□ Copie Juré
□ Copie Conseiller
□ Copie Infothèque

h e g

Haute école de gestion
Genève

How does the collection and use of private data slow down the development of eHealth solutions and which are the recommendations that can speed up innovation of eHealth solutions?

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Antonio Joao SCHUHMANN DOS SANTOS

Conseiller au travail de Bachelor :

Marc-André EGGIMANN, PhD.

Carouge, 17 Août 2018

Haute École de Gestion de Genève (HEG-GE)

Filière économie d'entreprise

Hes·so// GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l’examen final de la Haute école de gestion de Genève, en vue de l’obtention du titre de Bachelor of Science en économie d’entreprise < … >.

L’étudiant a envoyé ce document par email à l'adresse d'analyse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND. http://www.urkund.com/fr/student/392-urkund-faq

L’étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J’atteste avoir réalisé seul< e > le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 17 Août 2018

Antonio Schuhmann dos Santos

Antonio

Acknowledgements

I would like to particularly thank and express my gratitude to my advisor Mr. Marc-Andre Eggimann for the precious help and advice provided during the whole research.

I would like to thank Mr. Pierre-Mikael Legris, Mrs. Evelina Georgieva and Pryv's staff for the time spent to introduce me to the complex but interesting health sector.

I would like to also thank all persons and speakers I have met during the eCom and STIB conferences. Their testimonies were helpful to understand the key challenges and role of data in the modern society.

I would also like to thank Ms. Fleur Hohenhim, Ms. Luce Sandfort, Ms. Lysberth Wouters and Mr. Vincent Sandfort for the time spent to read and correct the present Bachelor thesis.

Finally, I would also like to thank my whole family and friends who provided a warm support all along the research.

Executive summary

The concept of eHealth was created in the late 1990s to automate and optimise healthcare. Even though various eHealth technologies exist nowadays, only some of them are available to consumers, while similar technologies are actually being used in other industries, such as the transportation industry. The aim of this paper is to understand how personal data can impact the development of eHealth solutions in Europe, by doing literature research and giving recommendations.

The role of computers and data has changed since the 1930s, moving from the first large digital computer in 1939 to the current mobile connected devices that are able to process lots and lots of information in real time. In the past, stored data was difficult to access and use, while nowadays, people can easily access to all kinds of data anywhere and anytime. Not only the role of computers and data has changed, but also the healthcare sector. Today, healthcare workers can provide people with better healthcare by using new technologies, such as eHealth. EHealth automates and optimises medical services and tasks and improves the sharing of medical information.

Nowadays, the healthcare sector faces many challenges regarding personal data. First of all, there is so much data that especially large companies do not even know how their data is being used and by whom. Secondly, cybercriminals have been stealing more and more personal data. Starting from 2017, the healthcare sector has become their main target, since health data is more valuable than credit card data. Next to this, consumers trust medical companies less to handle their personal data with care. Finally, new regulations force life science companies to be accountable for tracking personal data, which is very complicated due to the large amount of data.

To accelerate the innovation speed of eHealth solutions, several steps can be taken. By handing out labels and giving certifications, medical solution makers do not have to prove the safety of their products anymore. Also, research on treatments, devices and drugs can be accelerated by using the latest data protection solutions, because data sharing will become easier. Furthermore, if life science companies adopt a subscription business model, they will have a constant flow of revenue allowing them to update their devices and software regularly. Last but not least, a joint eHealth association will enable the creation of cheaper and safer healthcare devices and software and after that, distribution at a quicker pace.

Table of contents

1. Introduction

Since the 1930s, new information and communication technologies (ICTs) have appeared and starting from the 1960s these ICTs have been improved even more. According to Hamelink in 1997, ICTs refer to all technologies that enable the handling of information and facilitate different forms of communication, both among human actors and electronic systems (Hamelink Cees Jan 1997).

ICTs have deeply changed our ways of life. It can give people access to services or products that are not available locally or that are hard to access, such as seeing a movie from a person's home instead of going to the cinema. ICTs also improved our daily lives by automating parts of daily life. Autonomous vehicles, for instance, will bring you to your destination safely without you having to lift a finger. Finally, ICTs optimise people's activities, both professional and personal, as can be seen in people using the text editor Word instead of writing on paper.

In 2011, the German Federal Government introduced the concept of Industry 4.0, in which autonomous technologies will flourish and the automatisation of society will reach its paroxysm (VDI Nachrichten 2011). In Industry 4.0, society will get smarter and smarter and all kinds of objects and organisations will be able to work without human interventions or interactions. This is because of the latest ICT solutions, such as new Artificial Intelligence (AI) technologies and the so-called Internet of Things (IoT), in which every electronic object is connected. However, not all industries can automate their products or services at the same fast pace, even if the industries share the same technologies. The healthcare industry is probably the best example to illustrate this situation.

To automate and optimise healthcare, the concept of eHealth was created in the late 1990s (Jolly 2011). EHealth stands for electronic health and it aims to provide medical health devices and online health solutions, such as online prescriptions, to all individuals and organisations involved in healthcare. In this way, any individual has access to personalised healthcare, even remotely from their homes. Also, researchers can access health data of individuals to accelerate research and treatment improvements.

Even though various eHealth technologies exist, only some medical devices and online services are available to consumers. For instance, one of the only healthcare devices that uses AI and remote healthcare is the insulin pump presented by Medtronic in 2015, which will be available for consumers with diabetes in 2018. However, in other industries, such as the home appliances industry or the transportation industry, many products already use IoT and AI technologies.

The aim of this paper is to understand how personal data can impact the development of eHealth solutions in Europe, by doing literature research. Europe was chosen as the region for this research, since it has the strictest data protection regulations and is the most advanced region in eHealth development and adoption. To research this, the following two research questions were devised:

- How does the collection and use of private data slow down the development of eHealth solutions?
- Which are the recommendations that can speed up the innovation of eHealth solutions?

This research was commissioned by Pryv, a Swiss ICT company that specialises in healthcare. The company is located in the EPFL Innovation Park in the canton of Vaud. It provides solutions for health industry stakeholders to make data management easier and to make data collection safer and compliant with the latest (health) data protection regulations.

This paper consists of five chapters. After the first introductory chapter, the second chapter will discuss the role of computers and data starting from the 1930s until the current situation. Next, the third chapter looks at how healthcare evolved with the digitisation of society. It also gives a thorough explanation of eHealth and its current situation. Chapter four is about the challenges of data in general. Here, topics like privacy and regulations will be discussed. Finally, chapter five shows an overview of the best solutions to accelerate the development of eHealth.

2. Information society

The development of ICTs allowed for the creation of electronic systems to improve the creation, sharing and modification of data. By digitising society all activities, services and products will generate data and use these data to create the digital age, an era in which data is abundant and easily accessible to anybody at any time.

2.1 Digitisation of the society

The digitisation of society happened in several stages. The first stage refers to the creation of digital computers and the second stage is the digital revolution. The smartphone revolution can be seen as the third stage.

2.1.1 First digital computers

Between the 1930s and the 1960s, the world witnessed the creation of a new way to store, share and manage data, thus gradually digitising society.

This digitisation of society started with the first and second digital computer generations. With the creation of vacuum tubes during the late-1930s (Kloet, Van Tilburg 2006) and transistors a decade later (Brinkman, Haggan, Troutman 1997), digital computers were the first ICT devices that could create, store and manage data digitally (Hamelink Cees Jan 1997). However, those computers, which were sold during the 1940s to the 1960s, only had a limited impact on society. Thus, economists do not consider this period as the digital revolution, even if some parts of society were already being digitised (Nabi Khan 1987, p. 117-124).

Since the technology was brand new, many companies and consumers were not encouraged to acquire these new devices, since they were very expensive to build and to use. First of all, due to the lack of dominant design, computer manufacturers could not mass produce the devices, thus most of the first computers were unique pieces built for consumers, such as major finance and insurance companies. The devices also needed lots of electricity to run, making them very expensive to use. Moreover, they had hardly any functionalities, besides the ability to calculate or process data. Software and operating systems were not available at that moment and the first computers could not multitask. As a result, they were only able to run one task at a time: if the owner wanted to run another task, he had to reprogram the computer entirely. Finally, only mainframe computers were available at that time (Nabi Khan 1987, p. 117-124). Mainframe computers consist of a central processing unit that connects with several dumb workstations that do not have their own processing unit. Mainframe computers were too big and expensive for small and medium enterprises (SME), and thus not suitable for the consumer market.

For instance, the first fully operational digital computer, the Electronic Numerical Integrator and Computer (ENIAC), used about 167 square metres, weighed about 30 tons, used about 18,000 vacuum tubes and cost about 486,000 US dollars at that time (Neyer). With the current dollar, the ENIAC price would have been around 6.2 billion US dollars (Open Data Foundation 2018). When it was switched on for the first time in 1946, lights dimmed in some parts of Philadelphia.

However, big companies, research institutes and universities were all interested in this new technology, since all of their research and business activities generated, used and stored large data sets with huge quantities of information (Nabi Khan 1987, p. 117-124). Before the digital computer came into existence, data was stored on analog storage supports, such as books, paper and punched card systems. Analog storage supports had limited storage capabilities. Thus, if companies owned large amounts of data sets, they needed specific rooms to store all data. Moreover, it was difficult to access or copy a specific piece of information within these stacks of paper. Finally, analog storage supports needed special care because companies did not want to see their documents deteriorate because of humidity, insects or other conditions. So, even if digital computers did not offer a cheaper data storage and management solution, they were already more practical due to the easy access they provided to data by the establishment of an information technology (IT) infrastructure. This way, any user could access the data stored on the computer with the help of networked workstations.

2.1.2 Digital revolution

Even if the first generations of digital computers were not suitable for most of society, the computer industry witnessed a fast development between the 1960s to the late 1980s. This period is known as the digital revolution or the third industrial revolution (Nabi Khan 1987, p. 117-124), since all ICT innovations made during that period are still used today and have digitised our products, services and activities. Integrated circuits (ICs) led to the creation of microprocessors and microelectromechanical systems (MEMS). Operating systems were pre-installed on computers, many software applications appeared and these, combined with the creation of virtual machines, marked the beginning of office automation. Finally, the development and creation of internet allowed sharing and remote control of information by interconnecting all kinds of electronic devices. These innovations created electronic devices capable of generating and analysing data autonomously.

2.1.2.1 Hardware improvements

Transistors were a great upgrade compared to vacuum tubes. However, computers that were using transistors were only slightly smaller than the ones using vacuum tubes, since each transistor had to be soldered individually to an electronic circuit. However, this situation rapidly changed with the development of ICs. The idea behind ICs was to directly connect two or more transistors together. The first IC was created in 1958 and it connected two transistors together on a silicon base (Nobel Price 2014). This was the beginning of central processing units (CPUs) with microprocessors, and sensors with microelectronical systems.

2.1.2.1.1 Microprocessors

In 1971, the first microprocessor was created by Intel, a semiconductor company. This microprocessor, the Intel 4004, had the capacity to hold 2,300 transistors on only 10 square millimetres (Intel). The processing power of this first microprocessor was equivalent to the first digital computer, the ENIAC, which needed about 20 million times more space to carry out the same tasks.

The creation of the microprocessor led to a rapid improvement in processing power of computers and the miniaturisation of transistors. Only two decades after the first transistor was created, the power of the electronic components increased a thousand times (Nabi Khan 1987, p. 117-124), resulting in a reduction in the cost per function, such as the number of calculations, by several thousand times (Moore 1975).

The development of microprocessors also led to the miniaturisation of digital computers. While until the late 1960s only large mainframes were available, the early 1970s saw the creation of minicomputers. This type of computer is much smaller and cheaper than mainframe computers, making them more suitable for SME. Following the minicomputers, personal computers (PCs) appeared in the late 1970s. Even smaller than minicomputers, PCs only used one microprocessor as a CPU, making them relatively inexpensive compared to other computer types. The PC was the first type of computer suitable for both business and consumer markets (Nabi Khan 1987, p. 117-124).

Microprocessors continue to develop: the number of transistors doubles every year, following Moore’s law (Moore 1975). Only a decade after the Intel 4004, Intel’s newest microprocessor had about 134,000 transistors (Intel 2007). Nowadays, semiconductor companies are able to pack up to 100.8 million transistors on a square millimetre (Courtland 2017), making it possible to produce microprocessors with more than 30 billion transistors on a chip (Nield 2017).

2.1.2.1.2 Microelectromechanical Systems

Alongside the creation of microprocessors, microelectromechanical systems (MEMS) appeared. MEMS are very small systems, based on IC technology, which combine microsensors, microactuators and microelectronics. Compared to microprocessors, MEMS were not used for their processing power but for their capability to sense or interact with their surroundings, allowing electronic devices to interact with the physical world. The first MEMS was a pressure sensor, a prototype built in 1961, followed by the first accelerometer, another prototype that was built a decade later (PRIME Faraday Partnership 2002).

2.1.2.2 Software improvement

With the creation of microprocessors, computers were now powerful enough to handle complex software, resulting in a fast development during the middle 1970s. This period is characterised by the creation and spread of high-level programming language, such as the famous C language created in 1972 (Mundargi, Granchamp, Kaja, Chandra, Serrano 2014). Since then, more sophisticated software was created to enable a better creation, modification, visualisation and sharing of data. Some of the current famous programs were created during the 1980s, such as Word, released in 1983, Excel, released in 1985, and Photoshop, released in 1990 (Royal Pingdom 2009). The creation of virtual machines (VMs) also occurred during that period, allowing a computer to simulate one or many computing sessions at the same time (Neto 2014). VMs had a positive impact on companies because they did no longer need a physical computer for each of their employees.

2.1.2.3 Telecommunications improvement

With the creation of digital computers, society was also interested in interconnecting them in a worldwide network to improve information sharing. Until the 1970s, it was only possible to connect computers in a local network, for instance in a company or university facility. However, the telecommunications industry witnessed fast improvements starting from 1969. In that year, the first version of the modern internet went live (Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel 1997). Known as Advanced Research Projects Agency Network (ARPAnet), the project aimed to improve information sharing for the research community. The first two institutions that connected to the ARPAnet were the University of California, Los Angeles, and the Stanford Research Institute. The commercial version of ARPAnet only appeared five years later, with the creation of Telenet in 1974 (Internet hall of fame 2018). It was only with the creation of the World Wide Web (WWW) in 1989 that sharing and retrieving information became easier. This is because the WWW had the ability to store all kinds of information in virtual documents that could be found and visualised by using a web browser. To retrieve these documents, users only had to type in keywords. Initially built for researchers, the WWW finally went public in 1993 and this led to the modern web (CERN 2018). Since then, many webpages have been created, not only to store information, but also to provide online services and products through e-commerce (Slater 2002).

2.1.3 Smartphone revolution

In the final stage, the smartphone revolution, various objects become smart because of the (new) technologies used in smartphones. The internet network has been improved and the reduced size of sensors and ICs allows objects to get smarter and to get connected.

2.1.3.1 Smartphones

The idea behind smartphones was to create a device as small as a personal digital assistant (PDA), but with the functionalities of a personal computer. The first smartphone appeared in the mid-1990s (Canny, Hartmann 2010), but it is only a decade later that Apple succeeded in making the smartphone popular. The iPhone was the first smartphone that could achieve the same functionalities as a personal computer in the palm of your hand.

The success of Apple is related to the setup of an application market place, the App Store. Smartphones that were created before the iPhone were not popular due to the lack of services and software. They could barely do more than a primitive PDA or a regular phone, but they were more expensive. With their App Store, Apple allowed third-party developers to build and sell their applications or to provide them for free. These applications were specifically developed for smartphones. When the App Store went live in 2008, it already had over 500 applications available (Ricker 2008).

In 2008, Apple sold 3.3 million units worldwide, positioning the company as the fifth largest smartphone manufacturer. A year later, when the App Store went live with the release of the second generation of iPhones, Apple sales exploded. One year later, sales grew with about 245% to reach approximately 11.5 million units sold (Elmer-Dewitt 2009). At the same time, the App Store grew from 500 to 41,000 applications (Business Insider Intelligence 2016) and reached 1 billion downloads in only one year (Statista 2017).

Today, smartphones are driving the digitisation of the world. In 2018, about 1.5 billion smartphones were sold worldwide. The smartphone market should continue to grow with a compound annual growth rate of 2.8% for the next five years (Scarsella, Stofega 2018). In contrast, personal computers are not selling as well, with decreasing sales since their peak in 2011. Then, some 365.4 million units were sold while in 2016, sales only reached 269.7 million units (Dunn 2017). This is five times less than the smartphone sales. The two biggest application markets, the App Store and the Google Play Store, offered respectively 2.2 and 3 million applications in January 2017. Together, over 115 billion applications were downloaded (Dogtiev 2018).

Before smartphones turned into such a success in 2007, the world’s penetration rate of mobile broadband subscriptions was about 4%, slightly less than the fixed broadband subscriptions. A decade later, the penetration rate of mobile broadband subscriptions rose considerably to 56.4%, while the rate of fixed broadband subscriptions was four times smaller. Today, 48% of the world population is connected to the internet (ITU 2017) and it is expected that 75% of human beings will be connected by 2025 (Reinsel, Gantz, Rydning 2017).

2.1.3.2 Wireless network

The success of smartphones had a positive impact on the development of wireless mobile telecommunication technologies. The fast spread of smartphones led to a tremendous increase of data transfers on the mobile network. Data traffic was about 80 times lower than voice traffic before 2007. Only two years later, data traffic caught up with voice traffic on wireless networks and, in 2010, data traffic was twice as large as voice traffic (Ericson 2012). As a result, the third generation of mobile broadband (3G), which was presented in the early 2000s, was rapidly pushed to its boundaries. With a theoretical download speed of only 2 Mbps (Telecom-infoconso), 3G was too slow to handle the rapid increase in data demands. Even though 3G technology rapidly evolved to reach a theoretical download speed of 42 Mbps in 2008 (3GPP 2008), it was replaced by 4G, presented in 2010 (ITU 2010). 4G offered new possibilities with its promised theoretical download speed of 1 Gbps (Telecom-infoconso).

The high capabilities of 4G enabled the possibility of connecting other devices as well as a larger number of devices without the network being overflown. As a result, developing countries focused on wireless network development instead of fixed network development. Wireless network infrastructures are cheaper than fixed network infrastructures, since there is no need to wire all houses and buildings individually. A simple antenna needs to be installed and then all wireless devices can directly connect to it. Nowadays, many developing countries in Asia and South America have a better or an equal 4G coverage compared to western countries (OpenSignal 2018), even if a lower proportion of their citizens have a mobile broadband subscription (Broadband Commission 2017).

2.1.3.3 Increased amount of IoT devices

The Internet of Things (IoT) refers to all devices with the ability to connect to the internet and share information with other connected devices. The rise of smartphones rapidly increased the amount of IoT devices available around the world. This happened because of the increased development pace of semiconductors and sensors. According to Dr. Janusz Bryzek in 2012, the sensor demand grew from 10 million units to 3.5 billion units annually between 2007 and 2012. This is a growth of 222% per year. Nowadays, semiconductors and sensors are small, cheap and powerful enough for companies to implement them into everyday objects and make these objects “smart”. Smart objects work together to automate tasks or reduce costs. According to GrowthEnabler (2017) about 1 billion IoT devices were available in 2009. In 2017, the number of IoT devices surpassed the number of people on earth. In the future, the number of IoT devices around the world will continue to grow rapidly. Forecasts on how many IoT devices will be available by 2020 vary a lot, from 20 billion to 200 billion (GrowthEnabler 2017) (Intel 2018). This means that the number of IoT devices per human will vary between 4 and 26 (Reinsel, Gantz, Rydning 2017) (Intel 2018). The health sector will be a key industry in the IoT market, since 30% of IoT devices will be related to healthcare (Intel 2018).

2.2 Digital age

The beginning of the millennium was marked by the transition of human society into the digital age. The year 2002 was a landmark: for the first time, more data was stored on digital supports than on analog supports. Considering the first digital computer was only created in the late 1930s and that new ICTs only started their spread in society during the digital revolution in the late 1970s, the digitisation of society happened relatively fast. In the mid-1980s, only about 1% of data was stored on digital supports (Hilbert 2012), which was about 0.002 zettabytes (Hilbert 2018). Two decades later, almost 100% of the available data was stored in digital storage supports (Hilbert 2012), which was a little more than 0.3 zettabytes of data (Hilbert 2018).

The great increase in the data sphere is due to the multiplication of electronic devices in the consumer market. IC and microprocessor development allowed the production of small and inexpensive devices for entertainment purposes, such as video players, music players or even gaming consoles. However, the internet was still new, slow and quite expensive. Consequently, the amount of data stored on various supports, such as DVD or CD, increased a lot (Reinsel, Gantz, Rydning 2017).

2.2.1 Changes in the data landscape

During 1980-2000, companies generated only a small amount of data since MEMS were not widely used. The digitisation that happened in the business market enabled office automation (Hilbert 2012). However, MEMS were already used in various products and organisations but many products that were integrated with MEMS were not collecting data to be analysed. For instance, cars with MEMS could deploy airbags in a crash. Hard disk drives used MEMS for their ability to read data and pacemakers also used MEMS to operate. Despite, all those devices generated data. these data were not captured and just deleted after the devices were used (PRIME Faraday Partnership 2002).

During the 2000s, the landscape of data rapidly changed with the improvement of wireless technologies (Reinsel, Gantz, Rydning 2017). While in 2007 there were about 0.3 zettabytes of available data, in 2014 the data sphere rose to 4.6 zettabytes (Hilbert 2018). Today, there are more than 20 zettabytes data available around the world and forecasts expect that the data sphere will reach the 163 zettabytes by 2025 (Reinsel, Gantz, Rydning 2017).

Most data generated nowadays is still related to entertainment. After all, the global entertainment market grew relatively fast. In 2016, the entertainment sector generated about 1.9 trillion US dollars, with video games accounting for half of that amount (U.S. Department of Commerce 2017). However, the development of wireless technologies changed the way in which society uses and stores data. Today, various cloud-based services, such as Netflix and Spotify, allow people to consume entertainment on the go. There is no more need to own data since it is easily retrievable online. As a result, less data concerning entertainment is created, even if it is still a big part of the data sphere with the increased quality of the content, for instance, through 8k video (Reinsel, Gantz, Rydning 2017).

2.2.2 Massive amounts of data

The largest increase in data is related to IoT devices. The mass production of MEMS led to the fast improvement and reduction in price of MEMS. This also meant that MEMS could be used in all kinds of products, for instance in IoT devices. Now, MEMS are not only used to work by themselves, but also to work with other MEMS and create an entire system, the Internet of Things (Goldman Sachs 2014).

However, the amount of data that is created by IoT devices is tremendous. Even if each separate system inside an IoT device does not produce a large amount of data, all MEMS combined create a large dataset in just one IoT device. For instance, the engine used in the latest Bombardier aircraft has about 5,000 sensors that generate about 10 GB of data per second (Rapolu 2016). Due to the large amount of data created, it is not possible to store all of it. Moreover, it is also not necessarily useful to do so (Reinsel, Gantz, Rydning 2017).

The amount of data also increases because of people interacting with connected devices. In 2015, for instance, humans interacted with approximately 218 connected devices or services per day. This amount will slightly grow to reach 601 interactions per day in 2020, while the expected number of interactions per day will reach 4,785 in 2025 (Reinsel, Gantz, Rydning 2017).

2.2.3 Critical data

To make data valuable, IoT devices are increasingly integrating specific analytics or artificial intelligence solutions to analyse the data. This way, data is being used and erased in real-time. The multiplication of IoT devices also makes data critical since automatising daily-lives makes IoT devices are more and more data dependent. Critical data means that that data is “necessary for the expected continuity of users’ daily lives” (Reinsel, Gantz, Rydning 2017). For instance, if entertainment data is stolen or destroyed, it will not affect the proper functioning of the society. However, for data generated by autonomous cars it is different. If this is altered or if such a car is hacked, transportation services will just stop working and disturb the proper functioning of the society. In future, critical data might prove more and more important for society. While the overall amount of data rises by 30% each year, critical and hypercritical data. Compared to critical data, hypercritical data has a “direct and immediate impact on the health” of humans. Hypercritical data is created by IoT devices used for medical applications or control systems. From now on, the amount of hypercritical will double each year and reach 10% of the whole data sphere in 2025 while critical will account for 20% (Reinsel, Gantz, Rydning 2017).

3. Healthcare in the information society

Healthcare is among the first industries that have integrated ICT in their organisation, products or services. Activities, whether it was research or healthcare delivery, generated and needed to use a lot of data. Thus, when the first digital computers appeared that offered better data management, storage and access across their organisations, institutions involved in the health sector were the first to implement information technology (IT) infrastructures and to use office automation solutions to improve their productivity or efficiency.

It is the healthcare delivery organisations (HDO) that benefit the most from ICT. As for the organisations involved in the health sector, HDOs have implemented an IT infrastructure to improve data management and access. The creation of integrated circuits (ICs) and microelectromechanical systems (MEMS) also led to the modernisation of available medical devices and the creation of many new ones (The New York Times 2012). Electronic medical devices drastically improved healthcare services and procedures provided by HDOs and as such, have a great impact on people's lives. Firstly, they are more reliable than old electric devices or methods to get information about patients' health conditions. For instance, magnetic resonance imaging (MRI) machines were created during the digital revolution (Liu 2004). With these medical devices, it is possible to visualise in real time the inside of a patient without the need to cut him open. Secondly, electronic medical devices have the ability to monitor a patient's life all day long without interruption and under all circumstances. This practice is beneficial in various situations. It allows medical workers to react more quickly in the event a patient's vital health signs rapidly drop. It also enables the possibility to track symptoms with greater efficacity. Some symptoms only appear periodically, thus 24/7 monitoring can capture them. Finally, real time monitoring without interruption improved surgeries since doctors had extra information about patients' health and could also react faster in the case of an event. Finally, the devices are connected to the IT infrastructure of the HDO allowing the automatic storage of all data in a patient's electronic health record (EHR). On the one hand, this infrastructure allows doctors and nurses to keep an eye on a patient's health condition remotely. On the other hand, it also improves the efficiency of HDO services. When a patient comes back at the HDO, doctors have instant access to all previous treatments and health data.

3.1 Challenges of the actual healthcare system

However, the present healthcare system is challenged by changes in society and it shows its limitations. Today, half of the world's population still does not have access to primary healthcare services due to the high expenditure for healthcare and lack of proper infrastructure (WHO 2017). While it is the low-income countries that are primarily hit by those issues, high-income countries are now also facing limitations in their healthcare systems, but not for the same reasons. On the one hand, high-income countries are facing a rapidly aging population, thus increasing sedentary lifestyles and related health problems. In 2015, the population of people aged 60 or over was about 0.9 billion and it is estimated to be 3.5 times bigger by the end of the century. In the same period, the world population will only increase by 1.5 times (United Nations 2015). On the other hand, the number of chronic diseases around the world is increasing, especially in high-income countries, due to unhealthy life styles or conditions, diets and habits, giving rise to e.g. heart problems, diabetes, Parkinson, epilepsy or asthma. By 2020, chronic diseases will globally account for seven out of every 10 deaths (Anderson 2011). As a result, global healthcare expenditure has been growing 4.5% per year (Ibis Capital 2016) on average for the past decade and it accounted for 9.9% of world GDP in 2015 (The World Bank 2018), impacting primary healthcare access in both low- and high-income countries.

3.2 EHealth

Electronic health, more commonly known as eHealth, can be defined as “the use of information and communication technologies (ICT) for the organisation, support and networking of all processes and partners in the health system” (Swiss Federal Office of Public Health 2007).

EHealth is a relatively new concept since it only emerged in literature at the end of the 1990s. Moreover, it only gained interest in 2005, after the World Health Organisation (WHO) released its resolution WHA58.28 (WHO 2005). In this resolution, the WHO recognised the positive impact eHealth can have on the health sector. Consequently, the WHO integrated eHealth as a key element to achieve its universal healthcare coverage. At the same time, the WHO also pushed its member states to establish a long-term eHealth strategy and to promote the development of eHealth solutions. To help its member states with that task, the WHO provides advice and guidelines for policy makers, HDOs (Health Delivery Organisations) and life science companies (such as MedTech, BioTech and the pharmaceutical industry) to ensure the fast and safe development of eHealth solutions (WHO 2005). Since then, the rise of eHealth is considered as the first major revolution in the health sector (WHO 2016).

On the citizens’ side, eHealth has the potential to drastically improve the access to healthcare and the quality of care received by any individual. In the future, the use of portable IoT devices will allow all individuals to monitor their health on their own. Combined with a mobile health application (mHealth) of cloud-based analytics solutions, individuals will be able to get automated diagnostics. When eHealth solutions detect any health issues, the right treatment will be automatically generated and individuals will be automatically redirected to the right specialists. After all data is collected, generated or processed, it will be transferred to an individual’s electronic health record (EHR). This is a digital folder to store all health or medical information concerning an individual. National EHR will make life easier for patients. Individuals store all of their data in one place and they can access the data at any time and place.

HDO, research institutions and life science companies (MedTech, BioTech and Pharmaceutical companies) will have a greater efficiency with the creation of eHealth. The large amount of data stored in the EHR will speed up the research of new treatments and cures since researchers may have access to the specific data they need without having to collect it themselves. EHealth may also make it easier to conduct drug clinical trials, since patients will not have to be present at the test centre to get the drug because it can be sent to them directly. Patients will just monitor themselves and researchers will just have to follow the data they receive, all of which will make the trials cheaper. HDOs will also be able to automatise part of their services, such as using artificial intelligence (AI) to run analyses or using a robot to perform surgery. The particularity with AI is that it has a learning capacity: the more it is used, the more it learns with the help of machine learning (ML) programs. Finally, AI can also assist doctors by providing more than just real time patients' vital signs, and by acting more like a personal assistant giving advice.

For governments, eHealth will play an essential role in improving their citizens' physical and psychological health. Again, thanks to the large amount of data that will be available in EHRs, governments will be able to use AI programs to spot medical trends in their population and take more personalised action, for instance, in a specific neighbourhood. Governments will not only be able to understand health problems in a specific area or population, but also spot the spread and the origin of a new disease faster.

3.3 Slow development of eHealth

However, after more than two decades of development, eHealth has barely advanced compared to other industries using the same technologies. Half of the European countries have not introduced a national electronic health record (WHO 2018). Only 7% of European citizens have used an online health and care service three times or more in the past 12 months, while 81% of European citizens have not used online health and care services at all (Eurobarometer 2017). Health related wearables are barely available on the consumer market and the ones that are sold most often are fitness trackers. Even eHealth solutions like health applications and websites have a limited success. In 2017, only 3.7 million health or fitness related applications were downloaded, which equals 0.004% of the total of downloaded apps for the same period of time (Dogtiev 2018) (Research 2 Guidance 2017). Finally, the OECD indicator about eHealth adoption in hospitals in European countries was relatively low. In 2013, the indicator was only about 0.3 out of 1, with 1 being full adoption while 0 indicates no adoption at all (OECD 2016). In comparison, the digital technology adopted by the automobile industry is progressing faster: automated shuttles are already in use in some places, such as Sion in Switzerland (RTS 2017), while the first fully autonomous shuttles (Moon 2018) and cars (Hawkins 2018) will be available in the course of 2019.

4. Data challenges

The healthcare sector faces many challenges regarding the collection and storing of the large amount of personal data. This chapter discusses the key challenges, being data overflow, cybercriminal activity, consumer trust and ePrivacy and regulations.

4.1 Data overflow

The multiplication and distribution of ICT solutions led to a data explosion that companies cannot handle today. While companies that use their datasets to establish strategies are about 10% (Nesta 2015) more productive, only 12% of the data stored in those companies is used (Forrester 2014). To tackle this data overflow, companies are interested in the latest technologies, such as the Internet of Things, artificial intelligence and big data analytics solutions. This way, they can automatically process and transform data into usable insights such as what are consumers looking for, what are they listening to or which places do they visit in order to understand the consumers (profiling) and set up better marketing or business strategies.

4.1.1 Analysing big data

The increased amount of data generated by the use of online services and IoT devices has pushed companies to establish big data and analytics solutions (D&A). D&A is a software program built to automatically process large amounts of data sets in order to analyse trends. Today, 97% of companies use D&A software. The use of D&A offers many advantages, such as reducing operating costs, generating new sales, reducing business risks and the ability to understand consumers (KPMG 2015). Consequently, companies consider data as an important asset and share or sell data. In 2016, the revenues generated by data sales only reached 300 billion euros. By 2020, this amount will reach 739 billion euros (European Commission 2017). On average, companies tend to share their data with 40 different partners (Garessus 2017).

4.1.2 Big companies and their data control

The Cambridge Analytica case shows how big companies such as Facebook have little control over their data after this has been sold to other companies. They do not know what happens to the data and their users' privacy and often they do not even monitor what kind of data was taken (Lewis 2018). Most companies are interested in how much time is spent on a specific web site, what type of content is looked for online or the number of likes delivered online. These data allow them to understand and to target their consumers better. By doing so, companies can even manipulate consumers into buying products or services by showing specific advertisements, for instance.

On the one hand, about 10% of European companies do not know how much and where they store their data. On the other hand, companies try out different techniques to get more and more data about their consumers. For instance, the television manufacturer Vizio was caught selling televisions with the ability to spy on their users (Seydtaghia 2017). These televisions sent information about what the users were watching to Vizio. The company then sold the collected data to advertisers that aimed to set up more personalised and accurate marketing strategies. Not only companies abuse the use of data, but also governments and their organisations. The most famous recent case is the case in which the NSA (National Security Agency) puts millions of citizens from both the USA and the rest of the world under surveillance (Szadkowski 2013).

While the NSA and other governmental agencies promised to reduce their surveillance activities, reality shows the opposite. The NSA is still collecting a lot of personal information (LesEchos 2017) and other countries install solutions to track their citizens as well. For instance, China is deploying the largest camera surveillance network in the world, able to recognise not only its citizens, but also vehicles, and to predict if any conflicts will happen (Brostra 2018).

4.2 Cybercriminal activity

The fast expansion of different electronic devices and software has increased the opportunities for hackers to attack. They do not only have more targets to attack, but they also have more chances to succeed. Neither hardware nor software is entirely secure, but they are both exposed to vulnerabilities. Hackers can exploit these vulnerabilities to get into an electronic device or IT infrastructure and steal, erase, modify or encrypt all data available. In 2016, more than 10,000 vulnerabilities were publicly disclosed, a number that is constantly increasing, which shows that the amount of new opportunities for cybercriminals is increasing as well (IBM 2017).

4.2.1 Vulnerabilities

However, the problem does not only contain the vulnerabilities. ICT companies can easily fix their products with simple patches. Moreover, some of ICT companies even have programs that reward hackers who find and report any vulnerabilities in their products. For instance, Google has established a Vulnerability Reward Program (VRP) in which hackers get paid up to 31,117 US dollars per reported vulnerability. Programs to spot vulnerabilities have proven their efficacies (Google 2018). Since 2010, Google has already spent more than 12 million US dollars in rewards. Last year accounted for one fourth of this total reward, with 1,230 hackers participating in the program. The single highest reward was about 112,500 US dollars. Rewarding hackers for spotting vulnerabilities is an interesting concept, since they can get legally paid for carrying out illegal activities. At the same time, they contribute to a safer service or product (Keller 2018).

Vulnerabilities are disclosed when a patch is available (Rouse 2017). On the one hand, keeping the vulnerabilities a secret limits potential attacks. On the other hand, by disclosing vulnerabilities it allows companies to make their consumers aware of the risks and the need to update the computer or software. Cybercriminal attacks usually happen when users do not install updates or when they use end-of-life systems. In May 2017, for instance, ransomware WannaCry hit systems using Windows around the world using a Windows vulnerability that Microsoft had patched two months earlier (Kessem 2017).

4.2.2 End-of-life systems

End-of-life systems are even more dangerous than non-updated systems, since they will never be protected. The issue here is that many companies use devices or software that are considered end-of-life systems. ICT companies no longer support these systems, because they are too old or more recent versions are available, thus making them vulnerable to any new threat found. The most famous case of an end-of-life device is the ATM (Automated Teller Machine). Worldwide, many ATMs are still using an old Microsoft operating system (OS) which is not supported anymore. Moreover, in the near future, more ATM OSs will no longer be supported, leaving hundreds of thousands of ATMs vulnerable to new threats (Sancho, Huq 2017). However, the ATM is just one example of a company using an end-of-life system for its devices or IT infrastructure. For many years, numerous companies were using old systems and never updated them. A study in 2016 showed that 73% of North American companies are still using end-of-life devices in their IT infrastructure (BusinessWire 2016). Having a vulnerable device makes the full IT infrastructure vulnerable since these devices can be used as an entrance for hackers.

Smartphones are also getting interesting for hackers, not only because they are popular now, but also because most of them are considered as end-of-life devices. Smartphones running Android are the most widely used smartphones worldwide with a market share of 77.32% (GlobalStats 2018). However, only half of the Android devices are actually still supported by Google. In the latest Android security updates, the oldest Android version that Google supports is the 6.0. According to Google’s statistics, only two third of smartphones are running with versions 6.0 or higher (Developers 2018). To tackle this issue, Google has started a project known as Treble. Today’s practise is that Google provides the latest Android version and security patch to the smartphone manufacturers and telecommunication companies for those companies to install the updates in the smartphones. However, those companies tend to only update the new devices. With Treble, Google will be able to directly provide Android version and security updates to all compatible devices. Smartphone manufacturers and telecommunication companies will not have to think about it anymore (Malchev 2017).

4.2.3 IoT devices, the most vulnerable electronic device

The increasing demand and use of sensors in IoT have made this problem of vulnerability even worse. At the moment, IoT devices are easy to hack due to their lack of security (O'Donnell 2018). Manufacturers tend to rush the market without providing proper protection. As a result, cyber-attacks against IoT have increased by 600% over the last year (Symantec 2018). Threats against IoT devices have to be taken seriously. IoT devices, with all their sensors, have the ability to interact with physical space. Thus, this makes IoT devices prone to directly harm human beings. To show the lack of security of IoT devices and the dangers it may come from, two security researchers, Charlie Miller and Chris Valasek already hacked three different cars. The last one was in 2015, when they were able to take control of a Jeep remotely (Kochetkova 2015). This situation can be very harmful for both the people inside the car, but also for the surroundings of the car. After this discovery, Chrysler, Jeep's mother company, recalled 1.4 million vehicles to fix this issue (Greenberg 2015). However, the car company only fixed the vulnerability shown during this hack without checking the other electronic pieces. As a result, the two hackers hacked the car again a couple month later exploiting other vulnerabilities (Drozhzhin 2016).

Due to this situation, the European Union has decided to start a project known as Predictive Security for IoT Platforms and Networks of Smart Objects. The aim of the project is to provide the IoT device makers with a solution to protect their products. According to the European Union, present and future devices are almost impossible to protect by the companies. The project should change this situation by building an open source platform which can be used as a security base and by adding other security level above (European Commission 2018).

4.2.4 Cost of cyber-attacks

Cyber-attacks are very expensive for companies. In 2015, damages related to cybercriminal activities cost about 3 trillion US dollars worldwide and they are expected to double by 2021 (Morgan 2017). However, worldwide expenditure in cybersecurity solutions remained low last year. With 86.4 billion US dollars in global cybersecurity expenditure, it merely represents 2.88% of the costs of cybercrime damages. This shows how companies prefer to get attacked before taking proper measures to secure their IT infrastructure (Morgan 2017). Moreover, a study shows that organisations which were attacked by a small attack tend to not take security seriously and are more likely to get their data stolen a second time within the following two years, chances of which are about 27%. Organisations that were struck by a massive data breach tend to take serious measures and thus have only about 1% chance to lose their data again over the following two years (Ponemon Instiute 2017).

On average, damages after a data breach were about 3.62 million US dollars per incident, while lost data records were valued at about 141 US dollars per record. Health is the industry where data breaches cost the most: on average, data records in the health industry cost about 380 US dollars per record (Ponemon Instiute 2017).

The time to detect a data breach is relatively long. In 2017, the average time needed to detect a malicious or criminal attack took about 214 days and then, to correct it, about 77 days. This means that companies have their data unprotected for about 10 months when they are victim of a data breach (Ponemon Instiute 2017).

4.2.5 Ransomware, a new kind of attack

A new kind of attack is emerging which consists in blocking the access to data. Until now, most attacks consisted of stealing, altering or destroying data stored in electronic devices. However, the latest trend is to only block data by encrypting it. The only way for owners to regain access to their data is by paying cybercriminals to unlock the data. In 2017, without considering WannaCry and Petya/notPetya, there was an average of 1,242 ransomware attacks per day. The same year saw an increase in new ransomware variants with 350 new kinds, an increase of 46% compared to 2016 (Symantec 2018). The health sector is the most widely targeted by ransomwares. In 2016, about 88% of all ransomware attacks happened in the health sector (Goldman 2016). Compared to other industries, cyber-attack on health delivery organisations causes more dramatic damage. Thus, by kidnapping information, health delivery organisations are not merely shut down as companies, but patients' lives are threatened as well. When medical devices cannot access patients' electronic medical records, those devices will not be able to operate anymore. As a result, they will not only stop delivering treatment but also stop to monitoring patients. Which in turn will prevent doctors from operating their patients.

4.2.6 Healthcare, most vulnerable industry

Not only healthcare industry is the most target industry, but it is also considered to be the most vulnerable industry and prone to cybercriminal attack, because of two simple reasons. On the one hand, medical data is the most valuable kind of data on the dark web. Compared to credit card information, medical data is about ten to twenty times more valuable (Humer, Finkle 2014). The stolen records can be used for various purposes, such as for getting and selling prescription drugs, creating fake IDs based on real biological data or even insurance fraud. On the other hand, in health delivery organisations, patients' lives can be directly threatened by a security breach. Even the smallest attack, such as locking down an HDO's IT infrastructure can have dramatic effects. Medical devices will not work and HDO workers cannot access EHRs anymore. Thus, patients following specific treatments will not receive their treatments and doctors performing an operation will not have access to critical information about their patients. Furthermore, patients who are dependent on medical devices may suffer devastating consequences without their medical devices.

4.2.6.1 No proper measures against hacking

Cyber criminality would not be a problem if the healthcare industry was taking proper measures to protect its IT infrastructure and devices. However, this is far from reality. The healthcare industry is among the most, if not the most, unprotected industry. While other industries spend about 12% to 16% of their IT expenditure on security, healthcare organisations are far below with only 6% (Lyon 2017). Moreover, medical devices are absolutely not secure at all. After the WannaCry attack, it appeared that even in high-income countries HDOs rarely upgrade their devices. In 2017, Digital Health Age revealed that 60% of NHS Trusts, also known as the public hospitals of the UK, were still using Windows XP either in their medical devices or in their IT infrastructure, which again is an operating system that is not supported by Microsoft anymore. Its vulnerabilities are known and will not be fixed in the future.

4.2.6.2 The weakest point of HDOs

Medical devices are the weakest point of HDOs. A recent survey shows a critical lack of security in medical devices (Ponemon Institute 2017). While HDOs themselves are rather confident about their IT infrastructures, the survey shows that medical device makers feel the opposite about the devices they produce. Only 37% of the HDOs think their devices are free from vulnerabilities, while only a quarter assess that their devices are sufficiently secured. As was said earlier, a non-protected device can directly harm patients in a worst-case scenario (Ponemon Institute 2017). According to HDOs, events in which patients could have been injured, happen quite often. Thirty-seven percent of HDOs already had cases in which cybercriminals took control over medical devices. About the same percentage of HDOs indicate that devices had delivered the wrong treatment to a patient. Thus, patients' lives were directly threatened since machines can either physically injure patients during surgery or administer a lethal dose of drugs. Other less dangerous, but non-negligible events also occurred to medical devices and IT infrastructures, such as the denial of services, blocked access because of ransomware, theft of records or the installation of unknown software. This last event can lead to a loss of full control over the hospital, since medical devices tend to be connected to the whole HDO IT infrastructure. By getting the full control over a hospital, cybercriminals are able to target not only one patient, but all patients inside the HDO facility. Surprisingly, medical device makers tend to be less aware of the dangers of cybercriminals activities with regards to their devices. A lack of communication between HDO IT workers and the device makers may be the cause (Ponemon Institute 2017).

4.2.6.3 No improvements in security

Although the issues are known, hardly any steps are taken. An average of 16% of device makers and HDOs are actually taking concrete steps to prevent cybercriminal attack, even though two thirds of device makers think it is urgent to secure their devices. Many reasons may have led to this situation (Ponemon Institute 2017). First of all, 80% of both HDOs and device makers think securing medical devices is too difficult. In various surveys, they state that there is a shortage of IT workers (Ponemon Institute 2017) (HIMSS 2017), making it impossible for both the HDOs and device makers to properly secure their devices. Secondly, a lack in funds is also one of their main challenges. On the one hand, HDOs lack funds, especially in Europe, since healthcare is publicly funded (HIMSS 2017). On the other hand, medical device makers are mainly represented by micro or small enterprises. This is the case in Switzerland. This country is among the leaders in the MedTech industry, alongside Ireland and the United States of America. Its MedTech industry landscape reveals that more than 75% of MedTech companies have fewer than 50 employees (Swiss Medtech 2016). Thus, a large part of their funds goes into the development and marketing of their products, leaving hardly any funding for other features, such as security. Finally, as can be seen in Ponemon survey, 63% of medical device makers think it is more important to get proper IT security in HDOs first, rather than start by securing medical devices themselves. As a result, security is ignored most of the time, with 40% of medical device makers and HDOs taking no steps to protect the devices. Both of these will only change this wait-and-see practice if they experience a big cyberattack or if new regulations force them to (Ponemon Institute 2017).

Regular medical device testing is also relatively important since medical devices are not only easy targets, but also very vulnerable ones. When medical devices are tested, it turns out that an average of 15% of devices is infected with malware. Moreover, 30% is found to have critical vulnerabilities (Ponemon Institute 2017). However, only 11% of HDOs and 16% of device makers perform at least one test each year, while the majority is not performing any tests or is waiting for a cybercriminal attack before acting (Ponemon

Institute 2017). Moreover, only two thirds of device makers test the security of their devices during the development. One third of medical device makers only perform a security test after their products have been made available on the market (Ponemon Institute 2017).

4.3 Consumer trust and ePrivacy

The use of ICT is known to leave all kinds of (personal) information behind, like how much time was spent on a website or which pages a person visited. Ever since the internet was created, Europeans have been concerned about their privacy and the unauthorised use of their personal information. In 1997, about 72% of Europeans were worried about the leftover personal data after using online services. Thus, most of them would avoid using these services to avoid the risks (INRA 1997). Only 16.4% did not mind if their data was used. However, the majority of European citizens would actually use these services if they could fully understand how their data is collected, how companies use the data and what kind of data the companies collect (INRA 1997). Thus, if companies established proper privacy statements guaranteeing transparency, only about 16% of European citizens would still dislike these companies to collect and use their personal information. In the end, almost all citizens agree to the fact that the European Union has to properly protect their privacy outside Europe as well (INRA 1997).

However, in two decades the situation has barely changed, but even got worse. Today, it is possible to easily track people with all the connected electronic devices used in everyday life.

4.3.1 No control on personal data

In 2015, only 15% of Europeans felt they had full control of their data and 20% knew how their data was used (TNS Opinion & Social 2015). This is a relatively low score considering the high protection the European Union offers its citizens. Even so, citizens tend to easily give their personal information to online services and about 70% thinks this is quite normal. This is due to the increase of companies asking for the creation of user accounts in order to be allowed to use the company’s services (TNS Opinion & Social 2015). By doing this, companies can get various pieces of personal information, such as the user’s name and address. This leads to a tracking system, since companies easily know who is doing what on their websites. However, more than 50% of the population feels trapped by this situation, while only 35% thinks that providing personal information is not a big issue (TNS Opinion & Social 2015). They think there is no alternative for providing their personal information in order to use the services. However, 74% of the citizens does not like to see companies sharing their data without their permission (TNS Opinion & Social 2015).

4.3.2 Increased surveillance

With the increased amount of connected devices, Europeans are very concerned about the surveillance the companies might do. For instance, retailers use fidelity cards to track your consumption and then make you an offer on the products you purchase the most. Online services also track you to know what you like to read, watch or listen to on the internet. Two thirds of the Europeans do not want to accept this practice and they want to be able to choose whether their data is being used. However, smartphones are increasingly being used by companies to track European citizens, since almost everybody carries a smartphone around during the entire day. To protect their privacy, about one third of Europeans are using specific programs to prevent online monitoring, while 40% of Europeans avoid online services known to monitor their activities (TNS Opinion & Social 2015).

4.3.3 Low trust in companies, higher trust in governmental institutions

For now, people do not really trust companies: only 3% of Europeans actually trust online companies. The recent scandals, such as the Cambridge Analytica case, made their trust shrink even more. This is because even with the data and privacy regulations, companies still share data without checking the nature of the users' data. On the other end, healthcare institutions and national authorities are the most trusted institutions with respect to data protection. Citizens have the feeling that their data are well protected by those institutions and that the organisations do not abusively use or share data with third parties. However, over the years, fewer and fewer people trust healthcare and governmental organisations, because these are getting targeted by cybercriminals (TNS Opinion & Social 2015).

Concerning EHRs, a majority of Europeans agree to sharing their health or medical data with their doctors. However, they are more reluctant to share their data with public authorities for research purposes or companies (Leibniz Institute for the Social Sciences).

National Data Protection Authorities are also trusted by citizens. A survey in 2015 shows that the majority of European citizens would ask these authorities for help in case of misuse of data, for instance (TNS Opinion & Social 2015).

4.3.4 Complicated privacy statement

About 70% of European citizens still want to consent to data collection, regardless of the nature of these data. However, only a small portion of the citizens actually read the privacy statements entirely (TNS Opinion & Social 2015). The main reason for this is related to the size of these privacy statements. Some 67% of the citizens find the statements too long to read, which is discouraging them (TNS Opinion & Social). For 38% of the citizens, the second reason not to read privacy statements is related to the difficulty of those statements. Long and complicated texts are made to discourage people from fully reading or understanding them (TNS Opinion & Social). These texts are complicated since companies use difficult legal terms to protect themselves from lawsuits (Moretty, Naughton 2014). Moreover, about 65% of privacy statements use irrelevant information just to confuse the readers (Australian Government 2013). However, a small amount of citizens believes that data protection regulations will protect them from abusive data use (TNS Opinion & Social).

4.3.5 Improve citizens' trust

Users store most of their personal data in personal devices, but they will not allow websites or online services to collect their data. A strong majority of about 9 out of 10 citizens does not want companies to access their data or install monitoring tools on their personal devices. This is because they fear to lose data from their personal computer or their mobile device (TNS Opinion & Social).

While citizens are not happy with how their data is being handled, different practices can improve trust in electronic devices and online services among Europeans. A positive impact might be gained from certifications or labels for the fair collection and use of data; the use of specific security technologies, such as the finger print reader, face recognition or even encryptions might positively influence the citizens. If online services use those certifications or labels, citizens might be more inclined to use those services (Leibniz Institute for the Social Sciences).

Even if citizens have concerns about their personal information and how their data is being collected, used or shared with third parties, a majority of them think that recent digital technologies have a positive impact on their lives (Leibniz Institute for the Social Sciences).

4.4 Regulations

Regulatory affairs about data protection are a real nightmare for companies. While data can easily cross borders all around the world, countries are only adopting national data regulations. Moreover, regulations tend to evolve slowly compared to new technologies. As a result, companies are confused whether they are allowed to use new technologies without getting in problems. The healthcare sector is concerned about this. In the case of eHealth, the biggest issue that IT software vendors encounter is the lack of guidance from the various governments. However, in various countries, the authorities also think the regulations for data are a matter of concern (HIMSS 2017).

In 2017, about 120 countries had a data protection law. This is an increase of 9 new countries compared to the year before, showing that countries are taking data protection seriously. On average, 5.4 new countries adopt data protection regulations annually. Besides, more than 30 countries are undergoing changes in their data protection regulations annually (Greenleaf 2017).

4.4.1 International agreement regulations

Various international directives about data protection were made by various international organisations. The purpose is to uniformise regulations around the world while most of the countries are creating their own regulations. The purpose of those directives is to establish the same regulatory basis in every country. A directive is not a law that can be used immediately, but a set of guidelines with points that countries have to discuss, maybe alter and eventually adopt. However, governments are free to decide how strict they are going to be in each point and they are free to add points that are not listed in the directive.

Today, there are four different international directives. In 1948, the first one was established by the United Nations which protects privacy in its Universal Declaration of Human Rights (UDHR, article 12). This is by far the directive adopted most often since it is ratified by 167 countries who guarantee to not interfere with the privacy of their citizens. However, the UDHR is too general and thus does not efficiently protect all aspects of privacy (United Nations 2018).

The second international framework was made by the OECD, the Organisation for Economic Cooperation and Development. In 1980, they released their Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. In its guidelines, OECD introduced the eight principles of fair use and collection of personal data. In 2013, the OECD updated its guidelines to make them more accurate about today’s world. In this new paper, OECD introduced the principle of accountability and updated the international cooperation guidelines to improve transborder data flows. Those principles are now widely spread and used in most data protection regulations. However, although OECD’s guideline is not exclusive for its member states, it has only a limited impact worldwide since only 32 countries have adopted the OECD guidelines (OECD 2018).

The third international data protection agreement is known as the Council of Europe Convention 108 (CoE 108). This agreement is by far the most widely used and the strictest one worldwide. The CoE 108 was published for the first time in 1981, by the Council of Europe, but it is not limited to European countries, since the CoE 108 is also open to any country that is not a state member. In total, 53 countries have ratified CoE 108, while only 46 of them are COE member states (Council of Europe 2018a). Three more countries have started the adoption of the agreement after they announced their wish to sign it. CoE 108 is known to be the strictest international agreement on data protection. Based on the OECD guidelines, CoE 108 is an adapted framework that is used as the basis for European data protection regulation. After the European Union announced their new General Data Protection Regulation (GDPR) in 2016, the Council of Europe has released the third version of CoE 108 to be in phase with the new GDPR (Council of Europe 2018b).

In 2005, the last international agreement about data protection is carried by the International Conference of Data Protection and Privacy Commissioners (ICDPPC). The ICDPPC works like an international organisation, such as the World Trade Organisation (ICDPPC 2018). Each year, the data protection authorities from all countries meet up to discuss which steps to take next to ensure more privacy for citizens in all countries. At the end of each conference, the ICDPPC releases a resolution that all members have to follow. Their best known conference took place in Montreux, Switzerland. At the end of this 27th conference, the ICDPPC issued a resolution to not only improve regional regulation, but to work on a unique international regulation for the first time (ICDPPC 2005). However, even if the ICDPPC is the largest cooperation between National Data Protection Authorities, its impact is still limited. To begin with, they do not have a proper infrastructure. Thus, the ICDPPC cannot check whether countries have concretely adopted the resolutions or not. Furthermore, the organisation is mainly using the OECD or CoE 108 guidelines to establish the resolutions. However, since the conferences are held and followed by data protection commissioners, it allows countries to share specific issues that they are facing about establishing data protection and privacy laws and counteracting the threats of new technologies. It also helps to understand the latest challenges and prepare other countries to face these as well if they did not show up at the convention (UNCTAD 2016).

In the end, only the CoE 108 is playing a major role in international data protection agreements. The UN, OECD and ICDPPC do not have the proper infrastructure to monitor countries that sign the resolutions (UNCTAD 2016). Thus, they cannot ensure that all signing members have integrated the mandatory points in their own data protection regulation. Moreover, organisations such as the UN or ICDPPC have hardly any power over country authorities. For those reasons, the CoE 108 is the most serious international data protection agreement. As the CoE is part of the European Union, it has great power over the rest of the world, since non-member countries are monitored by data protection authorities from European countries. For instance, the Commission Nationale de l’Informatique et des Libertés (CNIL), the French data protection authority, provided an interactive map for European citizens. On this map, the CNIL provides information on other countries about their level of data protection and privacy (CNIL 2018). With this map, the CNIL do not only give information about who has signed the agreement, but also about their current enforced laws. While the United Nations assess there are more than 100 countries with proper data protection regulations (UNCTAD 2016), the European Union estimates are completely different. For them, only a few countries have regulations that match the CoE 108 basic points.

4.4.2 Regional agreements

Alongside international agreements, countries are also establishing regional agreements to ensure the free flow of information with nearby countries. Most of the time, those regulations are carried by the economic alliance from the region. For instance, in the European Economic Area (EEA), composed of 31 countries, the newly introduced General Data Protection Regulation (GDPR) represents the regional agreements, based on the CoE 108. This regulation was made by the European Parliament and the European Council for all member states of the EU. But, other nearby country partners also use the GDPR as a basis to enforce their own data protection regulations to comply with the GDPR, since they have ratified the CoE 108. This is the case for countries like Norway, Switzerland and Iceland. These countries have either announced a revision of their current law to comply with GDPR (Swiss Federal Department of Justice 2017) or just integrated it into their own law (DLA Piper 2017).

Similar initiatives can be found in other parts of the world. On the African continent, the African Union (AU), composed of 55 countries, has adopted the African Union Convention on Cybersecurity and Personal Data Protection in 2014 (African Union 2014). The convention works like the CoE 108, allowing member states to use it as a guideline while enacting their own laws. In 2018, only two members, Mauritius and Senegal, have ratified the convention, while ten others have signed it and are preparing their own bill (African Union 2018). The Pacific region has also adopted various data protection regulations with the Asian Pacific Economic Cooperation (APEC), with the establishment of privacy principles, in 2005, based on OECD's guidelines from 1980 (APEC 2005).

While a universal data protection regulation would be easy for all companies worldwide, the regional agreements or regulations are already making data sharing easier for companies. When the Data Protection Directive 95/46/EC (DPD) was established within the European Union, it was easier for companies to share data across the European Union, since companies only had to use the same guidelines. Moreover, if companies outside Europe wished to deal with companies within the EU, they only had to comply with the CoE 108 guideline. That was the common practise between companies established in the United States of America. Data protection regulations are less strict in USA, thus the EU made an agreement with the US Department of Commerce known as Safe Harbour in 2000 (European Parliament and of the Council 2000). Under this agreement, American companies had to get a certification from the US Department of Commerce to access the EU digital market. Companies had to prove they complied with the CoE 108 guidelines, otherwise they would not get the certification. As soon as a company gets a certification, it will be on a list stating that the company is allowed to share data with or get data from other EU companies. Due to the privacy incidents with US based companies, in particular Facebook, the European Court of Justice cancelled the Safe Harbour agreement in 2015 (Gibbs 2015). A new draft called Privacy Shield was then enacted a year later (CNIL 2017). An agreement similar to Privacy Shield can be found within the APEC with its Cross Border Privacy Rules System (CBPRS). It works the same way as the Privacy Shield. APEC countries have to enforce their own data protection laws. Thus, non-APEC based companies that wish to collect or share information with companies established inside APEC have to get the APEC CBPRS certification first (CBPRS 2011).

4.4.3 European Digital Single Market

Since 2015, the European Parliament and Council have adopted the Digital Single Market plan (European Commission 2015). The EU has understood the importance of ICT in its economy and thus is taking measures to ensure the free, secure and fast flow of data within the EU. To make this possible, the EU is undergoing significant changes in its old laws. For a couple of years already, the EU has been changing all its old directives into regulations. The difference lies in the fact that regulations are ready-to-use laws and enacted at the same time by all member states. The purpose of this practice is to standardise all member states' laws, providing not only the same rights to all of its citizens, but also making compliance for companies easier. Concerning eHealth, the EU has already changed its old data protection directive and will change its medical device directive and in vitro device directive by 2020.

4.4.3.1 General Data Protection Regulation

The General Data Protection Regulation 2016/679 (GDPR) (European Commission and of the Council 2016) is the latest European law on data protection. The GDPR is the update of the old Data Protection Directive 95/46/EC (European Commission and of the Council 1995). While most of the text remained unchanged from the DPD, the GDPR brings some novelty by empowering Europeans and by also making companies more responsible.

The first major change concerns the definition of personal data. In its second article, the GDPR has increased the list of information that can be defined as personal data, such as physical and psychological data. By being more specific about the definition of personal data, the EU wants to avoid a situation in which companies play with words to determine whether data is personal or not.

The second major change is related to the empowerment of European citizens. Under the new regulation, EU citizens will see their rights increase and they will have full control over their data (EU GDPR Compliant). On the one hand, companies have to provide a comprehensive, short and easy to read privacy statement. On the other hand, companies are not allowed to force citizens to consent if they want to use a product or service. Thus, citizens will be able to use any service without companies collecting any data. As a result, data will remain in the hands of the citizens even if they consent for the information to be used. At any time, citizens can get all information about their data, can ask to stop the practice of collecting and keeping data, and can transfer data from one company to another without needing a reason or being forgotten by the companies.

The third major change is the introduction of accountability and privacy by design. With the GDPR, the European Union wants companies to be more accountable for all issues that could happen with the data they store. On the one hand, data processors have to keep track of all data processing they have done. On the other hand, the Data Protection Officer (DPO) has to ensure that no data abuse takes place within the company and all necessary measures were taken to protect data. If a company fails to comply with the regulation, data protection authorities can threaten them with fines going up to 20 million euros or 4% of the company's annual turnover, whichever is higher.

Finally, the last major change is related to the scope of the regulation. The DPD was only effective within the EEA, leaving National Data Protection Authorities without power outside the EEA. With the GDPR, this situation has changed since all companies targeting Europeans can be subjected to a check by National Data Protection Authorities, since all companies have to comply with the regulation.

4.4.3.1.1 Impact on healthcare industry

The new regulation will have a significant impact on health delivery organisations. Since all of these organisations collect and use patients' biometric, genetic and health related data, they have to comply with the GDPR. Processing those kinds of data is allowed under specific conditions (article 9 paragraph 2). However, this also means that all organisations or companies using this kind of data have to comply with the regulation. While life science companies can easily install necessary measures to secure patients' data and setup protocols to monitor the data flow, HDOs will probably struggle to do so. As can be seen in the 2017 European eHealth survey, health delivery organisations are more challenged than other healthcare stakeholders. The lack of funds does not allow HDOs to hire enough skilled IT staff or to establish a proper and safe IT infrastructure (HIMSS 2017). This situation can also push ICT companies to not enter the healthcare market due to the high barriers around data safety and the prohibition to process data for other purposes than mentioned in the agreement.

4.4.3.2 New medical devices regulation

On the 25th of May, 2017, the European Union replaced the old Medical Device Directive 93/42/EEC (MDD) and the In Vitro Device Directive 98/79/EC (IVDD) with the new Medical Device Regulation 2017/745 (MDR) and the In Vitro Device Regulation 2017/746 (IVDR) (European Commission 2018). The MDR is expected to come into effect by the early 2020s, while the IVDR will be effective only two years later. The reason the European Parliament and the European Council changed this regulation is because of a succession of events which involved medical devices. Since 2010, the number of medical devices recalled from companies by National Health Authorities have increased due to safety issues (EY 2016). As a result, the EU revised its directive about medical and in vitro devices and came up with the new regulations of the MDR and the IVDR.

As for the GDPR, the EU introduced regulations to standardise the EEA market. If a device has been approved in one country, it can be freely used in other countries as well. This again benefits patients as well, since they can use the best devices available. However, this will again impact the healthcare industry. Not only new medical devices and software programs will have stricter ante- and post-market safety and efficiency checks, but the devices or software used currently might be checked and found not to be up to the standard. In 2013, when the new regulations were in preparation, Eucomed surveyed life science companies to understand the financial impact of the new regulation. It appeared that an additional 17.5 billion euro would be necessary to get authorisations to access the market (MedTech Europe 2013). Moreover, the regulations would postpone the entry of new devices onto market for 3 to 5 additional years. This was because additional safety and efficiency checks had to be carried out. In the end, it was the small and medium enterprises (SMEs) that were hurt the most in this process. Big and well-established life science companies have protocols and specific teams to get the certification faster. However, 95% of the life science industry is composed of SMEs, which only have few products. This means increasing certification control will only dissuade companies from trying to make health related products.

4.4.3.2.1 Impact on eHealth solutions

The new MDR and IVDR regulations will heavily impact the development of eHealth solutions, especially the mobile health (mHealth) industry. Even though the mHealth industry is the largest market in the eHealth industry, the increased control that is needed and the classification of software as medical devices will probably slow down its development. Moreover, the increased cost in safety and efficiency checks will lead to a decrease in safety investments. Since most electronic health devices are barely protected, SMEs will probably be less keen on improving the safety of these devices because of this increase in checks in both the ante- and post-market. Moreover, software can now also be considered as a medical device according to the law. Thus, medical software will also get controlled more strictly than before. However, this will not only impact HDOs, since this can also dissuade device or software makers to directly propose eHealth solutions to consumers considering the GDPR. If this happens, software and device makers have to propose a proper security architecture as a solution. Already now, they are struggling with security, so the increased expenditures in future testing will have a negative impact on eHealth solution development.

5. Recommendations

In order to secure patients’ sensitive data, the following recommendations may be considered for follow-up action.

5.1 Labels, certifications and standards

Regardless of the next solutions that might be adopted, getting certifications or labels is probably the most obvious solution. While labels or certifications do not directly protect eHealth solutions, it proves that companies or HDOs that own a label or certification have taken enough measures to protect the security and privacy of their consumers’ data. This means they have established a strong IT security architecture and protocols. Since certifications and labels are not granted eternally, companies are forced to regularly audit their products or IT infrastructure to verify whether they still match with the minimum security and privacy protection required for the certifications or labels.

Companies themselves can audit their own IT infrastructure or product. However, it is better that an external IT expert conducts the audit. On the one hand, an external expert does not know the product or the infrastructure, so (s)he will have an unbiased view. On the other hand, expert auditors are experienced and they will have seen all kinds of products or IT infrastructures. Thus, they can include potential risks that they have seen in other infrastructures, but that the company under audit has not even thought about. By performing an audit, companies will come to realise their weak points for which they can take proper actions, in order to secure their product or IT infrastructure properly.

After completing their audit, companies can apply for certification. For this part, it is recommended they choose a company from the lists of the National Data Protection Authorities. Two reasons can lead to this decision. To start out with, private companies providing a privacy seal might not be as reliable as they might show. That was the case of TrustArc, previously known as TRUSTe. The company was caught by the Federal Trade Commission in 2014 for not conducting re-certification processes (Federal Trade Commission 2014). Over 1000 companies that already had their TRUSTe certification, had not received any re-certification checks between 2006 and 2013, even though their certification was renewed every year. TRUSTe had been responsible for delivering certifications for the Safe Harbour regulation. Besides, Europeans have a high trust in National Data Protection Authorities, as was observed earlier. Thus, using certifications or labels issued by National Data Protection Authorities directly or their approved partners, is the best solution to comply with the new regulations and to be sure that data is protected by state-of-art solutions. National labels can be found directly through the National Data Protection Authorities. For instance, the CNIL, the French data protection authority, provides all information on how to conduct an audit and the requirements for the CNIL label (CNIL 2018a). Moreover, the organisation also provides a list of all companies owning a CNIL label, making it easy for consumers, partners or citizens to check whether a specific company owns the labels. To find a private certification company or an auditor, EuroPriSe, short for European Privacy Seal, provides a list with trusted experts from within and outside Europe (EuroPriSe 2018). EuroPriSe, is a European Union backed organisation to provide privacy labels or certification.

The adoption of ISO standards is also recommended. Again, an ISO certification does not entirely guarantee the security of products or solutions. However, they can guarantee that products or solution makers have followed specific steps to ensure the production of a safe and reliable product. Companies with the ISO certification are also regularly audited by independent companies. For instance, complying with the new ISO 13485:2016 standard can help to avoid troubles with the future MDR and IVDR and can accelerate the adoption of, for instance, the CE marking. This certification mark is the seal saying that a product can be sold in the EU.

5.2 Using latest data protection solutions

Usage of software data protection solutions is recommended. As was observed in chapter 4, security is not a domain of expertise for either healthcare solution makers or users.

However, this should not be a reason to not take any steps to protect the solutions and make patients' data safe. Moreover, with the new GDPR it will be mandatory for companies dealing with data to use new solutions to provide enough data security.

The first kind of software that can be used, is considered as middleware. This type of software cannot be used on its own. It is only a piece of code that is meant to be integrated into other software, working like a feature. Middleware can easily be added to any medical device or medical software to make data transfer more secure. Middleware is the most versatile solution since it can adapt to any medical product or service in line with the company's needs and wishes. It also may be one of the most complicated solutions to use since companies have to integrate middleware into their product. Even if a company can be supported by the middleware seller to integrate the software, it is usually up to the company's IT workers to actually do so.

The next solution is to use new technologies, such as blockchain. "Blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called block. Each block contains a timestamp and a link to a previous block". For years, interest in blockchain has grown among ICT companies. This is because of its capabilities to secure data transfer and to have a great traceability . However, blockchain is relatively new and might not be interoperable with all existing devices or software. Moreover, compared to middleware, blockchain can only be integrated in the whole network and not in a specific machine alone. Thus, it is less versatile than the use of middleware and besides, it is more expensive.

5.3 Adopt a subscription business model

Today, most life science companies use a product sales business model. This means that companies basically develop a product, sell it and use the money gathered from the sales to build the next version. However, with the digitisation of society, developing new products every year is not the solution anymore, because the old products do not receive updates. This can be seen in ICT companies such as Microsoft or Adobe. Both companies used a product sales business model in the past.

However, this product sales business model is not efficient at all any more. On the one hand, the product was too expensive, since it was a one-time purchase. Thus, companies had to charge as much as they could to generate revenue. On the other hand, the development required a lot of resources. Since the products were usually redesigned from scratch, the development of new products started even before the previous ones were released. With the introduction of the subscription business model, companies do not develop a new product on a specific schedule, but they provide upgrades to existing products. The upgrades can be the addition of new functionalities or improvements in security or stability. In the end, the ICT companies that adopted this business model have been far more profitable than before and they have also been more profitable than compared to other companies that still use the product sales business model.

By adopting subscription models, life science companies providing medical devices or software will be able to solve security issues while improving and securing their revenue. As was observed in chapter 4, HDOs often still use end-of-life devices or software. Since HDOs do not have the funds to constantly buy new devices and software, these devices are outdated. For now, HDOs can actually already lease medical devices. However, this is not a great solution, since it will just add a costly intermediary and leasing companies are only providing the same devices produced by device makers. With the subscription model, device and software makers will be able to provide HDOs with cheaper solutions that have a longer life span, which will increase the security of medical devices and software over time.

5.4 Joint eHealth association

The concept of eHealth is to network the whole health sector, which will result in a better cooperation for various tasks. However, the development of new eHealth solutions is still not done in cooperation. Companies involved in the health industry prefer to limit partnership with other companies involved in the health industry; they want to acquire new technologies or cooperate with companies from outside the sector in order to prevent competitors from getting a greater market share. However, this practice works against the concept of eHealth, which encourages a greater cooperation within the industry.

Besides, eHealth solutions, including all devices and software programs, are getting more and more complex, due to all the technologies and functionalities involved. Consequently, the chance that eHealth solutions have vulnerabilities is also getting greater, making them more prone to cyber-attacks. As seen previously, eHealth solution makers and consumers, such as HDOs, device makers, doctors and patients, find it complicated to protect the eHealth solutions and, in general, IoT devices just lack security.

To face those issues, companies should found an association that can act like a bridge between the various health sector stakeholders, but also connect ICT companies not present in the industry. The association has to be independent and has to be financed by its members, who can either be eHealth solution manufacturers, eHealth intermediate product companies (such as MEMS companies), IT companies and eHealth consumers or users. The members will pay an annual fee to ensure the run of the association and to have access to all services. The association will have three defined functions that will ensure the creation of many more secure and “privacy” protecting eHealth products and IT infrastructure. These three functions are eHealth customs, a vulnerability reward program and an eHealth security advisor.

5.4.1 EHealth customs

The first function is probably the most important. The association will play the role of eHealth customs. One of the biggest problems in eHealth solutions, especially in medical devices, is their complexity, since they use many different intermediate products, such as various MEMS. However, if these intermediate products are not protected before they are combined to produce medical devices, the intermediate products will remain vulnerable parts of the total eHealth solution. This can be avoided by essentially building an eHealth solution with parts that are already secured. This is where the eHealth customs will come into play.

EHealth customs is the first function in which the association will be active, by ensuring that eHealth solution consumers get secure products out of the box. To achieve that, the association will make a list of the parts that are actually certified by European and ISO standards in security and privacy for medical devices and medical infrastructures. By listing those parts, eHealth solutions makers can safely choose secure components or middleware to integrate into their products. This will make the products easier to secure since parts are already protected. Consequently, eHealth solution makers’ expenditure in security will drop. Moreover, the devices might get their certification faster since they comply with the latest European regulations. For the eHealth solution consumers, it will also make the search for safe solutions easier. Using eHealth solutions secured straight out the box will also make the spending in security lower, especially in large infrastructures in which one non-secure device or piece of software can compromise the whole. The consumers will also have a better trust in the producers since they are certified, so the products they purchase already integrate safety protocols and comply with privacy regulations. Finally, by listing all the eHealth solutions and intermediate product makers, the companies which produce eHealth solutions will also benefit from being on the eHealth customs list. Thus, companies on the list can be easily located by interested consumers.

5.4.2 EHealth vulnerability reward program

The second function of the eHealth association will be to establish a vulnerability reward program based on the Google vulnerability program. Most life science companies (like in the MedTech, BioTech and the pharmaceutical industry) are small companies which do not exceed 50 employees. Consequently, it is complicated for most of these individual companies to establish a vulnerability reward program such as Google’s, since they do not have the resources and most often they only have a few products. However, they could benefit from such a vulnerability reward program under the flag of the eHealth association. Hackers working for the eHealth association will be able to find vulnerabilities for any final or intermediate product listed or possibly wanting to be listed. For any vulnerability found and explained how to exploit it, hackers will be paid a varying amount of money depending on the gravity of the vulnerability. If hackers provide a fix or patch for the vulnerability, they will be paid extra. With this system, the eHealth solution producers and part makers will be able to reduce vulnerabilities significantly and faster due to the open collaboration type of work, since the eHealth association will play the central role in bridging the gap between hackers and solution makers. Again, this could have a positive impact for eHealth solution consumers since they can count on the quality of the products that are followed and updated by the producers, not only with respect to functionality or stability, but also with respect to security and privacy. Consumers will have a higher trust in eHealth solution producers, which should accelerate the adoption of eHealth.

5.4.3 EHealth security advisor

The last function that the eHealth association will have is the eHealth advisor who will have two tasks. The first task of the eHealth advisor will be to track all the issues that eHealth solution consumers have encountered, from bug to human error to cyberattack. With the information collected, the association will publish an annual report with all the findings. The report allows the members to realise what kind of problems their product is facing or might be facing. For instance, if a kind of malware is spreading to various medical devices, companies will be able to react and stop its spread. It can also be used to improve the quality of a product if it has shown critical errors. This will spread awareness of all kinds of issues that consumers encounter and will lead to the faster improvement of eHealth products. Security will also be improved since the whole health industry will know what kind of cyber-attacks are trying to undermine their solutions.

The second task of the eHealth advisor will be to establish stress test programs. With the information collected from the devices and the requirement for security in EU regulations and international standards, it might be interesting to establish an easy to use stress test program, like the ones that are used in the finance industry. With it, all health sector stakeholders will be able to test the solutions, whether they are in production or in use. With this program, solution producers will be able to see if their existing or developing products are safe enough against the latest threats and if they comply with security and privacy standards. For the eHealth solution consumers, it will allow them to regularly check their infrastructure to understand the strengths and weaknesses of the infrastructure and to take measures if necessary. This will drastically improve the security of eHealth solutions and will ensure all health sector stakeholders to comply with the latest regulations.

More ideas can be found in the Appendix.

6. Conclusion

The role of computers and data has changed since the 1930s, from the first digital computer in 1939 to the current smartphones that are able to process lots and lots of information at the same time. In the past, stored data was difficult to access and use, while nowadays, with a click of the mouse button, you can access any file and any online service available. The healthcare sector also evolved significantly, especially during the past four decades. Healthcare workers can provide better healthcare by making use of new technologies, such eHealth, which automates medical services and tasks and improves the sharing of medical information. Nowadays, data is not secure. The healthcare sector also faces challenges in protecting medical data against theft and in sharing medical data between companies and services. The innovation of eHealth solutions may help overcome healthcare challenges, such as improving healthcare access and reducing its costs.

For now, the innovation of eHealth solutions is too slow. The most important improvements that can speed up innovations in eHealth are the use of security labels for (intermediate) eHealth products, the application of the latest data protection solutions, the adoption of subscription business models for eHealth device makers and software producers and the creation of a joint eHealth association. Out of these solutions, the joint association can probably make the biggest difference in the future. First of all, such an association will enable cheaper healthcare devices and software to be made. Besides, the production of those devices and software will be accelerated, because companies will have to spend less time on protecting these technologies, since they are already well protected. Furthermore, products will be available on the markets faster, because the intermediate products of the medical devices and software will already have the security certifications. This allows health authorities to spend less time on checking whether the products meet the regulations.

This research also contains some limitations, of which the large size of the topic was the most important one. This research focused on both data and eHealth, which are already vast topics by themselves. By combining these into one paper, the overall situation was described, but not the individual, smaller topics, such as how hospitals or medical device makers are handling data now.

This is where future research should start. Future researchers should focus on one specific stakeholder in the health sector to understand that particular stakeholder’s challenges regarding healthcare and data. For instance, how does this stakeholder protect healthcare data now and what can be improved. When looking at eHealth and data on an individual level, researchers can devise individual solutions for each stakeholder.

In the end, if this paper’s recommendations are followed and future research has been done lots of situations will improve. First of all, the lives of people will improve because of a larger amount of available medical devices and software. Secondly, companies can build their products more cheaply and bring them to the markets faster. And finally, the work of doctors will be made easier, since they can use all medical devices and software without worrying about possibly negative influences.

Bibliography

HAMELINK, Cees Jan, 1997. New information and communication technologies, social development and cultural change. *Pure.uva.nl* [online]. June 1997. [viewed 9 April 2018]. Available from:

https://pure.uva.nl/ws/files/2117542/35518_dp86.pdf

VDI NARCHRICHTEN, 2011. Industrie 4.0 : Mit dem Internet der Dinge auf dem Weg zur 4. industriellen Revolution. W*oflgang-wahlster.de* [online]. April 2011. [viewed 28.04.2018]. Available from:

http://www.wolfgang-wahlster.de/wordpress/wp-content/uploads/Industrie_4_0_Mit_dem_Internet_der_Dinge_auf_dem_Weg_zur_vierten_industriellen_Revolution_2.pdf

JOLLY, Rhonda, Dr., 2011. The e health revolution – easier said than done. *Aph.gov.au* [online]. 17 November 2011. [viewed 29.04.2018]. Available from:

https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1112/12rp03

MEDTRONIC, 2015. Medtronic Launches MiniMed 640G System, Breakthrough in Artificial Pancreas Technology, Outside the U.S.. *Newsroom.medtronic.com* [online]. 21 January 2015. [viewed 28 April 2018]. Available from:

http://newsroom.medtronic.com/phoenix.zhtml%3Fc%3D251324%26p%3Dirol-newsArticle%26ID%3D2009123

KLOET, Bas, VAN TILBURG, Paul, 2006. John Vincent Atanasoff Inventor of the Digital Computer. *Paul.lueon.net* [online]. 3 October 2006. [viewed 28.04.2018]. Available from:

http://paul.luon.net/essays/HoC-Atanasoff.pdf

BRINKMAN, W.F., HAGGAN, D.E., TROUTMAN, W.W., 1997. A history of the invention of the transistor and where it will lead us. *Ieeexplore.ieee.org* [online]. December 1997. [viewed 28.04.2018]. Available from:

https://ieeexplore.ieee.org/document/643644/

NABI KHAN, Rahat, 1987. La troisième révolution industrielle: tour d'horizon économique. *Unesdoc.unesco.org* [online]. July 1987. [viewed 28.04.2018]. Available from:

http://unesdoc.unesco.org/images/0007/000754/075479fo.pdf

NEYER, Mark P. The Electronic Numerical Integrator and Computer. *Cs.xu.edu* [online]. [viewed 28.04.2018]. Available from:

http://www.cs.xu.edu/~neyer/MachineOrg/ENIACPaper.pdf

OPEN DATA FOUNDATION. Inflation Calculator. *Officialdata.org* [online]. 10 August 2018. [viewed 28.04.2018]. Available from:

https://www.officialdata.org/1946-dollars-in-2018?amount=486000

NOBEL PRIZE, 2014. The History of the Integrated Circuit. *Nobelprize.org* [online]. 5 May 2003. 2014. [viewed 28.04.2018]. Available from:

https://www.nobelprize.org/educational/physics/integrated_circuit/history/

INTEL. The Story of the Intel 4004. *Intel.com* [online]. [viewed 28.04.2018]. Available from:

https://www.intel.com/content/www/us/en/history/museum-story-of-intel-4004.html

MOORE, Gordon E., 1975. Progress In Digital Integrated Electronics. *Eng.auburn.edu* [online]. 1975. [viewed 28.04.2018]. Available from :

http://www.eng.auburn.edu/~agrawvd/COURSE/E7770_Spr07/READ/Gordon_Moore_1975_Speech.pdf

INTEL, 2007. 60 years of the transistor : 1947-2007. *Uio.no* [online]. 2007. [viewed 28.04.2018]. Available from:

https://www.uio.no/studier/emner/matnat/ifi/INF5510/v17/material/timeline-intel-moores-law.pdf

COURTLAND, Rachel, 2017. Intel Now Packs 100 Million Transistors in Each Square Millimeter. *Spectrum.ieee.org* [online]. 30 March 2017. [viewed 28.04.2018]. Available from :

https://spectrum.ieee.org/nanoclast/semiconductors/processors/intel-now-packs-100-million-transistors-in-each-square-millimeter

NIELD, David, 2017. IBM's New Computer Chips Can Fit 30 Billion Transistors on Your Fingertip. *Sciencealert.com* [online]. 6 June 2017. [viewed 28.04.2018]. Available from :

https://www.sciencealert.com/new-computer-chips-can-fit-30-million-transistors-on-your-fingertip

PRIME FARADY PARTNERSHIP, 2002. An Introductioin to MEMS (Micro-Electromechanical Systems). *Lboro.ac.uk* [online]. January 2002. [viewed 28.04.2018]. Available from :

http://www.lboro.ac.uk/microsites/mechman/research/ipm-ktn/pdf/Technology_review/an-introduction-to-mems.pdf

MUNDARGI, Kishori, GRANDCHAMP, Myriam, KAJA, Sarawathi, CHANDRA, Sourav, SERRANO, Oscar, 2014. History of C Programming language. *Peoi.org* [online]. 23 May 2014. [viewed 28.04.2018]. Available from :

http://www.peoi.org/Courses/Coursesen/cprog/frame1.html

ROYAL PINGDOM 2009. Version 1.0 of today's most popular applications, a visual tour. *Royal.pingdom.com* [online]. 17 June 2009. [viewed 28.04.2018]. Available from :

https://royal.pingdom.com/2009/06/17/first-version-of-todays-most-popular-applications-a-visual-tour/

NETO, Maximilliano, 2014. A brief history of cloud computing. *Ibm.com* [online]. 18 March 2014. [viewed 28.04.2018]. Available from:

https://www.ibm.com/blogs/cloud-computing/2014/03/18/a-brief-history-of-cloud-computing-3/

LEINER, Barry, CERF, Vinton, CLARK, David, KAHN, Robert, KLEINROCK, Leonard, LYNCH, Daniel, POSTEL, Jon, ROBERTS, Larry, WOLFF, Stephen, 1997. A Brief History of the Internet. *internethalloffame.org* [online]. 1997. [viewed 28.04.2018]. Available from:

https://www.internethalloffame.org/brief-history-internet

INTERNET HALL OF FAME, 2018. Internet history, timeline. *Internethalloffame.org* [online]. 2018. [viewed 28.04.2018]. Available from:

https://www.internethalloffame.org/internet-history/timeline

CERN. The birth of the web. *Home.cern* [online]. 2018. [viewed 28.04.2018]. Available from:

https://home.cern/topics/birth-web

SLATER, William, 2002. Internet History and Growth. *Unc.edu* [online]. September 2002. [viewed 28.04.2018]. Available from:

https://www.unc.edu/~tgr/inls572/Slater2002-InternetHistory.pdf

CANNY, John, HARTMANN, BJÖRN, 2010. Beyond the Cell Phone – Introduction & Historical Perspective. Bid.berkeley.edu [online]. Fall 2010. [viewed 28.04.2018]. Available from:

http://bid.berkeley.edu/cs298-50-fall10/images/c/c2/Cs298-50-slides-01-intro.pdf

RICKER, Thomas, 2008. Jobs: App Store launching with 500 iPhone applications, 25% free. *Engadget.com* [online]. 10 July 2008. [viewed 28.04.2018]. Available from:

https://www.engadget.com/2008/07/10/jobs-app-store-launching-with-500-iphone-applications-25-free/?guccounter=1

ELMER-DEWITT, Philip, 2009. iPhone sales grew 245% in 2008 – Gartner. *Fortune.com* [online]. 12 March 2009. [viewed 28.04.2018]. Available from:

http://fortune.com/2009/03/12/iphone-sales-grew-245-in-2008-gartner/

BUSINESS INSIDER INTELLIGENCE, 2016. The App Store will have more than 5 million apps by 2020 which could be a major problem for small developers. *Businessinsider.fr* [online]. 12 August 2016. [viewed 28.04.2018]. Available from:

http://www.businessinsider.fr/us/the-app-store-will-have-more-than-5-million-apps-by-2020-which-could-be-a-major-problem-for-small-developers-2016-8

STATISTA, 2017. Cumulative number of apps downloaded from the Apple App Store from July 2008 to June 2017 (in billions). *statista.com* [online]. June 2017. [viewed 28.04.2018]. Available from:

https://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/

SCARSELLA, Anthony, STOFEGA, William, 2018. Worldwide Smartphone Forecast, 2018-2022. *Idc.com* [online]. March 2018. [viewed 28.04.2018]. Available from:

https://www.idc.com/getdoc.jsp?containerId=US43624118

DUNN, Jeff, 2017. PC sales in 2016 were the lowest they've been in a decade. *Businessinsider.fr* [online]. 17 January 2017. [viewed 28.04.2018]. Available from:

http://www.businessinsider.fr/us/pc-sales-decline-year-chart-2017-1

DOGTIEV, Artyom, 2018. App Download and Usage Statistics. *Businessofapps.com* [online]. 17 July 2018. [viewed 28.04.2018]. Available from:

http://www.businessofapps.com/data/app-statistics/

ITU, 2017. Global ICT developments, 2001-2017. *Itu.int* [online]. 2017. [viewed 28.04.2018]. Available from:

https://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2017/Stat_page_all_charts_2017.xls

REINSEL, David, GANTZ, John, RYDNING, John, 2017. Data Age 2025. *Seagate.com* [online]. April 2017. [viewed 28.04.2018]. Available from:

https://www.seagate.com/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

ERICSON, 2012. Traffic and market report. *Mb.cision.com* [online]. June 2012. [viewed 28.04.2018]. Available from:

http://mb.cision.com/Main/15448/2245894/661938.pdf

TELECOM-INFOCONSO. Les technologies 2G, 3G et 4G. *Telecom-infoconso.fr* [online]. [viewed 28.04.2018]. Available from:

http://www.telecom-infoconso.fr/les-technologies-2g-3g-et-4g/?format=pdf

3GPP, 2008. 3rd Generation Partnership Projet ; Technical Specification Group Radio Access Netwrok; Dual-Cell HSDPA operation. *3gpp.org* [online]. 6 December 2008. [viewed 28.04.2018]. Available from:

http://www.3gpp.org/ftp//Specs/archive/25_series/25.825/

ITU, 2010. ITU World Radiocommunication Seminar highlights future communication technologies. *Itu.int* [online]. 6 December 2010. [viewed 28.04.2018] Available from:

https://www.itu.int/net/pressoffice/press_releases/2010/48.aspx

OPENSIGNAL, 2018. The State of LTE (February 2018). *Opensignal.com* [online]. February 2018. [viewed 28.04.2018] Available from:

https://opensignal.com/reports/2018/02/state-of-lte

BROADBAND COMMISSION, 2017. The State of Braodband: Broadband catalyzing sustainable development. *Itu.int* [online]. September 2017. [viewed 28.04.2018] Available from:

https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.18-2017-PDF-E.pdf

BRYZEK, Janusz, Dr., 2012. Roadmap for the Trillion Sensor Universe. *Eecs.barkeley.edu* [online]. 2 April 2012. [viewed 28.04.2018] Available from:

https://www-bsac.eecs.berkeley.edu/scripts/show_pdf_publication.php?pdfID=1365520205

GRWOTHEABLER, 2017. Market Pulse Report, Internet of Things (IoT). *Growthenabler.com* [online]. April 2017. [viewed 28.04.2018]. Available from:

https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

INTEL, 2018. Inforgraphie Guide de l'internet des objets. *Intel.fr* [online]. 2018. [viewed 28.04.2018]. Available from:

https://www.intel.fr/content/www/fr/fr/internet-of-things/infographics/guide-to-iot.html

HILBERT, Martin, 2012. How Much Information is There in the "Information Society"?. *Martinhilbert.net* [online]. 2012. [viewed 28.04.2018]. Available from:

http://www.martinhilbert.net/Hilbert_Significance_pre-publish.pdf

HILBERT, Martin, 2018. Information & communication quantity. *Martinhilbert.net* [online]. 18 January 2018. [viewed 28.04.2018]. Available from:

http://www.martinhilbert.net/information-communication-quantity/

U.S. DEPARTMENT OF COMMERCE, 2017. 2017 Top Markets Report Media and Entertainment Sector Snapshot. *Trade.gov* [online]. 2017. [viewed 28.04.2018]. Available from:

https://www.trade.gov/topmarkets/pdf/Top%20Markets%20Media%20and%20Entertinment%202017.pdf

GOLDMAN SACHS, 2014. The Internet of Things: Making sense of the next mega-trend. *Goldmansachs.com* [online]. 3 September 2014. [viewed 28.04.2018]. Available from:

https://www.goldmansachs.com/our-thinking/outlook/internet-of-things/iot-report.pdf

RAPOLU, Bhoopathi, 2016. Internet Of Aircraft Things: An Industry Set to Be Transformed. Aviationweek.com [online]. 18 January 2016. [viewed 28.04.2018]. Available from:

http://aviationweek.com/connected-aerospace/internet-aircraft-things-industry-set-be-transformed

THE NEW YORK TIMES, 2012. Milestones in Medical Technology. *Archive.nytimes.com* [online]. 10 October 2012. [viewed 28.04.2018]. Available from:

https://archive.nytimes.com/www.nytimes.com/interactive/2012/10/05/health/digital-doctor.html?_r=2#/

LIU, Thomas T., PhD, 2004. *ECE187 Introduction to Biomedical Imaging* [PDF Document]. 2004.

Course material: Course “MRI Lecture”, University of California San Diego, Fall Quarter 2004

WHO, 2017. World Bank and WHO: Half The world lacks access to essential health services, 100 million still pushed into extreme poverty because of health expenses. *Who.int* [online]. 13 December 2017. [viewed 28.04.2018]. Available from:

http://www.who.int/news-room/detail/13-12-2017-world-bank-and-who-half-the-world-lacks-access-to-essential-health-services-100-million-still-pushed-into-extreme-poverty-because-of-health-expenses

UNITED NATIONS, 2015. World Population Prospects. *Esa.un.org* [online]. 2015. [viewed 28.04.2018]. Available from:

https://esa.un.org/unpd/wpp/Publications/Files/WPP2015_Methodology.pdf

ANDERSON, Gerard, PhD., 2011. Responding to the Growing Cost and Prevalence of People With Multiple Chronic Conditions. *Oecd.org* [online]. 2011. [viewed 28.04.2018]. Available from:

https://www.oecd.org/els/health-systems/48245231.pdf

IBIS CAPITAL, 2016. Global HealthTech Investement Report. *Cdn2.hubspot.net* [online]. 2016. [viewed 28.04.2018]. Available from :

https://cdn2.hubspot.net/hubfs/681972/HTX%20-%20Health%20Branding%20and%20Imagery/2016_IBIS_Capital_Global_HealthTech_Investment_Report.pdf

THE WORLD BANK, 2018. Current health expenditure (% of GDP). *Data.worldbank.org* [online]. 2018. [viewed 28.04.2018]. Available from:

https://data.worldbank.org/indicator/SH.XPD.CHEX.GD.ZS?end=2015&start=2000&type=shaded&view=chart

SWISS FEDERAL OFFICE OF PUBLIC HEALTH, 2007. Stratégie Cybersanté (eHealth) Suisse. *E-health-suisse.ch* [online]. June 2007. [viewed 28.04.2018]. Available from:

https://www.e-health-suisse.ch/fileadmin/user_upload/Dokumente/2007_2008/F/070627_strategie_cybersante_ehealth_suisse_resume_F.pdf

WHO, 2005. Resolutions and decisions, fifty-eighth world health assembly. *Who.int* [online]. 25 May 2005. [viewed 28.04.2018]. Available from:

http://www.who.int/healthacademy/media/WHA58-28-en.pdf

WHO, 2016. Global diffusion of eHealth: Making universal health coverage achievable. *Apps.who.int* [online]. December 2016. [viewed 28.04.2018]. Available from:

http://apps.who.int/iris/bitstream/handle/10665/252529/9789241511780-eng.pdf?sequence=1

WHO, 2018. National HER system exists. *Gateway.euro.who.int* [online]. 2018. [viewed 28.04.2018]. Available from:

https://gateway.euro.who.int/en/indicators/ehealth_survey_84-has-a-national-ehr-system/visualizations/#id=31759

EUROBAROMETER, 2017. Special Eurobarometer 460: Attitudes towards the impact of digitisation and automation on daily life. *Data.europe.eu* [online]. 10 May 2017. [viewed 28.04.2018]. Available from:

https://data.europa.eu/euodp/en/data/dataset/S2160_87_1_460_ENG

RESEARCH 2 GUIDANCE, 2017. mHealth App Economics 2017/2018. *Research2guidance.com* [online]. November 2017. [viewed 28.04.2018]. Available from:

https://research2guidance.com/wp-content/uploads/2017/11/R2G-mHealth-Developer-Economics-2017-Status-And-Trends.pdf

OECD, 2016. Health at a Glance: Europe 2016. *Oecd.org* [online]. 23 November 2016. [viewed 28.04.2018]. Available from:

http://www.oecd.org/health/health-at-a-glance-europe-23056088.htm

RTS, 2017. Mission allongée et prolongée pour les bus autonomes à Sion. *Rts.ch* [online]. 17 October 2017. [viewed 28.04.2018]. Available from:

https://www.rts.ch/info/regions/valais/9005727-mission-allongee-et-prolongee-pour-les-bus-autonomes-a-sion.html

MOON, Mariella, 2018. Baidu will deploy its self-driving buses in Japan. *Engadget.com* [online]. 7 April 2018. [viewed 28.04.2018]. Available from:

https://www.engadget.com/2018/07/04/baidu-self-driving-buses-japan/

HAWKINS, Adres J., 2018. GM will make an autonomous car without steering wheel or pedals by 2019. *Theverge.com* [online]. 12 January 2018. [viewed 28.04.2018]. Available from:

https://www.theverge.com/2018/1/12/16880978/gm-autonomous-car-2019-detroit-auto-show-2018

NESTA, 2015. Skills of the datavores talent and the data revolution. *Media.nesta.org.uk* [online]. July 2015. [viewed 28.04.2018]. Available from:

https://media.nesta.org.uk/documents/skills_of_the_datavores.pdf

FORRESTER, 2014. The Forrester wave: Big Data Hadoop solutions, Q1 2014. *Forrester.com* [online]. 27 February 2014. [viewed 28.04.2018]. Available from:

https://www.forrester.com/The+Forrester+Wave+Big+Data+Hadoop+Solutions+Q1+2014/-/E-PRE6807

KPMG, 2015. Clarity on Data & Analyitics. *Assets.kpmg.com* [online]. 2015. [viewed 20.04.2018]. Available from:

https://assets.kpmg.com/content/dam/kpmg/pdf/2016/02/ch-pub-20160122-clarity-on-data-analytics-en.pdf

EUROPEAN COMMISSION, 2017. Final results of the European Data Market study measuring the size and trends of the EU data economy. *Ec.europa.eu* [online]. 2 May 2017. [viewed 06.03.2018]. Available from:

https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy

GARESSUS, Emmanuel, 2017. La directive sur la protection des données sera le cauchemar de 2018. *Letemps.ch* [online]. 13 November 2017. [viewed 14 May 2018]. Available from:

https://www.letemps.ch/economie/directive-protection-donnees-sera-cauchemar-2018

LEWIS, Paul, 2018. Utterly horrifying: ex-Facebook insider says covert data harvesting was routine. *Theguardian.com* [online]. 20 March 2018. [viewed 27 March 2018]. Available from:

https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas

SEYDTAGHIA, Anouch, 2017. Comment un téléviseur peut vous espionner. *Letemps.ch* [online]. 7 February 2017. [viewed 5 May 2018]. Available from:

https://www.letemps.ch/economie/un-televiseur-espionner

SZADKOWSKI, Michaël, 2013. Prism, Snowden, surveillance : 7 questions pour tout comprendre. *Lemonde.fr* [online]. 2 July 2013. 8 August 2013. [viewed 19 May 2018]. Available from:

https://www.lemonde.fr/technologies/article/2013/07/02/prism-snowden-surveillance-de-la-nsa-tout-comprendre-en-6-etapes_3437984_651865.html#ancre2

LESECHOS, 2017. La NSA a collecté plus de 150 millions de relevés téléphoniques en 2016. *Lesechos.fr* [online]. 3 May 2017. [viewed 3 April 2018]. Available from :

https://www.lesechos.fr/03/05/2017/lesechos.fr/0212033767571_la-nsa-a-collecte-plus-de-150-millions-de-releves-telephoniques-en-2016.htm

BROSTRA, Rosa, 2018. La reconnaissance faciale se répand en Chine. *Letemps.ch* [online]. 10 January 2018. [viewed 4 May 2018]. Available from:

https://www.letemps.ch/economie/reconnaissance-faciale-se-repand-chine

IBM, 2017. IBM X-Force Threat Intelligence Index 2017. *Public.dhe.ibm.com* [online]. 2017. [viewed 17 March 2018]. Available from:

https://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03140usen/WGL03140USEN.PDF

GOOGLE, 2018. Google Vulnerability Reward Program (VRP) Rules. *Google.com* [online]. 2018. [viewed 26 May 2018]. Available from:

https://www.google.com/about/appsecurity/reward-program/

KELLER, Jan, 2018. Vulnerability Reward Program: 2017 Year in Review. *Security.googleblog.com* [online]. 7 February 2018. [viewed 6 May 2018]. Available from:

https://security.googleblog.com/2018/02/vulnerability-reward-program-2017-year.html

ROUSE, Margaret, 2017. Vulnerability disclosure. *Searchsecurity.techtarget.com* [online]. October 2017. [viewed 9 June 2018]. Available from:

https://searchsecurity.techtarget.com/definition/vulnerability-disclosure

KESSEM, Limor, 2017. WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerabilities. *Securityintelligence.com* [online]. 14 May 2017. [viewed 7 March 2018]. Available from:

https://securityintelligence.com/wannacry-ransomware-spreads-across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/

SANCHO, David, HUQ, Numaan, 2017. Cashin in on ATM Malware. *Documents.trendmicro.com* [online]. 2017. [viewed 19 March 2018]. Available from:

https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf

BUSINESSWIRE, 2016. Softchoice Finds an Increasing Number of Businesses with At-Risk Devices in Their Corporate Networks. *Businesswire.com* [online]. 19 September 2016. [view 24 April 2018]. Available from:

https://www.businesswire.com/news/home/20160919005893/en/Softchoice-Finds-Increasing-Number-Businesses-At-Risk-Devices

GLOBALSTATS, 2018. Mobile Operating System Market Share Worldwide. *Gs.statcounter.com* [online]. 2018. [viewed 2 May 2018]. Available from:

http://gs.statcounter.com/os-market-share/mobile/worldwide

DEVELOPERS, 2018. Distribution dashboard. *Developer.android.com* [online]. 23 July 2018. [viewed 6 August 2018]. Available from:

https://developer.android.com/about/dashboards/

MALCHEV, Iliyan, 2017. Here comes Treble: A modular base for Android. *Android-developers.googleblog.com* [online]. 12 May 2017. [viewed 14 June 2018]. Available from:

https://android-developers.googleblog.com/2017/05/here-comes-treble-modular-base-for.html

O'DONNELL, Lindsey, 2018. IoT Security Concerns Peaking – With no End In Sight. *Threatpost.com* [online]. 19 April 2018. [viewed 21 April 2018]. Available from:

https://threatpost.com/iot-security-concerns-peaking-with-no-end-in-sight/131308/

SYMANTEC, 2018. Internet Security Threat Report. *Mktgassets.symantec.com* [online]. April 2018. [viewed 4 June 2018]. Available from:

http://images.mktgassets.symantec.com/Web/Symantec/%7B3a70beb8-c55d-4516-98ed-1d0818a42661%7D_ISTR23_Main-FINAL-APR10.pdf?aid=elq_

KOCHETKOVA, Kate, 2015. Shock at the wheel: your Jeep can be hacked while driving down the road. *Kaspersky.com* [online]. 23 July 2015. [viewed 15 May 2018]. Available from:

https://www.kaspersky.com/blog/remote-car-hack/9395/

GREENBERG, Andy, 2015. After Jeep hack Chrysler recalls 1.4M vehicles for bug fix. *Wired.com* [online]. 24 July 2015. [viewed 2 March 2018]. Available from:

https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/

DROZHZHIN, Alex, 2016. How that Jeep was hacked. Again. *Kaspersky.com* [online]. 10 August 2018. [viewed 15 May 2018]. Available from:

https://www.kaspersky.com/blog/jeep-hacked-again/12752/

EUROPEAN COMMISSION, 2018. SecureIoT. *Cordis.europa.eu* [online]. 1 January 2018. 24 January 2018. [viewed 27 July 2018]. Available from:

https://cordis.europa.eu/project/rcn/213095_en.html

MORGAN, Steve, 2017. 2017 Cybercrime Report. *Cybersecurityverntures.com* [online]. 2017. [viewed 14 March 2018]. Available from:

https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

PONEMON INSTITUTE, 2017. 2017 Cost of Data Breach Study. *01.ibm.com* [online]. June 2017. [viewed 3 May 2018]. Available from:

https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

GOLDMAN, Jeff, 2016. 88 Poourcent of all ransomware targets the Healthcare Sector. *Esecurityplanet.com* [online]. 3 August 2016. [viewed 3 May 2018]. Available from:

https://www.esecurityplanet.com/malware/88-percent-of-all-ransomware-targets-the-healthcare-sector.html

HUMER, Caroline, FINKLE, Jim, 2014. Your medical record is worth more to hackers than your credit card. *Reuters.com* [online]. 24 September 2014. [viewed 18 April 2018]. Available from:

https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

LYON, Dan, 2017. HDO Customer Needs. *Cybersecuritysummit.org* [online]. 2017. [viewed 24 April 2018]. Available from:

https://cybersecuritysummit.org/wp-content/uploads/2017/10/2.30-Dan-Lyon-Future-Proofing-Panel-HDO.pdf

ARMSTRONG, Reece, 2017. 60% of NHS Trusts still use Windows XP. *Digitalhealthage.com* [online]. 21 December 2017. [viewed 27 May 2018]. Available from:

http://digitalhealthage.com/60-nhs-trusts-still-use-windows-xp/

PONEMON INSTITUTE, 2017. Medical Device Security: An Industry Under Attack and Unprepared to Defend. *Synopsys.com* [online]. May 2017. [viewed 30 April]. Available from:

https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf

HIMSS ANALYTICS, 2017. Annual European eHealth survey. *Himss.eu* [online]

https://www.himss.eu/sites/himsseu/files/education/whitepapers/171013_eHEALTH_TRENDBAROMETER_2017_Q3_Annual%20Survey.pdf

SWISS MEDTECH, 2016. The Swiss Medtech Industry 2016. *Helbling.ch* [online]. 2016. [viewed 15 March 2018]. Available from:

https://www.helbling.ch/hol-en/newsroom/swiss-medical-technology-industry-smti-sector-report-2016/SMTI_2016_final_e.pdf/at_download/file

INRA, 1997. Information technology and data privacy. *Ec.europa.eu* [online]. January 1997. [viewed 17 May 2018]. Available from:

http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_109_en.pdf

TNS OPINION & SOCIAL, 2015. Data Protection. *Ec.europa.eu* [online]. June 2015. [viewed 17 May 2018]. Available from:

http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

LEIBNIZ INSTITUTE FOR THE SOCIAL SCIENCES, 2017. Special Eurobarometer 460: Attitudes towards the impact of digitization and automation on daily life. *Data.europa.eu* [online]. 11 May 2017. [viewed 17 May 2018]. Availabler from:

https://data.europa.eu/euodp/fr/data/dataset/S2160_87_1_460_ENG

MORETTI, Marcus, NAUGHTON, Michael, 2014. Why Privacy Policies Are So Inscrutable. *Theatlantic.com* [online]. 5 September 2014. [viewed 29 April 2018]. Available from:

https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/

AUSTRALIAN GOVERNMENT, 2013. Privacy Commissioner: Website privacy policies are too long and complex. *Oaic.gov.au* [online]. 14 August 2013. [viewed 31 May 2018]. Available from:

https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex

GREENLEAF, Graham, 2017. Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. Papers.ssrn.com [online]. 30 January 2017. [viewed 7 February 2018]. Available from:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

UNITED NATIONS, 2018. Universal Declaration of Human Rights. *Un.org* [online]. 2018. [Viewed 7 February 2018]. Available from:

http://www.un.org/en/universal-declaration-human-rights/index.html

OECD, 2018. OECD work on privacy. *Oecd.org*. 2018. [viewed 8 February 2018]. Available from:

http://www.oecd.org/sti/ieconomy/privacy.htm

COUNCIL OF EUROPE, 2018a. Chart of signatures and ratifications of Treaty 108. *Coe.int* [online]. 15 August 2018. [viewed 15 August 2018]. Available from:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=NeSojLE0

COUNCIL OF EUROPE, 2018b. 128th Session of the Committee of Ministers. Search.coe.int [online]. 18 May 2018. [viewed 23 July 2018]

https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

ICDPPC, 2018. International Conference of Data Protection & Privacy Commissioners. *Icdppc.org* [online]. 2018. [viewed 26 July 2018]. Accessible from:

https://icdppc.org/

ICDPPC, 2005. Montreux Declaration “The protection of personal data and privacy in a globalized world: a universal right respecting diversities”. *Itu.int* [online]. 16 September 2005. [viewed 26 July 2018]. Accessible from:

https://www.itu.int/net/wsis/docs2/pc3/contributions/misc/montreux-declaration.pdf

UNCTAD, 2016. Data protection regulations and international data flows: Implications for trade and development. *Unctad.org* [online]. 2016. [viewed 27 July 2018]. Accessible from:

http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

CNIL, 2018. La protection des données dans le monde. *Cnil.fr* [online]. 2018. [viewed 27 July 2018]. Accessible from:

https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

SWISS FEDERAL DEPARTMENT OF JUSTICE, 2017. Renforcement de la protection des données. *Bj.admin.ch* [online]. 15 September 2017. [viewed 4 April 2018]. Accessible from:

https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/datenschutzstaerkung.html

DLA PIPER, 2017. Norway: preparing to implement the GDPR – Draft for new personal data act. *Blogs.dlapiper.com* [online]. 13 July 2017. [viewed 4 April 2018]. Accessible from:

https://blogs.dlapiper.com/privacymatters/norway-preparing-to-implement-the-gdpr-draft-for-new-personal-data-act/

AFRICAN UNION, 2014. African Union Convention on Cyber Security and Personal Data Protection. *Au.int* [online]. 27 June 2014. [27 July 2018]. Accessible from:

https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

AFRICAN UNION, 2018. List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection. *Au.int* [online]. 10 May 2018. [viewed 27 July 2018]. Accessible from:

https://au.int/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf

APEC, 2005. APEC Privacy Framework. *Apec.org* [onlince]. 2005. [viewed 28 July 2018]. Accessible from:

https://www.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf

EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2000. 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441). *Eru.lex-eu* [online]. 26 July 2000. [viewed 28 July, 2018]. Accessible from:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0520

GIBBS, Samuel, 2015. What is “safe harbour” and why did the EUCJ just declare it invalid? Theguardian.com [online]. 6 October 2015. [viewed 28 July 2018]. Accessible form:

https://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection

CNIL, 2017. Le Privacy shield. *Cnil.fr* [online]. 24 May 2017. [viewed 27 July 2018]. Accessible from:

https://www.cnil.fr/fr/le-privacy-shield

CBPRS, 2011. About the APEC CBPR system. Cbprs.org [online]. 2011. [viewed 28 July 2018]. Accessible from:

http://cbprs.org/GeneralPages/About.aspx

EUROPEAN COMMISSION, 2015. Shaping the Digital Single Market. Ec.europa.eu [online]. 25 March 2015. 12 April 2018. [viewed 24 July 2018]. Accessible from:

https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016. 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). *Eur-lex.europa.eu* [online]. 27 April 2016. [view 21 January 2018]. Accessible from:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

EUROPEAN PARLIAMENT AND OF THE COUNCIL, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Eur-lex.europa.eu* [online]. *24 October 1995*. [view 21 January 2018]. Accessible from:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

EU GDPR COMPLIANT, 2018. EU Citizens' right under the EU GDPR. *Eugdprcompliant.com* [online]. 2018. [visited 21 Janury 2018]. Accessible from:

https://eugdprcompliant.com/eu-citizens-rights/

EUROPEAN COMMISSION, 2018. Regulatory framework. *Ec.europa.eu* [online]. 17 August 2018. [visited 21 January 2018]. Accessible from:

https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework_en

EY, 2016. How the new EU Medical Device Regulation will disrupt and transform the industry. *Ey.com* [online]. 2016. [visited 21 January 2018]. Accessible from:

https://www.ey.com/Publication/vwLUAssets/ey-how-the-new-eu-medical-device-regulation-will-disrupt-and-transform-the-industry/$FILE/ey-how-the-new-eu-medical-device-regulation-will-disrupt-and-transform-the-industry.pdf

MEDTECH EUROPE, 2013. € 17.5 billion for unnecessary measures will be a blow to medical device innovation in Europe. *Medtecheurope.org* [online]. 12 September 2013. [visited 21 January 2018]. Accessible from:

www.medtecheurope.org/node/120

FEDERAL TRADE COMMISSION, 2014. TRUSTe Settles FTC Charges it Deveiced Consumers Through Its Privacy Seal Program. *Ftc.gov* [online]. 17 November 2014. [visited on 24 May 2018]. Accessible from:

https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its

CNIL, 2018a. Les Labels CNIL. *Cnil.fr* [online]. 2018. [visited 24 May 2018]. Accessible from:

https://www.cnil.fr/fr/les-labels-cnil

EUROPRISE, 2018. Register of EuroPriSe Experts. *European-privacy-seal.eu* [online]. 2018. [visited 30 May 2018]. Accessible from:

https://www.european-privacy-seal.eu/EPS-en/register-of-experts#france

SHANTI BRUYIN, A. 2017. Blockchain an introduction. *Beta.vu.nl* [online]. 26 August 2017. [visited 4 Jully 2018]. Accessible from:

https://beta.vu.nl/nl/Images/werkstuk-bruyn_tcm235-862258.pdf

Appendix 1: Complementary information for eHealth association

Health sector companies and organisations should fund an independent association together, which will have three major functions.

Possibly in line with Germany‘s “Platform Industrie 4.0” which will speed up the development of IoT

The health sector industries should do the same and introduce an association specialised in ehealthcare, such as “platform ehealth”

The association is the bridge between security and ehealth solutions; the bridge between ehealth companies, hardware makers, telecommunication companies and security maker.

Association

ehealth: network the whole health sector

However, companies tend to only work on their own, or have partnerships with other companies outside the health sector to get the technology; companies that cannot compete with them because they are not present in the health sector.

This is not following the idea of ehealth and the global network

Moreover, ehealth solutions are getting complex because they integrate many parts that can have vulnerabilities

- Many electronic components, each of these can have a vulnerability
- Software to control electronic components
- Software to handle / process / send data

As seen chapter 4 (vulnerability in medical devices) HDO and device makers do not know how to protect their devices or their infrastructure, too complicated

As seen in chapter X, IoT in general have a lack of security since the producer is not into that industry (car maker does not create the sensors but just buys them on the go)

Solution

Companies within the health sector should build an association that will act like a bridge between all health industry stakeholder and ICT companies not involved in the health industry specifically.

The association will be composed of professionals from all kinds of stakeholders to understand the needs of each.

The association will be funded by the members but has to stay independent

Its main mission will be to improve the security of ehealth solutions, advice the companies about the security improvements; they can do also provide a “glossary or phone book or list” with all the trusted and certified companies

The association will have three branches: software, hardware, components.

Customs

Problem: ehealth solutions can be sold unprotected, as seen chapter 4

Solution:

- The association will check the ehealth solutions and see if they match European standards in term of security, privacy and interoperability
- The association will install a “phone book” or list with all the ehealth solutions that match the criteria
- Not only final products can be found in the “phone book” or list, but also intermediate products, such as electronic components or middleware.
- The association will have to check every period of time that the products are still eligible for the “phone book” or list

The outcomes arising from ehealth customs are:

- Ehealth product makers will have the ability to easily find trustworthy components, middleware and security solutions, reducing the time needed to build a product and enter the market
  - It will be again in time for ehealth solution companies to build their product since they will easily find already protected products and will not need to protect these products later themselves. This will also lead to a reduction in expenditure.
  - This can also be again in time to get the healthcare authorities to get its product approved since the solutions already use certified and protected components
  - Offers a recognition to state their products are secure
  - Offers a greater visibility to their consumers since they are in the trusted list
- For intermediate part maker
  - Offers a greater visibility to their consumers since they are in the trusted list
  - Offers a recognition to state their intermediate products are secure
- For consumers

- Easier way to find secure products to get a safer infrastructure. By buying safe devices or solutions, the risk of getting damaged by cyberattacks is lower.
- Less time spent on security since products are already secure straight out of the box. Also reduce the cost of building a security architecture in the facility for HDO only (normal consumers are not targeted for that part).
- Confidence will be high, thus can push a faster adoption

Vulnerability Program

Problem: even if the products get a certification, IT solutions are known to always have an undetected flaw

Solution: establish a vulnerability program like Google did. All products and intermediate products are eligible for the vulnerability program. Hackers can then try to find vulnerabilities, explain the process to fix to the vulnerability and get paid according to the gravity of the vulnerability. If they provide a solution to fix it, they get an extra.

The outcomes:

- Faster vulnerability finding and fixing.
- Fast action can have a positive impact on consumer trust, again, making the adoption of ehealth solutions faster.
- Less chance to get targeted by a cyber attack

Advisor

The association will keep a track of all bugs, issues or attacks that occurred on the product listed in its “book phone” or list.

Annually, or more often, the association will provide a report listing the problems that occurred and give advice.

The function of the report is not to only point out what was wrong but more to show the trend on how those issues occurred:

- Evolution of type of cyber-attacks on the products. Maybe it can also target other products but by knowing the trend it can help to protect it in advance.
- Evolution of errors or human errors. To know how errors happened so they can be fixed by software or just improve the design of the next version of the product

The outcomes

- Better understanding of the challenges about the products concerning the cyber-attacks and data protection

- Faster reaction to defend the products

The association will also establish different stress test programs for both side, ehealth solution makers and ehealth solution consumers. Based on the trends that appear, the association will be able to make them up-to-date. This will allow all its members to detect any flaw in their infrastructure or their products

- For ehealth solution consumer
  - Better understanding of the strengths and weaknesses in its IT infrastructure making it possible to correct it
- For ehealth solution makers
  - Allow to test new products with the stress test and see if they are resilient enough

The outcomes:

- By testing devices beforehand, it promises to provide a better protection
- Allows the consumers to be more confident of the solutions they use.