a series of clinical trials to monitor the effectiveness, stability, and accuracy of collected data. Based on those trials, the assessment is made by the FDA, and then the device or application is classified as a medical device.

The FDA has established classifications for approximately 1,700 different generic types of devices and grouped them into 16 medical specialties referred to as panels. Each of these generic types of devices is assigned to one of three regulatory classes based on the level of control necessary to assure the safety and effectiveness of the device. The three classes and the requirements which apply to them are: [31]

Device Class and Regulatory Controls

1. Class I General Controls

- With Exemptions
- Without Exemptions

2. Class II General Controls and Special Controls

- With Exemptions
- Without Exemptions

3. Class III General Controls and Premarket Approval

Device classification depends on the intended use of the device and also upon indications for use. For example, a scalpel's intended use is to cut tissue. A subset of intended use arises when a more specialized indication is added in the device's labeling,

such as "for making incisions in the cornea." Indications for use can be found in the device's labeling but may also be conveyed orally during the sale of the product. [33]

In addition, classification is risk-based; that is, the risk the device poses to the patient and/or the user is a major factor in the class in which it is assigned. Class I includes devices with the lowest risk, and Class III includes those with the greatest risk. [33]

As indicated above, all classes of devices are subject to General Controls. General Controls are the baseline requirements of the Food, Drug, and Cosmetic (FD&C) Act that apply to all medical devices, Class I, II, and III. [33]

FDA has given Class II classification to Apple electrocardiograph software device for over-the-counter use. The ECG app is a software-only mobile medical application intended for use with the Apple Watch to create, record, store, transfer, and display a single-channel ECG. The ECG app determines the presence of AFib or sinus rhythm on a classifiable waveform. The ECG app is not recommended for users with other known arrhythmias. The ECG app is intended for over-the-counter (OTC) use. The ECG data displayed by the ECG app is intended for informational use only. The user is not intended to interpret or take clinical action based on the device output without the consultation of a qualified healthcare professional. The ECG waveform is meant to supplement rhythm classification for the purposes of discriminating AFib from normal sinus rhythm. It is not intended to replace traditional methods of diagnosis or treatment. [33]

In the EU, the ECG application is categorised into CE Class I.

5.2.2. European Union Medical Devices Regulations (EU MDR)

The EU MDR is also known as a Regulation (EU) 2017/745 on medical devices “Ensuring the safety and performance of medical devices”. In the EU, smartwatch or smartwatch applications have to be compliant with EU MDR in order to receive the classification. The CE sign, that marks the compliance with the needed law for the device, is timeless. But the technical documentation has to be updated by the manufacturers when needed. There is also the same directive under the name Regulation (EU) 2017/746 on medical devices, “on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU”. That directive

contains same legal paragraphs but the key difference is between the annexes VIII-XI. This directive is meant for the in vitro diagnostics devices, smartwatch is not in vitro device.

Medical devices are products or equipment intended for a medical purpose. In the European Union (EU), they must undergo a conformity assessment to demonstrate they meet legal requirements to ensure they are safe and perform as intended. They are regulated at the EU Member State level, but the European Medicines Agency (EMA) is involved in the regulatory process. [32]

Besides medical devices, the regulation also covers certain groups of products which do not have an intended medical purpose. These include colored contact lenses (i.e. lenses that do not correct vision) and liposuction equipment. Medical devices are classified according to their intended purpose and their inherent risks (classes I, IIa, IIb, and III). Smartwatches and their applications are also included. [32]

The regulation specifies what is required in the data collection of clinical investigations on medical devices. These include rules on informed consent and protecting vulnerable subjects (e.g. people under the age of 18).[32]

The medical device that has passed the assessment in Europe is marked with CE (Conformité Européenne) mark.

For the manufacturers to get the CE mark, they have to:

1. Identify applicable standards and regulations;
2. Verify the products requirements;
3. Identify if the conformity assessment needs to be done by an independent body;
4. Test the product and its conformity with the regulations;
5. Compile and update the technical documentation;
6. Affix the CE marking and compile the EU declaration of conformity; [34]

5.2.3. Guidance Document MEDDEV (Medical Devices)

MEDDEV is a guidance document, which means it is not legally binding. For the smart watch or the smart watch application, it is a document for step-by-step process on how to get to the point of being ready for EU MDR assessment. The purpose of this document is to define the criteria for the qualification of stand-alone software when used in the healthcare setting, as a medical device and the application of the classification criteria to such software. [35]

MEDDEV describes the qualification criteria as medical device as such:
Decision step 1: if the stand-alone software is a computer program, then it may be a medical device. If the software is not a computer program, then it is a digital document and, therefore, not a medical device. Examples of computer programs are software applications, macros, scripts, dynamically linked libraries, batch files, style sheets, and any document containing active formatting or filtering instructions.[36] With the ECG example, the application categorises as a software application that may categorise as a medical device.[36]

Decision step 2: If the software is incorporated into a medical device rather than stand alone software, it must be considered part of that medical device in the regulatory process of that device. [36]

Decision step 3: if the software does not perform an action on data or performs an action limited to storage, archival, communication, ‘simple search’, or lossless compression, it is not a medical device. Altering the representation of data for embellishment purposes does not make the software a medical device. In other cases, including where the software alters the representation of data for a medical purpose, it could be a medical device. [36]

Software that is intended to create or modify medical information might be qualified as a medical device. If such alterations are made to facilitate the perceptual and/or interpretative tasks performed by the healthcare professionals when reviewing medical information, (e.g. when searching the image for findings that support a clinical

hypothesis as to the diagnosis or evolution of therapy) the software could be a medical device. [36]

Decision step 4: an example of software for the benefit of individual patients is software intended to be used for the evaluation of patient data to support or influence the medical care provided to that patient. [36]

Decision step 5: if the software is an accessory to a medical device, it is not a medical device. The legal definition of 'putting into service' requires that a device is made available to the final user/operator as being ready for use on the Community market.[36]

5.2.4. General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a privacy and security law. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018. The GDPR will give fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros. [37] There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages.

Personal data — Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data. Pseudonymous data can also fall under the definition if it’s relatively easy to ID someone from it. [37]

Data processing — Any action performed on data, whether automated or manual. The examples cited in the text include collecting, recording, organizing, structuring, storing, using, and erasing.[37]

Data subject — The person whose data is processed. These are, for example, customers or site visitors.[37]

Data controller — The person who decides why and how personal data will be processed.[37]

Data processor — A third party that processes personal data on behalf of a data controller. The GDPR has special rules for these individuals and organizations. [37]

Medical devices handle sensitive data, which requires explicit agreement from the data subject. This also applies to the smartwatch manufacturers and software applications that operate within EU borders or handle EU citizens' data. Because in many cases, the data is not stored locally in the country (e.g if the user is in Estonia and using Apple Watch, it does not mean that the data is stored in Estonia), Article 44 about general principle of data transfer and article 9 about the processing of special categories of personal data applies.

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation can happen only if the other party is compliant with the GDPR standards. This also applies to the controller and processor, including the case when the data is then yet forwarded to another organization or third country.[38]

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the receiving party in question ensures an adequate level of protection. [39]

5.3. Conclusion

It is important to tell the difference between consumer products that could be used for basic everyday health overviews and medical devices that are used for diagnosing, preventing, or assisting guidance to doctors. The difference is that consumer products may not collect the same signals as traditional medical devices. For example, a medical-grade ECG monitor is used to monitor and display heart rate and cardiac waveforms in a clinical setting via a series of electrodes that collect and interpret electrical signals directly from the heart. In contrast, a consumer fitness tracker that reads and displays heart rate is really collecting the pulse rate using an electronic sensor embedded in a wristband. The fitness tracker may not be FDA/EU MDR cleared to

diagnose specific cardiac conditions that the medical-grade ECG monitor is cleared for. [22]

Consumer products may not fulfill their marketing claims. While the devices can be marketed as a source for accurate health data overview, the patients must be aware of the risks of false negatives and false positives. Risks from false negatives include a false sense of security, leading patients to avoid necessary care, whereas false positives can lead patients to seek unnecessary care. There is little evidence on the reliability and accuracy of data obtained from certain unregulated consumer-grade products, which may not function as intended. In addition, the ability of consumer products to fulfill the expectancy of the consumers relies at least in part on a user entering and updating their own data—a requirement that leaves the products vulnerable to data entry errors. Missing or incorrect data can confuse users, impede care, and waste the patient's and physicians' time.[22] More often than not, clear warning signs from the manufacturer may be missing that inform the end user about the products' unsuitability as the sole source of diagnosis. That may result in the consumer ignoring the requirement for medical attention or, the opposite, encouraging hypochondriac behaviour.

Answering Rq 1. "What legislations must manufacturers follow in order to categorize the smart wearable as a medical device in Estonia" the legislations that must be followed apply to every nation in the EU. Estonia is no different, legislation that is in force regarding the classification and use of medical devices is EU MDR. For the smart watch to be categorized as a medical device in the EU, the manufacturer must follow the regulation of EU MDR and GDPR. GDPR is important in regards of the data safety. EU MEDDEV is used as a guidance document to get to the point of being ready for assessment.

5.4. 5G

Smart continuous eHealth monitoring using 5G is a transformative approach to healthcare that leverages the capabilities of fifth-generation (5G) wireless technology to provide real-time, remote, and continuous monitoring of patients' health conditions. This approach offers numerous benefits, including better patient care, less healthcare costs, and improved accessibility to healthcare facilities. [40] 5G is used to provide a single seamless architecture. Because health data is sensitive, according to the GDPR,

extra steps must be taken to provide CIA (Confidentiality, Integrity, and Accessibility) to the data that is transferred between the parties. In this section, author analyses the 5G as a core network and a solution to the privacy concerns regarding sensitive data flow.

5G radio represents a major step in mobile network capabilities. Up to now, mobile networks have mainly provided connectivity for smartphones, tablets, and laptops for consumers. 5G will take traditional mobile broadband to new heights in terms of data rates, capacity, and availability. In addition, 5G will enable new services, including industrial IoT connectivity and critical communication. 5G targets are set very high with data rates up to 20 Gbps and capacity increases of up to 1000 times with flexible platforms for device connectivity, low latency, and high reliability. A number of new use cases and applications can be run on top of 5G mobile networks. [41] It is estimated that in the year 2025, there will be over 1 billion 5G connections, and in the year 2030 over 25,44 billion IoT devices. [42]

In the traditional mobile network, the data transmission path is from the base station (BS) through the transmission network to the core cloud and then to the application servers located on the Internet. As a result, the latency of the service can not be well controlled, the data security is threatened, and the reliability and stability of the service can not be guaranteed. That could mean, that the conformity with the GDPR is not guaranteed. On the other hand, 5G MEC (Multi-access edge computing) moves the core cloud's data plane as close to subscribers as possible. [43]

5G has the potential to improve eHealth as it is not only quicker and more stable than previous generations but also gives the possibility of using network capacities more extensively. One benefit of 5G for eHealth is the improved possibility of at-home monitoring of patients with chronic illnesses, enabling the continuous observation of patient health by doctors.[40] This would improve the patient's quality of life and reduce costs, as there would be less need for hospitalisations and the patient can monitor their health in the comfort of their own home.

5G introduces a new range of technologies in order to achieve the goals. In Figure 5, all the new key technologies are highlighted.

- New spectrum. 5G is the first mobile radio technology that is designed to operate on any frequency band between 400 MHz and 90 GHz. The low bands are needed for coverage and the high bands for high data rates and capacity. [41]
- Massive Multiple Input Multiple Output (MIMO) beamforming can increase spectral efficiency and network coverage substantially. Beamforming is more practical at higher frequencies because the antenna size is comparable to the wavelength, and the antenna size becomes smaller at higher frequencies. In practice, massive MIMO can be utilized at frequencies above 1 GHz in the base stations and at millimeter wave even in the devices. [41]
- Network slicing. It will create virtual network segments for the different services within the same 5G network. This slicing capability allows operators to support different use cases and enterprise customers without having to build dedicated networks.[41]
- Dual connectivity and Long-Term Evolution (LTE) coexistence. 5G can be deployed as a stand-alone system, but more typically, 5G will be deployed together with LTE in the early phase. A 5G device can have simultaneous radio connections to 5G and to LTE. Dual connectivity can make the introduction of 5G simpler, increase the user data rate, and improve reliability. 5G is also designed for LTE coexistence, which makes spectrum sharing feasible and simplifies spectrum refarming.[41]
- Support for cloud implementation and edge computing. The current architecture in LTE networks is fully distributed in the radio and fully centralized in the core network. The low latency requires the content to be brought close to the radio, which leads to local breakout and edge computing. Scalability requires the cloud benefits to be brought to the radio networks with edge cloud architecture. 5G radio and core networks are specified for native cloud implementation, including new interfaces inside the radio network.[41]

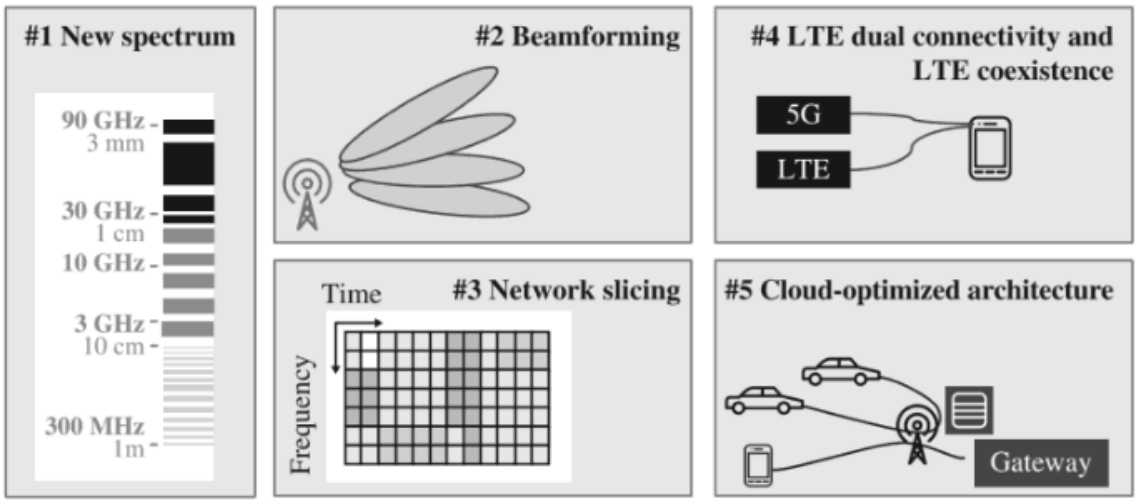

Figure 5. Key 5G technology components [41]

5.4.1. Current Situation in Estonia

5G, as a prerequisite, needs a fully built 4G network, in Estonia 4G is available to 96% of the population. [42] Telia has opened about 450 5G support stations, and Elisa has covered over half of the Estonian population currently. The first 5G network was opened by Telia in 2020.

5.4.2. Wi-Fi 6 vs 5G

Wi-fi 6 and 5G are different in their technology types. 5G is a cellular technology that uses base stations, small cells, and radio signals to transfer data and provide connectivity to end-user devices. 5G typically covers a large geographic area. Wi-Fi is a wireless local area network (LAN) technology that uses routers, access points, and radio signals to connect devices in a limited range.[44]

Cellular technology is carrier-based, which is also true for 5G technology. This means operators run cellular networks on licensed spectrum bands, which exist to prevent interference between connected devices. In contrast, Wi-Fi operates in unlicensed bands that don't require permission to use. 5G, in difference from other generations, supports both, unlicensed and licensed broadbands.[44]

5G operators use different frequency bands for their mobile networks, such as 600 MHz, 800 MHz and millimeter wave, which operates between 30 GHz and 300 GHz.

Meanwhile, Wi-Fi 6 operates in unlicensed spectrum at 2.4 GHz and 5 GHz. Wi-Fi 6E, an extension of Wi-Fi 6, operates at 6 GHz.[44]

While Wi-Fi technology's unlicensed bands don't require permission to use, access to the Wi-Fi network itself does. Users typically require a service set identifier/network name and password to access a Wi-Fi network. In addition, Wi-Fi 6 introduces a new authentication type called Simultaneous Authentication of Equals for added protection against bad actors.[44] Cellular networks don't have the same authentication requirements as Wi-Fi networks, so it's simple and easy for connected devices to gain access. However, 5G also uses several authentication types, which include 5G Authentication and Key Agreement, Extensible Authentication Protocol-AKA and EAP-Transport Layer Security to bolster 5G network security. [44]

5G New Radio (NR) is designed specifically to co-exist with the LTE to utilize existing cellular structure and enhances overall network performance by reduced interference, low latency, usage of beamforming and multiple antennae. [45] With that in mind, the 5G network would be used with other networks. Since smartwatches do not provide a connection with 5G yet, using wi-fi and bluetooth connections, the smartwatch is tethered through the phone with 5G network.

5.4.3. Radio Access Network

The Radio Access Network is the portion of the network that connects the user device to the core network.

The traditional radio access network consists of 3 major components. The baseband, which provides a set of computer-intensive signal processing functions that makes wireless communication possible. To enable the high computational power required, the baseband uses tailor-made electronics that delivers high data processing speeds. To realize the full potential, it also houses software with several million lines of code to provide efficient wireless communication that constantly pushes the boundaries of efficient and secure use of spectrum. [46]

The radio which converts digital information into signals that can be transmitted wirelessly and that ensures that the transmitted signals are in the right frequency bands and have the right power levels. [46]

In healthcare, there is an increase in the number of gadgets and technologies that offer better, more efficient services, transforming healthcare facilities into smart hospitals. 5G provides seamless connectivity, eliminating the need to move between in-building Wi-Fi and mobile networks, and enables the merging of several incompatible IoT radio networks into a single network. [46] Using one network system within the medical ecosystem simplifies the configuration and management of the network and devices.

A 5G network with low latency and bigger bandwidth can speed up the entire healthcare process. Patients can use specialized devices to monitor their health from the comfort of their homes and still be connected to the healthcare provider. Sensors in these specialised gadgets will generate data. Healthcare experts can send and analyse these sensors to better access and treat data. Paramedics may transfer patient data immediately from the ambulance and link an experienced professional to give emergency care online using 5G. Furthermore, continuous remote patient monitoring will allow people with chronic conditions to call doctors as soon as possible. Doctors will be able to check the status of their patients no matter where they are. [46] Using smart wearables within the hospital or at home, with the use of 5G, would mean faster data transportation, opportunity to transfer massive amounts of data together. Within the medical context, that could mean the elimination of data congestion.

5.4.4. Core network

The core has been the basis of the network since the early days of the telephone when it served as the manual switching board, allowing operators to route calls to where they needed to go. [47] Many people are simultaneously accessing their mobile network to watch Netflix, listen to iTunes, book holidays, access banking, play games and more over their smart devices. Adding to that, the growing number of industrial devices that are interacting with the network. [47]

The core manages all of this. It is the network intelligence that provides traffic handling, as well as billing, location and security, ensuring that services are only accessed by the

people and devices that have permission to do so and that they are accurately billed for what they use. [47]

In addition to enhanced mobile broadband features such as faster data rates – 5G delivers speeds that are 1,000 times faster than 2G - the 5G core is more flexible, dynamic and open. [47] Some of the basic and crucial functions that the core network offers are authentication and authorisation and to maintain the location of the users so that services can be delivered to them. [48]

As 5G system architecture has to support use cases like virtual-reality (VR), real time operations, and use cases like smart health, smart transportation and smart cities, which all have varied requirements from the network, several concepts have been introduced into design of the 5G Core. Further, as scalability and protection of investment in equipment have gained in importance, softwarisation of the network has also increased. [48] Therefore the 5G core network is aimed to be:

a) Flexible: 5G Core should be able to flexibly add new services and configure the network on a shared infrastructure. [48]

b) Agile: The 5G Core should shorten the service implementation time from hours to minutes and delivers faster time-to-market (TTM) for new services from months to days. [48]

c) Scalable: 5G Core should be scalable rapidly and highly with telco-grade reliability. [48]

d) Tunable: 5G Core should be able to quickly adapt and optimise the network according to operating conditions. It should also support cost-efficient migration from 4G to 5G based on access agnostic common core. [48]

To achieve these aims, the key 5GC design principles are:

a. Network slicing: This feature enables independent scalability and decoupled technical evolution and flexible deployments & configuration of the network as per the needs of the different services. [48]

b. Modular function design: This is a form of functional disaggregation such that a function composed of multiple modules can be created according to the use case's requirements. [48]

c. Unified authentication framework : This is useful in multi-access core, for efficiency and to enable operators to offer "follow-the-user" services, independently of access method. [48]

d. “Stateless" network functions: With this feature, the "compute" resource is decoupled from the "storage" resource. This concept is derived from cloud applications. It enables much more efficient creation and consumption of network resources. [48]

e. Support for cloud native applications: This is further step from NFV (Network Function Virtualisation) and improves the scalability and efficient creation and consumption of network resources. [48]

f. Network capability exposure: Exposing information about the network's capabilities to internal and external applications is very important where operators want to integrate 5G with vertical industry processes. Standardizing this interface makes integration easier for vertical customers, especially those with international operations and multi-operator relationships. [48]

g. Support for mobile edge computing: This is to support access to low- latency services hosted in local data centres. Typically, user-plane functions might be deployed remotely i.e. near to the user, while the control plane is centralized. In very low-latency, mission-critical applications, the control plane may also be distributed.[48]

5.4.5. Software-defined network

At the highest level each element in traditional communication network handles two main tasks. Functions in the user plane (UP) forward traffic from one network element to another, for example by the use of routing tables, while those in the control plane (CP) carry out higher-level tasks such as configuring the routing tables and managing the network's resources. Once again, that approach is perfectly satisfactory, but has several limitations: the decision-making processes are distributed over the entire network, which makes the control plane unnecessarily complex, while those complexities limit how far the operator can distribute the functions in the UP.[49]

The central feature of software-defined networking (SDN) is a clear separation between the control and UPs. In a SDN, the control plane functions can be centralized, which allows for simpler, more integrated control over the network. Once centralized, those functions can easily communicate with authorized third-party application servers over a so-called northbound application programming interface (API), through which those servers can influence or control the network's operation. The third-part servers do not know any details of the network's physical implementation, as those are confined to the southbound API, through which the control plane functions configure the ones in the UP. In turn, the UP functions can be distributed to whichever physical locations are desired, without the constraints that the control plane previously imposed.[49]

5G has been designed with SDN in mind from the beginning. SDN can be applied to the radio access network as well as the core. Multi-access edge computing (MEC), also known as mobile edge computing, is a technology in which the UP connection to an external network is implemented close to the cell site, or even at the cell site itself. By shortening the communication path, the architecture provides the mobile with low-latency access to external servers to help support the most demanding forms of low-latency applications. Furthermore, if the UP function is implemented in software by means of NFV, then it can be relocated dynamically, for example, if the mobile starts running a low-latency service or if it subsequently changes cell. [49]

5.4.6. Network slicing

Network slicing is a technique that creates multiple virtual networks on top of a shared physical network to provide greater flexibility in the use and allocation of network

resources. For 5G, the network slicing is a fundamental feature. For 4G and older generations of cellular data services, it is not supported. [50]

Certain applications of devices can have detrimental modelling influence on what the 5G is going to become in terms of infrastructural display. For example, a wearable device (i.e. a smartwatch) will have a different purpose for a doctor issuing it to a patient as a monitoring device rather than a wearable for an individual casually monitoring his heartbeat during sports activity. Thereby, the same device, which will become part of a certain IoT network, will need a specific environment to which it will perform the activity it is envisioned for. Consequently, the privacy level is not very important for the person monitoring his heartbeat, whereas for preserving the doctor-patient confidentiality, it will be of utmost importance. Thus, in 5G the concept of network slicing is introduced, a novel approach for stipulating network segments, acclimatizing them to the conditions of the situation: different security levels, diverse network performance, various latency, distinct reliability, etc. One phone attached to two divergent network slices will experience two different performance levels, as well as access to different services. [51]

The end-to-end architecture of 5G network slicing enables network operators to create and manage network slices that are customized to meet the specific needs of different applications and users.[52]

Network slicing enables flexibility, simplicity, and performance customized to specific and demanding use case requirements to a degree that was not achievable in earlier generations of wireless. It also enhances the security of networks by isolating traffic between slices to enable tailored integrity enhancements. With network slicing, Communications Service Providers (CSPs) are able to provide optimized, end-user-specific connectivity services to industries and consumers to meet the demand for differentiated services while simultaneously maintaining a high-quality broadband internet experience for all users.[53]

5.5. Conclusion

5G data rates are up to 20 Gbps, and capacity could be increased up to 1000 times with flexible platforms for device connectivity, ultra-low latency, and high reliability. Those are topics that are crucial for medical institutions when it comes to remote monitoring of patients. Ultra-low latency assures that the data is being transported as fast as possible to the healthcare provider and higher broadband increases the possibilities to send massive amounts of data between the parties. When sensitive health data is at transfer, it increases the risk of attacks and spying. Using network slicing and local breakout could increase the safety of sensitive data transportation. Network slicing not only allows the institution and the user to support different use cases, frequency bands, and improves the use of energy and efficiency, but it also could improve the security of sensitive data transfer paths. With network slicing, it is possible to isolate sensitive data slices from basic data traffic slices.

Traditional mobile networks transport data from the BS through the transmission network to the core cloud and then to the application servers located on the Internet. This means that the data path is not controlled. 5G MEC, on the other hand, moves the data plane of the core cloud as close to subscribers as possible with the use of local breakout.[43] Local breakout spots could be mounted into patients' own homes or be used inside the hospital, which eliminates the need to use local network cells to transport sensitive health data and avoids unnecessary data traffic to different areas.

Since many smartwatches that are on the market today do not support the 5G connection, the 5G is used in coexistence with LTE and Wi-fi 6. The future goal would be to use an exclusively 5G core network to minimise the traffic between different types of networks and make the system more manageable.

To answer the Rq 2. “Benefits and risks of using 5G core network as a solution to secure data flow” 5G could be useful as a core network. Using local breakout and network slicing supports data sovereignty in the case that data is travelling through the user's preferred path.

5.6. Future Work and Limitations

The limitation is that the smart wearables do not support the 5G network connection, so there is no way to test the 5G architecture on smartwatches. There is also limited research on the topic of how accurately the smartwatch sensor collects data. Limitations also include the non-existence of the possibility to opt out of the choice that smartwatch collected data is not going to be collected by the manufacturer.

The topic for future works could include the exploration of possibilities on how to completely eliminate the data transfer that is collected through the smartwatch to the manufacturer. Right now, there is no possibility of eliminating manufacturers' data collection services from smartwatches.

Possible future studies could also explore architectures on how to incorporate 5G into Estonia's healthcare. The topic is broad and offers a lot of possibilities for combining the healthcare and consumer wearables topic. The Estonian healthcare sector is showing a bit of resistance towards using consumer wearables in medical settings. Could this be overcome if more manufacturers would pursue the categorization of their devices, like Apple watch and Samsung have class I categorization.

6.Summary

Smartwatches offer us many possibilities to keep an eye on our everyday health. Combining everyday wearables and the medical field could help with patients' remote monitoring, help physicians get a more in-depth view of the patients' health data, and offer faster assistance. With the convergence, it is important to know the legislative ecosystem.

The legal framework governing the classification of consumer devices is primarily derived from EU law in Estonia. If the smartwatch manufacturer wants to get medical device classification in Estonia, they must follow the European Medical Device Regulation. If the device handles data, then the General Data Protection Rule applies also. As of today, the Apple Watch and Samsung Smartwatch have received the United States Food & Drug Administration medical device classification. Apple Watch has received class II from the FDA and EU MDR class I categorization for the electrocardiography app that detects early atrial fibrillation. Samsung Smartwatch has received FDA De Novo classification for their sleep apnea feature on Galaxy Watch. Since Samsung, Apple, and Fitbit smartwatch servers are located in different countries, and all the data processing is done outside the smartwatch device, the sensitive data transfer privacy comes into question. In that topic, a 5G Core network was suggested as a possibility to enhance sensitive data flow. 5G Core offers the possibility of local breakout and network slicing. Local breakout spots could be mounted into patients' own homes or be used inside the hospital, which eliminates the need to use local network cells to transport sensitive health data and avoids unnecessary data traffic to different areas. Network slicing enhances the security of networks by isolating traffic between slices to enable tailored integrity enhancements. With both of those combined, the data flow would be more easily controlled, managed, and private. In conclusion, while the thesis shows the data flow of popular smartwatch brands, highlights the legal ecosystem, and offers the 5G Core as a solution, it also brings out the need for further research.

References

[1] Q. Tao, S. Liu, J. Zhang, J. Jiang, Z. Jin, Y. Huang, X. Liu, S. Lin, X. Zeng, X. Li, G. Tao and H. Chen, “Clinical applications of smart wearable sensors”, iScience, vol 26, no. 9,2023, 107485, ISSN 2589-0042, https://doi.org/10.1016/j.isci.2023.107485. <https://www.sciencedirect.com/science/article/pii/S2589004223015626>

[2] L. Lu, J. Zhang, Y. Xie, X. Gao, S. Xu, X. Wu, Z. Ye, “Wearable Health Devices in Health Care: Narrative Systematic Review”, JMIR Mhealth Uhealth, vol 8, no. 11, 2020, 18907
doi: 10.2196/18907, <https://mhealth.jmir.org/2020/11/e18907/ >

[3] F. Laricchia, “Number of connected wearable devices worldwide from 2019 - 2022”, Statista.com, Accessed: Dec, 10, 2023. [Online] Available: https://www.statista.com/statistics/487291/global-connected-wearable-devices/’

[4] S. Tian, W. Yang, J. M. Le Grange, P. Wang, W. Huang, Z. Ye,”Smart healthcare: making medical care more intelligent”, Global Health Journal, vol 3, no. 3, 2019, ISSN 2414-6447, doi: https://doi.org/10.1016/j.glohj.2019.07.001.

[5] Watch Comparison, Accessed: Mar, 22, 2024. [Online] Available: https://www.apple.com/watch/compare/

[6] S. Mahalingaiah,V. Fruh, E. Rodriguez,SC. Konanki, JP. Onnela, et al, “Design and methods of the Apple Women's Health Study: a digital longitudinal cohort study”, Am J Obstet Gynecol,vol 226 no.4,2022, doi: 10.1016/j.ajog.2021.09.041. https://pubmed.ncbi.nlm.nih.gov/34610322/

[7] ”Fitbit Products”, Accessed: Mar, 22, 2024, [Online]. Available: https://www.fitbit.com/global/us/products

[8] Mordor Intelligence, “European Smartwatch Market Size & Share Analysis”, Accessed Mar, 28, 2024, [Online]. Available: https://www.mordorintelligence.com/industry-reports/europe-smart-watches-market

[9] Watch Comparison Footnotes, Accessed: Mar, 22, 2024. [Online] Available: https://www.apple.com/watch/compare/#footnote-5

[10] Apple, “Health App & Privacy”, Accessed May, 03, 2024, [Online]. Available:https://www.apple.com/legal/privacy/data/en/health-app/

[11] O. Afonin, “Extracting Apple Health Data from iCloud”, blog.elcomsoft.com, Nov. 2018. [Online]. Available: https://blog.elcomsoft.com/2018/11/extracting-apple-health-data-from-icloud/

[12] Apple, “Apple Privacy Policy”, Accessed May, 03, 2024, [Online]. Available: https://www.apple.com/legal/privacy/en-ww/

[13] J. Williams, “Empowering people to live a healthier day Innovation using Apple technology to support personal health, research, and care”, Apple Inc, July 2022, Updated October 2023. [Online]. Available: https://www.apple.com/newsroom/pdfs/Health-Report-October-2023.pdf

[14] “Võrdle nutikellasid”, Accessed: Mar, 22, 2024, [Online]. Available: https://www.samsung.com/ee/watches/compare/?product1=sm-r925fzkaeue&product2=sm-r910nzaaeue&product3=sm-r920nzkaeue

[15] M.H Jung, K. Namkoong, Y. Lee, et al. “Wrist-wearable bioelectrical impedance analyzer with miniature electrodes for daily obesity management”. Scientific Reports, vol 11, no. 1238 ,2021. https://doi.org/10.1038/s41598-020-79667-3 https://www.nature.com/articles/s41598-020-79667-3

[16] Samsung, “Security and Privacy”, Accessed May, 03, 2024, [Online]. Available: https://www.samsung.com/ee/sustainability/security-and-privacy/privacy/

[17] Samsung, “Samsung Konto Privaatsusteade”, Accessed May, 03, 2024, [Online]. Available: https://policies.account.samsung.com/terms?appKey=j5p7ll8g33&type=PN&applicationRegion=EST&language=eng&region=USA&darkMode=true&rtl=false

[18] Samsung, “Samsungs’ Privacy Policy”, Accessed May, 03, 2024, [Online]. Available: https://privacy.samsung.com/privacy/samsung

[19] FitBit, “Heart Rate”, Accessed: Mar, 28, 2024, [Online]. Available: https://www.fitbit.com/global/us/technology/heart-rate

[20] B. Cyr, W. Horn, D. Miao, M. Specter, “Security Analysis of Wearable Fitness Devices (Fitbit)”, Massachusetts Institute of Technology Cambridge, Massachusetts,

2015, Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/03/20082016/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf

[21] J. Willemson & A. Ansper, “A Secure and Scalable Infrasturcture for Inter-Organizational Data Exchaange and eGovernment Applications”, Available: https://research.cyber.ee/~janwil/publ/xroadares07final.pdf

[22] ECRI, “The Growing Use of Consumer-Grade Medical Devices: Advice for Physicians and Their Patients”, Accessed: Apr, 7, 2024. [Online], Available: https://www.ecri.org/components/HDJournal/Pages/Advice-on-consumer-grade-medical-devices.aspx?tab=2

[23] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, K. Mankodiya, “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare”, Future Generation Computer Systems,vol 78, no. 2, 2018, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.04.036 Available: https://www.sciencedirect.com/science/article/pii/S0167739X17307677

[24] World Health Organization, “Medical Devices”, Accessed: Apr, 7 , 2024. [Online]. Available: https://www.who.int/health-topics/medical-devices#tab=tab_1https://www.who.int/health-topics/medical-devices#tab=tab_1

[25] M. V. Perez, K. W. Mahaffey, H. Hedlin, J. S. Rumsfeld, et al,”Large-Scale Assessment of a Smartwatch to Identify Atrial Fibrillation”, journal of Medicine, vol 381, no. 20, 2019, doi: 10.1056/NEJMoa1901183https://www.nejm.org/doi/10.1056/NEJMoa1901183?url_ver=Z39.88-2003&rfr_id=ori:rid:crossref.org&rfr_dat=cr_pub%20%200pubmed

[26] S. H. Browne, F. Vaida,, A. Umlauf, J. Kim,P. DeYoung, R. L. Owens,”Performance of a commercial smart watch compared to polysomnography reference for overnight continuous oximetry measurement and sleep apnea evaluation”, Journal of Clinical Sleep Medicine, 23. April 2024, doi: https://doi.org/10.5664/jcsm.11178 [Online], Available: https://jcsm.aasm.org/doi/pdf/10.5664/jcsm.11178

[27] U.S Food and Drug Administration, “De Novo Classification Request”, Accessed May, 05, 2024 [Online], Available: https://www.fda.gov/medical-devices/premarket-submissions-selecting-and-preparing-correct-submission/de-novo-classification-request

[28] P. Clarke, “Major privacy breach in the misuse of personal information used by HealthEngine”, peterclarke.com.au. Accessed: Mar, 18, 2024. [Online]. Available: http://www.peteraclarke.com.au/2018/06/25/major-privacy-breach-in-the-misuse-of-personal-information-used-by-healthengine/

[29] P. Maluga, “HealthEngine may be in breach of privacy law in sharing patient data”, The Conversation, June, 2018. [Online]. Available: https://research-management.mq.edu.au/ws/portalfiles/portal/105587956/Publisher_version.pdf

[30] D. Ribeiro, “Consumer-Grade Versus Medical Devices: Where Do Paths Intersect And The Lines Blur?” ,Life Science Academy, Accessed: Apr, 2, 2024. [Online]. Available: https://lsacademy.com/en/consumer-grade-versus-medical-devices-where-do-paths-intersect-and-the-lines-blur/

[31] U.S Food and Drug Administration, “Classify Your Medical Device”, Accessed: Apr 2, 2024, [Online]. Available:https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device

[32] European Medicine Agency, “Medical Devices”, Accessed: Apr, 3, 2024, [Online]. Available: https://www.ema.europa.eu/en/human-regulatory-overview/medical-devices

[33] U.S Food and Drug Administration, “De Novo Classification Request for ECG App”, Date of De Novo: Aug, 2018. Accessed: Mar, 3, 2024. [Online], Available: https://www.accessdata.fda.gov/cdrh_docs/reviews/DEN180044.pdf

[34] European Comission, “CE Marking”, Accessed: May, 05, 2024, [Online]. Available: https://single-market-economy.ec.europa.eu/single-market/ce-marking/manufacturers_en?prefLang=de

[35] European Commission, “MEDDEV Guidance List”, Accessed Mar, 28, 2024, [Online]. Available: https://www.medical-device-regulation.eu/meddev-guidance-list-download/

[36] European Commission, “Medical Devices: Guidance Document”, Accessed: Apr: 7, 2024. [Online]. Available: http://www.meddev.info/_documents/2_1_6_ol_en.pdf

[37] GDPR.eu, “What is GDPR”, Accessed Mar, 28, 2024, [Online]. Available: https://gdpr.eu/what-is-gdpr/

[38] GDPR Info, “Art. 44 GDPR General principle for transfers”, Accessed Mar, 28, 2024, [Online]. Available:https://gdpr-info.eu/art-44-gdpr/

[39] GDPR Info, “Art. 45 GDPR Transfers on the basis of an adequacy decision”, Accessed Mar, 28, 2024, [Online]. Available:https://gdpr-info.eu/art-45-gdpr/

[40] D. Manimegalai ,M. Karthikeyan, "Exploring the Impact of 5G and the Promise of 6G: Transforming Healthcare Strategies and Technology," 2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), 2023, pp. 1-8, doi: 10.1109/RMKMATE59243.2023.10368780. Accessed Mar, 28, 2024, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10368780

[41] H. Holma and A. Toskala, “5G Technology: 3GPP new radio”, First ed, Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd., 2020, pp. 1- 13, [Online]. Available: https://books.google.ee/books?id=V2s0jgEACAAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false

[42] 5G Eestis, Accessed: Mar, 30, 2024. [Online] Available: https://5geestis.ee/

[43] L. -C. Kao and W. Liao, "5G Intelligent A+: A Pioneer Multi-Access Edge Computing Solution for 5G Private Networks," in IEEE Communications Standards Magazine, vol. 5, no. 1, pp. 78-84, March 2021, doi: 10.1109/MCOMSTD.001.2000036 Available: https://ieeexplore.ieee.org/abstract/document/9392781

[44] TechTarget, “A Deep Dive into the Differences Between 5G and Wifi 6”, Accessed Mar, 28, 2024, [Online].

Available:https://www.techtarget.com/searchnetworking/feature/A-deep-dive-into-the-differences-between-5G-and-Wi-Fi-6

[45] A. M. Nidhi and R. Prasad, "Overview of 5G New Radio and Carrier Aggregation: 5G and Beyond Networks," *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)*, Okayama, Japan, 2020, pp. 1-6, doi: 10.1109/WPMC50192.2020.9309496 [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9309496

[46] Ericsson, "5 Key Facts About 5G radio access networks", Accessed May, 03, 2024. [Online]. Available: https://www.ericsson.com/en/public-policy-and-government-affairs/5-key-facts-about-5g-radio-access-networks

[47] Nokia, "5G Core Explained", Accessed May, 03, 2024, [Online]. Available: https://www.nokia.com/about-us/newsroom/articles/5g-core-explained/

[48] Telecommunication Engineering Centre, "5G Core Network", Study Paper, Accessed May, 03, 2024. [Online]. Available: https://www.tec.gov.in/public/pdf/Studypaper/5G%20Core%20Network_Study%20Paper_v8.pdf

[49] C. Cox, "An Introduction to 5G", Chichester, West Sussex, United Kingdom: John Wiley & Sons Ltd., 2021 pp. 4,7,11. [Online]. Available: https://books.google.ee/books?hl=en&lr=&id=w0fxEAAAQBAJ&oi=fnd&pg=PR21&dq=%225g+new+radio%22&ots=VAGBZhEHQO&sig=qZotwUXSn-zXZgHlA5FydtYb4XA&redir_esc=y#v=onepage&q&f=false

[50] Tech Target, "Network Slicing", Accessed Mar, 28, 2024, [Online]. Available: https://www.techtarget.com/whatis/definition/network-slicing

[51] B. Dzogovic, V. T. Do, B. et al, "Secure Healthcare: 5G-enabled Network Slicing for Elderly Care," 2020 5th International Conference on Computer and Communication Systems (ICCCS), 2020, pp. 864-868, doi: 10.1109/ICCCS49078.2020.9118583. Accessed Mar, 28, 2024, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9118583

[52] X. Li, M. He and J. Ni, “Secure and Privacy-preserving Network Slicing in 3GPP 5G System Architecture”, Accessed May, 03, 2024. [Online]. Available: https://arxiv.org/pdf/2305.17524

[53] Ericsson, “Network Slicing for 5G Success”, Accessed May, 03, 2024. [Online]. Available:https://www.ericsson.com/en/blog/2023/10/network-slicing-for-5g-success

Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I, Britta Sillaots

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis , supervised by Dr. Matthew James Sorell and co-supervised by Aleksi Oskar Johannes Kajander,
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

1 The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.