HEALTHCARE SECTOR REPORT

Cyber security for the healthcare sector

WG3 I Sectoral Demand

MARCH 2018

www.ecs-org.eu

ABOUT ECSO

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-for-profit organisation under the Belgian law, established in June 2016.

ECSO represents the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP). ECSO members include a wide variety of stakeholders across EU Member States, EEA / EFTA Countries and H2020 associated countries, such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and association as well as European Member State's local, regional and national administrations. More information about ECSO and its work can be found at www.ecs-org.eu.

Contact

For queries in relation to this document, please use wg3_secretariat@ecs-org.eu.
For media enquiries about this document, please use media@ecs-org.eu.

Disclaimer

The use of the information contained in this document is at your own risk, and no relationship is created between ECSO and any person accessing or otherwise using the document or any part of it. ECSO is not liable for actions of any nature arising from any use of the document or part of it. Neither ECSO nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

This document will be continuously updated based on developments within the sector and ECSO members' input.

Copyright Notice

TABLE OF CONTENTS

1 INTRODUCTION

After the amount and criticality of incidents experienced in the healthcare sector in the last years and particularly in 2017 there can be few doubts still that cyber security is an essential need in the systems and networks of healthcare organisations. A lack of cyber security has already been proven to be one of the main causes of disruption to health services but the need for cyber security goes far beyond. Attackers' interest in health organisations and data grows every day as health services become more dependent on information technology. Threats to data privacy, health services' availability, or even the lives of patients exist and can be exploited by terrorists, cybercriminals and other attackers.

The trend towards eHealth, a patient ecosystem of internet connected devices that gather health information of patients and provides diagnosis and even treatment, is unstoppable. The aging society in Europe and the increase in chronic illnesses boosts this trend as a solution to maintain national health services within a reasonable percentage of the national budget.

The increase in health data is an incredibly valuable source of information to improve and speed up patient diagnosis even using mobile devices thanks to the Electronic Health Record, but also to research and study effects of external conditioning (e.g. pollution, weather, sport, medications or social conducts) in our health. This value can only be obtained by sharing and having access to substantial amounts of information.

All the above trends give rise to a substantial amount of cyber threats that target citizens' privacy and safety. The present document analyses these trends, their consequences in terms of the threat landscape and challenges that lay ahead to guarantee that healthcare services and organisations continue to provide resilient and secure health services. To do so, the cyber security landscape of the healthcare sector is analysed in chapter 2. Chapter 3 identifies all actors involved in the healthcare sector and impacted in one way or another by cyber security considerations. The specific characteristics of healthcare and their influence on the cyber security challenges and solutions are described in chapter 4. Finally, chapter 5 analyses several aspects of the cyber security market within the healthcare sector such as its size and expected evolution in the upcoming years.

The present document has been elaborated by ECSO's sub-working group 3.6 on Healthcare stakeholders' cyber security needs and challenges. Future activities foreseen for this sub-working group includes liaison with several healthcare organisations to maintain a continuous collaboration, organisation of workshops to disseminate the activity, and involving more actors and gathering feedback to improve the current document with information about cyber security needs in terms of education, standardisation, research and other issues.

2 Landscape

It is currently a trend in Europe that the population is aging. In other words, the proportion of elderly people in our countries is increasing, due both to fewer children as well as a longer life expectancy. According to the report *Redesigning Health in Europe for 2020*[1], healthcare costs in Europe are currently increasing. These costs are in most European countries a growing component of the GDP, and in some cases still a growing part of public finances, representing between 4% and 12% of GDP in EU Member States.

Another important aspect of the health sector in the EU is that about 40% of the population above the age of 15, i.e. over 100 million citizens, are reported to have a chronic disease. This proportion climbs to 66% of the population who have reached retirement age having at least two chronic conditions.

The EU Member States are facing a situation where more than 70% of healthcare costs are spent on chronic diseases, and this figure is expected to rise in the coming years. For this reason, EU Member States are trying to achieve an affordable, more efficient, less intrusive and more personalised care for citizens.

In order to achieve this, the application of Information and Communication Technologies and also an ethical exploitation of data is of great help. In other words, the use of the concept of eHealth is seen as a main driver to maintaining quality health services in an affordable way. Consequently, eHealth solutions and technologies are expected to significantly increase in the upcoming years. Such solutions involve a broad group of activities that use electronic means to deliver health-related information, resources and services. These include supportive eHealth policy, legal and ethical frameworks, infrastructure development and developing the capacity of the health workforce through training.

From the cyber security point of view, all these trends should be carefully analysed. They introduce or boost the quantity of sensitive information systems and data from patients through monitoring signals, health status and a patient's history and data in electronic format, ready for sharing. All this information can be considered confidential and sensitive data. Therefore, strong requirements and efforts to conveniently anonymise it and protect it should be made, considering especially existing threats and trends in cyber-attacks.

Cyber-attacks are constantly increasing. These kinds of attacks focus mainly on stealing financial information, billing information, and bank account numbers using stolen devices with un-encrypted data, phishing and spam mails. Technological advancements have led to advanced cyber warfare using SQL injections, advanced persistent threats (APT), zero-day attacks, and advanced malware.

The eHealth sector is no exception. We are seeing the trend of an increasing number of cyber-attacks to the health sector. A lack of adequate IT spending by healthcare organisations and a lack of awareness about cybercrime have exposed the vulnerabilities of

[1] eHealth Task Force. Redesigning Health in Europe for 2020. European Union 2012.

healthcare organisations. The overall impact of cyber-attacks on hospitals and healthcare systems is estimated to be nearly six billion per year[2].

Furthermore, health organisations face specific threats due to factors such as the use of cloud services, unsecure networks, employee negligence, bring your own device (BYOD) policies, lack of internal identification and security systems, stolen devices with un-encrypted files and others.[3]

Finally, the safety risks linked with patients' lives due to the compromise of health or eHealth equipment shall not be forgotten and strong attention shall be paid to this aspect. Medical devices which are critical to the safety of life are more and more based on standard operating systems, rarely patched and often interconnected to the hospital networks. Even when these devices are personal devices, they can often be updated OTA (Over The Air) leaving room for manipulation and hacking with the consequent risk to the patient's health and even life. Adequate cyber security safeguards at the design, development but also operation of these devices is of crucial importance.

[2] Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute
[3] Predictions 2016: Cybersecurity Swings to Prevention. Forrester.

3 User Engagement

Several actors play an important role in the eHealth sector from patients to healthcare organisations and each and every one of them has specific cyber security needs and requirements around eHealth services and information which may, in some cases, even enter in conflict. It is therefore crucial to gather complete and comprehensive cyber security requirements from each group.

Below are the actors identified in the eHealth sector and the strategy designed to obtain cyber security requirements from each of them:

- **Patients**: European citizens are the main users of eHealth services and as such essential actors for the success or failure of these services depending on, among others, whether offered services fulfil their needs and expectations also in terms of cyber security. Two essential aspects have to be taken into account for patients: privacy of personal information and resilience of eHealth services.
  Patient needs are, mostly in terms of privacy of personal information, protected by European regulations. Nevertheless, additional cyber security requirements for eHealth services shall be adequately identified.

  The strategies to gather these requirements from patients come mainly from two main actions, on the one hand, liaising with European organisations that represent patients, such as European Patient Forum (*www.eu-patient.eu/*), citizens over 50 such as Age Platform Europe (http://www.age-platform.eu/) or with organisations dealing with ageing such as the EIP on AHA (https://ec.europa.eu/eip/ageing/home_en) and, on the other hand, organising events, such as workshops, where patients, their families and other users are represented and where their requirements can be identified.

- **Physicians and other healthcare professionals**: As those with direct contact with the patients and those ultimately responsible for providing health advice and services, physicians definitely have a key role in defining requirements for eHealth services. Physicians require fast and full access to Electronic Health Records (EHR) in order to be able to make a diagnosis on their patient's health status. As such, their cyber security requirements are more aligned with transparency, ease of use and availability of information.
  Similarly to patients, the main strategies to gather requirements from physicians are liaising with European organisations that represent physicians such as the Comité Permanent Des Médecins Européens (http://www.cpme.eu), the Association of General Practitioners (UEMO http://www.uemo.eu/) the association of specialists (UEMS https://www.uems.eu/) and some of their members (such the Radiologists https://www.myesr.org) and organising workshops where those actors participate to gather their requirements.
  Other healthcare professionals shall be addressed as well such as nurses, technicians and administrative personnel. While the latter can be more difficult to liaise with, since there are no healthcare specific associations for these professionals, the European Federation of Nurses Associations (EFN http://www.efn.be) is an interesting objective to contact to receive input from them.
  The community pharmacists should be approached as well with are the Pharmaceutical Group of the European Union (http://www.pgeu.eu/en/)

- **Healthcare Organisations**: eHealth services are provided and offered by public and private healthcare organisations. Their ultimate interest resides in providing quality services appreciated by patients at a reasonable cost. They are also, at the same time, the main clients of the eHealth industry products and services.
  In this case, in addition to the liaison with organisations such as the European Hospital and Healthcare Federation – Hope (www.hope.be) or the European Public Health Association (https://eupha.org) and the organisation of workshops already described in the previous paragraphs, a third strategy is added. This strategy consists in exploiting the contacts of healthcare industry organisations present in ECSO to either involve healthcare organisations directly in ECSO, or at least act as contact point with these organisations to gather their needs and requirements on behalf of ECSO.
- **Pharmaceutical** companies also play an important role in the eHealth sector. One of their key interests resides in having information necessary to perform studies and tests. Their activity is highly regulated but they can certainly benefit from the introduction of technology within healthcare organisations to generate the fastest and largest access to relevant data without compromising patients' privacy rights.
  Strategies for gathering requirements from pharmaceutical companies are similar to those identified for healthcare organisations, including exploiting contacts within ECSO participants.
  Pharmaceutical organisations which are good candidates to liaise with are: EFPIA (http://www.efpia.eu/) and Medicines for Europe (http://www.medicinesforeurope.com/).
- **Healthcare Industry** offers products and services to healthcare organisations and pharmaceutical companies to improve the eHealth services and products offered by them. This is the actor which is better represented within ECSO and therefore cyber security requirements can be, partially, directly derived from the corresponding ECSO members. However, some areas of the healthcare industry are not represented in ECSO, in particular European manufacturers of medical devices.
  The first option would be to identify medical devices manufacturers and involve them in ECSO as members so that they can have a direct voice and collaborate within ECSO. The other strategies identified for pharmaceutical and healthcare organisations are also valid alternatives in this case to gather their cyber security requirements around eHealth.
  Organisations of the healthcare industry that have been identified as candidates to liaise with are COCIR the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries (http://www.cocir.org/), MedTech Europe (http://www.medtecheurope.org/) that represent diagnostics and medical devices manufacturers operating in Europe and the European Health Telematics Association (https://www.ehtel.eu/) which is a multi-stakeholder forum with significant presence of eHealth industry

4 Sector Specificities

There is no doubt that ICT will be a relevant player in the future of Healthcare, with predictive, preventive, personalised and participative medicine being the main pillars of future medicine. In this context, current technologies like telemedicine, home care systems, remote monitoring, mHealth, wearable, big and smart data are just some examples of technologies that will be relevant to ensure the quality and sustainability of future health care models. In this environment, resilience of healthcare systems and the full patient ecosystem is a crucial need. Unlike other sectors, there is a direct and immediate impact on human life derived from the unavailability of certain healthcare systems. Therefore, resilience is a pillar in the generation of trust and confidence for patients in eHealth services. Conversely, in the last years we have seen an increase in attacks threatening and jeopardising this availability due to the increasing interconnection of healthcare systems, the stronger reliance on IT to execute basic healthcare activities and the growing interest of attackers in attacking health organisations because they have proven to be an easy target prone to paying requested ransoms in order to be able to regain control of their attacked systems.

Another essential need is full confidence in the integrity of information being managed since false data can lead to invalid researches, incorrect diagnostics and ultimately even serious threats on the health of the patients. The need for confidence in the integrity of information is increasing mainly due to two current trends within the healthcare sector. On the one hand, the increasing amount of health information being gathered from patients, sometimes even in a continuous manner. On the other hand, the growing number of medical devices which are network connected and poorly protected. These devices introduce a triple threat to healthcare services. First, their lack of resilience due to the lack of adequate protections. Second, the serious threat to the health of the patients if information exchanged in and out of the medical device is intentionally or unintentionally altered. Third, due to their poor protection they introduce an entry point to the full health organisation's IT systems potentially compromising not only the availability of all systems as discussed before but also the integrity of information stored and exchanged.

The third and last essential need within the healthcare environment is the need to provide confidence to patients that their information is being handled responsibly. A responsible management of private patients' information involves several aspects. Patients are full owners of their personal health information. They have the right to decide for which purposes such data is used, as well as who can use it and when. The privacy of this personal information is therefore crucial. Responsible management is also that the information is available when and where needed as long as this does not contradict the previous condition. Hence, secure health data exchange and access solutions have to be defined and available. On the other hand, data access and how to obtain relevant and valuable information from those data will be a key pillar for new advances like personalised medicine. Solutions that permit a simple, fast and accurate access to that information while at the same time preserving the first two clauses for responsible management would be a huge facilitator for the health research sector, empowering its growth.

Based on the above the main needs within the eHealth sector can be summarised as:

- eHealth service resiliency against cyber-attacks, prevention against data leakage and loss of patient data and identity theft. The same applies to more traditional health care devices and equipment of the hospital.

- Real-time security and dependability monitoring is a much needed feature. A significant advancement in current technologies must be achieved soon, since it is a fundamental prerequisite to the real take up of ICT in the eHealth domain.
- Since the human factor is one of the major security threats in the eHealth domain, it is key that the personnel be made aware of the basic cyber security threats they are exposed to. This entails improving the skills – both technical and behavioural – of the personnel via innovative training techniques that are well received by the (non-IT-expert) workforce. The awareness level in cyber security aspects for all levels of healthcare personnel, e.g., nurses, technicians, administrative personnel and doctors, is an important aspect. The user is most often the weakest link when attacking the target.
- System availability and business continuity is the key component for providing seamless electronic healthcare services. Access to critical health information by authorised professionals as well as secure access control by end-users needs to be guaranteed in order to ensure the best healthcare services. Lack of system availability may significantly affect the eHealth service delivery and some of the critical aspects of eHealth systems. In order to guarantee an acceptable degree of healthcare service availability, the whole healthcare service needs to be provided not only with security mechanisms but with the means to automatically recover from a cyber-attack in the shortest time possible.
- Data security and integrity is another important challenge, in particular related to data storage, network elements (e.g. an access router to a site hosting the eHealth application) for exchanging health data and Identity and Access Management Systems (IAM).
- Medical research can largely benefit from access to a large set of data not only coming from clinical trials, but also from monitoring the actual health parameters of patients and correlating them with environmental characteristics, population data, location etc. Healthcare digitalisation can provide this data in unprecedented volume and quality, but it needs to be ensured that data privacy as well as data integrity is preserved, and data subjects can control the usage of their data. Transparency of the usage of the data is a prerequisite.
- Hospitals have become incrementally digitalised often with complex and still largely unsolved security problems, tied to the standards used, the lack of harmonisation of services and problems with both roles in the hospitals and harmonising laws among different countries (especially in Europe).
- Include security and privacy by design in the evolution of hospital services.
- When new devices or systems are implemented, cyber security aspects need to be planned and implemented already from the beginning, meaning the procurement, outsourcing and maintenance phases of new systems needs to be defined beforehand.
- Hospitals have evolved from a place of care to a delocalised network of care services. The development of Assisted Living systems is only one of the evolutionary aspects of the healthcare system. The long-term radical change of perspective goes under the name of “Patient Ecosystem”. This evolution started a few years ago, but it is exponentially accelerating thanks to the following factors: the recent evolutions of mobile services, the better penetration of information technology to the patients and the increased impact of mobile wellness solutions.

5 Market Study

According to a report from Grand View Research Inc[4] the eHealth market is expected to reach over 280.000 million Euro by 2022 driven mainly by the digitalisation of the healthcare industry.

Such a market will be divided in several different fields where secure ICT Technology will play an essential role[5]:

- **Health Analytics and Big Data in Health**. Analytics is in this context the transformation of data for the purpose of providing insight and evidence for decision- and policy-making. The term big data makes reference to a big amount of data, larger and more complex than traditional data processing can process. This requires the use of distributed systems and advanced methods of data analysis.
- **mHealth**. Use of Mobile Technologies to support health information and medical practices. The main characteristic of mHealth is the potential to reach wide geographical areas and the use of portable forms. mHealth is incorporated into healthcare services such as health call centres or emergency number services and also includes functions such as lifestyle and well-being apps, health promotion and wearable medical devices or sensors.
- **Telehealth**. Medical Services delivered from a distance that encompasses remote clinical diagnosis and monitoring. Telehealth also include a wide range of non-clinical functions encompassing prevention, promotion and curative elements of health. It also involves the use of electronics means or methods for health care, public health, administration and support, research and health education.
- **Electronic Health Records (EHRs)**. Electronic health records are real-time patient-centred records that provide immediate and secure information to authorised users. EHRs include typically a record of the patient's medical history, diagnoses, treatment, medications, allergies and immunisations, as well as radiology images and laboratory results. The fact that this information is in a digital format makes it easier to search, analyse and share.
- **eLearning in Health**. This topic refers to the use of electronic technology and media for training and education that could be used to improve the quality of education and also to increase the access to learning in geographically isolated locations or those locations with insufficient training facilities. This will contribute to increasing the number of trained professionals with specialised or general skills.
- **Social Media in Health**. These online communication channels, which are informal and socially driven, can be used by healthcare providers to share health information and educate the public, discuss care policy and practice, propose healthy behaviours and increase awareness of the services. Patients can also make uses of social media to communicate with healthcare providers as well as with other patients.

These topics can be summarised in five main levers that will move the Healthcare sector market in the following years:

- **My data, my decisions**. Patients and institutions share their data with flexible consent mechanisms.

[4] http://www.grandviewresearch.com/industry-analysis/e-health-market
[5] World Health Organization Europe. From Innovation to Implementation. eHealth in the WHO European Region. 2016. http://www.euro.who.int/en/ehealth

- **Liberate the data**. Health outcomes and performance data will be freely published with full transparency.
- **Revolutionise health**. Technology and information management drives the pace of change.
- **Connect up everything**. This will link the lifestyle data with health data by means of lots of new apps and tools.
- **Include everyone**. In other words, the contribution and benefits from eHealth for all.

It is clear that cyber security must play a crucial role in the development of the above markets to build the trust required in society for these services to flourish. The cyber security investment required by actors in the eHealth market will necessarily be comparatively higher than in other sectors since the direct costs derived from incidents will be otherwise unacceptable. As an example, the overall impact of cyberattacks on hospitals and healthcare systems is estimated to be nearly six billion per year only in terms of financial costs.

The above levers introduce a number of challenges and opportunities in the cyber security industry which will need to define specific solutions to address them:

- Citizens are more and more aware of their privacy in the cyberspace and, at the same time, processes in the healthcare sector are becoming more automated and computerised every day. Cyber security, traceability and privacy of Electronic Health Records is going to be a growing need where specific cyber security solutions will be needed.
- This liberation of data will create a growing need of anonymisation and pseudo-anonymisation solutions in the upcoming years. The new EU General Data Protection Regulation (GDPR) specifies the need to protect even from the inference of private information not explicitly listed which introduces an additional challenge.
- As the eHealth reliance on Information Technology increases a number of challenges will need to be faced that have already been expressed previously in the document. Resilience, cyber security and privacy are only some of the increasing needs that will need to be addressed.

References

eHealth Task Force. Redesigning Health in Europe for 2020. European Union 2012

Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute

http://www.grandviewresearch.com/industry-analysis/e-health-market

Predictions 2016: Cybersecurity Swings to Prevention. Forrester

World Health Organization Europe. From Innovation to Implementation. eHealth in the WHO European Region. 2016. http://www.euro.who.int/en/ehealth