ICT security certification opportunities in the healthcare sector

V1.0

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use isdp@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank all experts that provided support in elaboration of this study, from various organisations – manufacturers of semiconductors, resellers and integrators, producers of medical equipment and medical cloud services providers.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-276-9, DOI: 10.2824/939028

Table of Contents

Executive Summary 4

1. Introduction 7

1.1 Overview 7

1.2 Scope and objectives 8

1.3 Methodology 8

2. Baseline security requirements for products, services and processes 9

3. Healthcare systems 11

3.1 Overview 11

3.2 Healthcare Information Technology 11

3.3 Internet of Medical Things 12

4. Legislation in the area of healthcare 14

5. Healthcare Information Technology security 16

5.1 Assets 16

5.2 Threats 16

5.3 Security requirements for healthcare products and services 17

5.4 Additional considerations 19

6. Healthcare certification 21

6.1 Overview 21

6.2 Healthcare standards 21

6.3 Opportunities for certification 23

6.4 Recommendations 23

7. Bibliography 25

Annex A: Technical security requirements for IoT 27

Executive Summary

Digital solutions for healthcare open a plethora of new possibilities in this area. They provide a technical base for easy testing, they improve significantly the quality of service by allowing immediate access to medical data – results of tests, history of treatment; they facilitate correct diagnosis by easier analytics and correlation of data and easier monitoring of patients' health parameters. They facilitate setting up appointments with appropriate doctors at a convenient time. Some medical treatments can be even conducted online. Digitisation supports the promotion of a healthy life style and can prevent diseases. Electronic healthcare solutions can be offered across borders, giving citizens the feeling of security in this respect.

However, in order for all stakeholders to fully benefit from and trust electronic services and products, they must be properly designed, implemented in cost-effective way and provide an acceptable level of security and privacy.

Specific Healthcare Information Technology systems and network-connected medical devices ("Internet of Medical Things") can be considered as two main components of the healthcare ecosystem, where certification schemes could be envisaged. Functionally they include various sub-categories – starting from the semiconductor chips used in the devices, passing by small medical devices (meters, pacemakers, etc.), large equipment (x-ray, MRI), to IT systems and services (cloud, portals). They all have their particularities, which need to be taken into account when discussing possible certifications.

Health Information Technology is in fact the way of application of IT to the healthcare sector. It has a purpose of managing information exchange among all its stakeholders – government healthcare agencies, doctors, patients, administrators of data, insurance companies and others.

The term "Internet of Medical Things" refers to the Internet of Things (IoT) technologies in the healthcare sector. It consists of an infrastructure connecting various medical devices over the network.

The particularity of the healthcare sector consists in the fact that it is highly regulated by multiple legislative acts at European level. This report identifies directives and regulations that have a relation to Healthcare Information Technology and Internet of Medical Things in Section 4.

In Section 5 the report analyses assets and threats related to the healthcare sector and discusses its security requirements. There are several categories of threats that can affect healthcare IT systems, which in fact consist of various elements and technologies. Healthcare devices are highly interconnected, having even the ability to connect automatically to other devices, therefore a proper threat analysis is complex.

Because of a lack of homogeneity of healthcare information technology systems, consisting of many functional and technical parts, in scope of this report fall distinct components:

- Semiconductors – chips used in medical equipment
- Medical devices – all medical equipment, from glucose meters and insulin pumps to sophisticated hospital equipment, interconnected by Internet of Medical Things
- Electronic services – using traditional IT systems and cloud technology

Security requirements for healthcare products and services (involving their foreseeable use or misuse, and appropriate environment of deployment) are grouped in the following categories:

- Security by design
- Privacy by design
- Operational measures
- Technical measures.

Security issues in the healthcare sector start by fragmentation (for example all hospitals have different ICT systems and use different data formats) and lack of privacy (emergency messages are sent in clear text, including potentially sensitive data). Electronic Health Records (EHR) are driven by vendors, which creates a lock-in situation. There is no open, standardised format of EHR, which would allow to exchange in the EU medical data between healthcare providers, institutions and medical staff. An obvious need for the healthcare community is to close the gaps in standardisation and harmonize various ICT systems.

In the healthcare sector safety issues prevail over ICT security. Convergence of safety and security is important especially where human lives are endangered. For example, while in other areas an IoT device in front of critical fault can just shut down, a heart pacemaker has to enter safe mode, in frame of fail-safe operation. However, security should be built-in in the devices, and manufacturers should obey security-by-default rules. Functional security requirements have to be collected for all building blocks (component level, device level etc.) – as pieces of a puzzle. Identifying them properly is very important; predicting possible misuse cases is necessary.

Medical devices are already subject to certification, during which the evaluation of safety and functional requirements is carried out. Also service providers (i.e. operators of medical clouds) have to undergo certification procedures, evaluating methods of handling and processing of data, and being based on ISO standards from series 27000 and 20000.

There are several standards that could potentially be used for ICT security certification in the area of healthcare – published by traditional Standard Developing Organisations as above, or industrial ones. They relate either to specific medical devices, or more broadly, to technologies used in this sector, like IoT or cloud. Traditional standardisation processes, however, can be time-intensive, potentially causing delays in the application of necessary standards and interoperability. Solutions to improve this situation include the support of European industry and best practices as precursors.

After having assessed ICT security requirements and reference standards it is clear that it is impossible to certify the healthcare sector as a whole. There are different requirements for semiconductors used in medical devices, devices themselves, the Internet of Medical Things, medical clouds various sets of data. A solution to overcome this situation would be to establish a segregated scheme, providing links between other schemes. Synergies across various “certifiable” areas should be used to a large extent to reduce the amount of similar certification approaches.

Concrete considerations for certification in the area of healthcare, collected through a series of interviews, include:

- It is important to certify semiconductor components of devices, but final products should be evaluated. Use of certified components in the product should become a requirement.
- Evaluation of components should include assessment of full traceability of manufacturing, integrity of supply chain, design, security features, lifecycle etc.

- With exceptions (like against IEC 62304[1] or the IEC 80001[2] series), currently mainly hardware is subject to certification. Certification of software should be envisaged, in particular security features of the firmware – key management, storage of data, secure booting.
- ICT security certification of IoMT devices should differ from IoT, as more stress should be put on data protection and privacy issues.
- Assurance level of certification should be linked to the risk associated with the concrete product or service. Depending on risk assessment, not the same technological aspects have to be evaluated in the same way.
- In medical equipment, safety prevails over cybersecurity, but both have to be evaluated at the same time for certification. For medical devices, availability can be perceived as the most important from the components of security.
- For online healthcare services, confidentiality and integrity of data is of utmost importance, therefore stress should be put on data storage and processing.
- Healthcare is an area for which a vulnerabilities disclosure obligation could work out best, as there is sufficient public interest as it relates to human life to ensure that known vulnerabilities of components are sufficiently communicated and mitigation measures have been taken against them.
- Certification needs to be based on a sound risk assessment of risks perceived in the specific application area in question.
- In healthcare at the data level it is important to gravitate towards robust solutions as all personal data is potentially sensitive with very few exceptions.
- In the same vein, solutions regarding the privacy of personal data in transit (e.g. managed on a health care cloud, transmitted across networks etc.) need to offer a high level of assurance.
- The use of recognised solutions to known issues, even when it is not entirely mandated by legislation (partially mandated by MDR) e.g. eIDAS for the management of administrative data, is desirable as healthcare systems require a high level of assurance.

[1] Medical device software -- Software life cycle processes, https://www.iso.org/standard/38421.html
[2] Application of risk management for IT-networks incorporating medical devices, https://www.iso.org/standard/44863.html

1. Introduction

1.1 Overview

Digital solutions for healthcare open a plethora of new possibilities in this area. They provide a technical base for easy testing, they improve significantly the quality of service by allowing immediate access to medical data – results of tests, history of treatment; they facilitate correct diagnosis by easier analytics and correlation of data and easier monitoring of patients' health parameters. They facilitate setting up appointments with appropriate doctors at a convenient time. Some medical treatments can be even conducted online. Digitisation supports promotion of a healthy life style and can prevent diseases. Electronic healthcare solutions can be offered across borders, giving citizens the feeling of security in this respect.

However, in order for all stakeholders to fully trust electronic services and products, they must be properly designed, implemented in a cost-effective way and provide acceptable levels of security and privacy.

According to the opinion published jointly in December 2016 by ENISA and European semiconductor producers[3], in general *today we are seeing a market failure for cybersecurity and privacy: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy. […] The smart card world already knows the relevance and risks of physical attacks when devices are physically accessible to an attacker. With the rise of the Internet of Things (IoT) enabling cars, critical infrastructure, and health applications using the same pipes and systems to communicate, attacks will get even more risky and threatening.* The study discusses in a holistic approach effective baseline requirements for security and privacy in the networked architecture and value chain. It also proposes that well-established Common Criteria related certification of security products has to be complemented by new schemes, adapted to new challenges related to Internet of Medical Things (subset of IoT) and healthcare sector using this technology.

According to ISO/IEC 17067:2013[4], certification is *the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated.* In practical terms, certification offers assurance that a product, service or process underwent an evaluation procedure and has been judged as fulfilling a certain set of requirements.

In September 2017 the European Commission announced the Cybersecurity Package, to further improve resilience, deterrence and defence of EU networks. The proposal, among other matters, envisaged the creation of a pan-European cybersecurity certification framework for ICT products and services. Such a framework would include several certification schemes, potentially of sectorial dimension. Healthcare may be perceived as one of the sectors that could be covered by one or more ICT security certification schemes.

[3] Infineon – NXP – STMicroelectronics – ENISA Common Position On Cybersecurity, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity
[4] Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes, https://www.iso.org/standard/55087.html

1.2 Scope and objectives

The scope of this report covers functional requirements for a potential ICT security certification scheme for a widely understood healthcare sector.

Its objectives are:

- To provide a high-level overview network and information security of the healthcare sector;
- To identify the ICT components of products and services of the healthcare sector and their security requirements;
- To review the opportunities for certification in the area of healthcare and define functional requirements for a potential certification scheme.

1.3 Methodology

This report was developed combining:

- Desk research – reviewing state of the art documentation, research papers and articles, legal acts, recommendations from industry and Member States authorities, and other ENISA studies;
- A series of one-to-one and group interviews with industry representatives from various companies involved in healthcare – manufacturers of semiconductors, resellers and integrators, producers of medical equipment, medical cloud services providers.

2. Baseline security requirements for products, services and processes

Discussing certification in any industrial sector, including healthcare, has to start by identification of what this term represents. Currently we can provide two formal definitions:

ISO/IEC 17067:2013 defines certification as "*the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated*".

According to the proposal of the European Commission, EC COM(2017) 477[5], certification is a "*formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria standards and the issuing of a certificate indicating conformance*".

Both definitions stipulate that specific requirements for defined products, services and processes have to be fulfilled in order to be granted a certificate, while the draft EU Cybersecurity Act puts emphasis on standards, presumably published by Standard Developing Organisations recognised by the European regulations[6].

Based on an ENISA study from 2016[7], we can identify four principles for secure products, services and processes:

- Security by design – the product, service or process has been conceived, designed and implemented to ensure the key security properties are maintained: availability, confidentiality, integrity and accountability;
- Security by default – the product, service or process is supplied with the confirmed capability to support these security properties at installation;
- Security throughout the lifecycle – security should be maintained from initial deployment through maintenance to decommissioning;
- Verifiable security – each of the above principles should be verifiable.

According to the same study, these principles can be extended into the following baseline security requirements:

- Security by design – the provider shall design and pre-configure the delivered product such that functionalities are based on well-established security practices and are reduced to the strict minimum required for system operations;
- Least privilege – the provider shall design and pre-configure the product according to the least privilege principle, whereby administrative rights are only used when absolutely necessary, sessions are technically separated and all accounts will be manageable;

[5] Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

[6] Regulation (EU) 1025/2012 of the European Parliament and of the Council on European standardisation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=EN

[7] Indispensable baseline security requirements for the procurement of secure ICT products and services, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

- Strong authentication – the product shall provide and support strong authentication mechanisms for all accounts. If authentication is unsuccessful the product shall not allow any user specific activities to be performed;
- Asset protection – the product shall provide an adequate level of protection for critical information assets during storage and transmission;
- Supply chain integrity – the provider should provide means to ensure that the product is genuine, cannot be tainted during operation, and its integrity is warranted throughout the product's lifecycle. Currently this requirement can be technically fulfilled only partly;
- Documentation transparency – the provider shall offer comprehensive and understandable documentation about the overall design of the product, describing its architecture, functionalities and protocols, their realisation in hardware or software components, the interfaces and interactions of components with each other and with internal and external services, in order to be able to implement and use the product in the most secure way possible;
- Quality management – the provider shall be able to provide evidence that a managed security by design approach has been adopted, including documented secure software development, quality management and information security management processes;
- Service continuity – the provider shall guarantee support throughout the agreed lifetime of the product such that the system can work as agreed and is secure;
- Conformance to law – the provider shall accept that all contracts (including those with subcontractors) are conform to the legal requirements in place;
- Data usage restriction – the provider shall explicitly declare, justify and document, context and purpose wise, all data collection and processing activities that take or may take place, including relevant legal obligations stipulating them.

The list above is not exhaustive and can be extended, basing on specific requirements of concrete areas. Requirements related to the healthcare sector are discussed in section 5.

3. Healthcare systems

3.1 Overview

Specific Healthcare Information Technology systems and network-connected medical devices (“Internet of Medical Things”) can be considered as two main components of the healthcare ecosystem, where certification schemes could be envisaged. Functionally they include various sub-categories – starting from the semiconductor chips used in the devices, passing by small medical devices (meters, pacemakers, etc.), large equipment (x-ray, MRI), to IT systems and services (cloud, portals). They all have their particularities, which need to be taken into account when discussing possible certifications.

3.2 Healthcare Information Technology

Health Information Technology is in fact the way of application of IT to the healthcare sector. It has a purpose of managing information exchange among its all stakeholders – government healthcare agencies, doctors, patients, administrators of data, insurance companies and others.

According to a study by HealthCatalyst[8], healthcare information systems have been developed since the 1960’s, with various drivers and goals:

- 1960’s – hospital accounting systems, typically on mainframes
- 1970’s – transactional proprietary systems, not interconnected and not interoperable
- 1980’s – first limited interoperability of financial and clinical systems
- 1990’s – consolidated healthcare systems, having access to robust networks and distributed computing
- 2000’s – more integration, first real-time Electronic Health Records
- 2010’s – Electronic Medical Records broadly implemented, pervasive computing, Internet of Medical Things becomes reality.

Among the components of Health Information Technology we can distinguish the following elements (the list is not comprehensive):

Electronic medical record (EMR)

This is an electronic replacement of paper-based health records, and can be considered as the basic IT system for healthcare. An EMR system contains history of the patient, but can also send notifications when specific actions with regard to the patient have to take place – tests, screenings, medical visits etc.

Electronic Health Record (EHR)

EHR is a more advanced system than EMR. It allows not only to review the patient’s history, but also to consult results of examinations, tests, screenings, MRIs, X-rays, prescribed medicines, treatments, medical diagnoses etc.

[8] Healthcare Information Systems: A Look at the Past, Present, and Future, https://www.healthcatalyst.com/insights/healthcare-information-systems-past-present-future

ISO TR 20514[9] provides the two following definitions:

EHR: *A repository of information regarding the health status of a subject of care, in computer processable form. An EHR provides the ability to share patient health information between authorized users of the EHR and the primary role of the EHR is supporting continuing, efficient and quality integrated health care.*

EHR system: *The set of components that form the mechanism by which electronic health records are created, used, stored, and retrieved. It includes people, data, rules and procedures, processing and storage devices, and communication and support facilities*.

Patient Healthcare Record – PHR[10]

A PHR is the interface between the EMR/EHR and the patient. It allows for medical data to be accessible not only to the hospital/clinic/doctor, but also to the patient, who can check online his/her records.

Scheduling systems

These complement the patient's portals and are used to book appointments with doctors, for tests or for simple medical procedures.

e-Prescription

An e-prescription / e-dispensing system serves the patient's need on the prescription and dispensing of medicine and automate/optimize the process. The first step of the process is the patient visiting a physician, who examines the patient and prescribes medicine on the system (if needed). The second step is the patient visiting a pharmacy, which dispenses the medicine to the patient.

Health Information System – HIS

This is the core IT system of every clinic or hospital, allowing management of every day operations. It is interconnected with other systems, described above.

3.3 Internet of Medical Things

This name refers to the Internet of Things (IoT) technologies in the healthcare sector. It consists of the infrastructure and various medical devices connecting over the network. ENISA conducted a study on Smart Hospitals identifying smart assets in Healthcare organisations, some of them are listed below[11].

Among the types of "Medical Things", which can be connected through the network, we can distinguish:

- smart wearable devices – monitors of heart rate, perspiration levels, oxygen levels in the bloodstream alcohol levels
- home-use medical devices – glucose monitors, blood pressure meters, insulin pumps
- implantable devices – cardioverter defibrillators, heart pacemakers
- point-of-care kits – diagnostic tests, analysers
- emergency response systems – reacting to alerts
- virtual home assistants – e.g. monitors of adherence to prescriptions

[9] Health informatics -- Electronic health record -- Definition, scope and context, https://www.iso.org/standard/39525.html

[10] https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services

[11] https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

- kiosks – dispensing medical products (see e-Prescriptions)
- sensors (RFID) in pharmaceutical packages
- mobile healthcare applications

With the progress of technology, connectivity of medical devices becomes ubiquitous. Advantages of using this feature are difficult to undermine, as they allow for a more precise diagnosis and correct treatment. The most prominent are:

- immediate access to results of tests or X-ray images – by both, patient and doctor
- real-time access to medical data – current or archival
- easier analytics – through sensors and actuators
- automatic correlation of data – from various sources
- health alerts – in case of permanent monitoring
- remote monitoring of chronic diseases – allows for spotting anomalies
- easier medicines management – through e-Prescriptions
- increased patient's interest – as he can have immediate information on his health parameters
- lower cost of healthcare

The market value of the Internet of Medical Things is still on the rise. According to a study by Deloitte[12], it will reach 140 billion EUR by 2022.

[12] Deloitte – Medtech and the Internet of Medical Things, https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html

4. Legislation in the area of healthcare

The healthcare sector particularity consists in the fact that it is regulated by multiple legislative acts at the European level. The following set of directives and regulations has relation to Healthcare Information Technology and the Internet of Medical Things.

Regulation on medical devices[13]

This Regulation aims to ensure the smooth functioning of the internal market as regards medical devices, taking as a base a high level of protection of health for patients and users, and taking into account the small- and medium-sized enterprises that are active in this sector. At the same time, this Regulation sets high standards of quality and safety for medical devices in order to meet common safety concerns as regards such products. Both objectives are being pursued simultaneously and are inseparably linked whilst one not being secondary to the other. This Regulation harmonises the rules for the placing on the market and putting into service of medical devices and their accessories on the Union market thus allowing them to benefit from the principle of free movement of goods. It sets high standards of quality and safety for medical devices by ensuring, among other things, that data generated in clinical investigations are reliable and robust and that the safety of the subjects participating in a clinical investigation is protected. It also introduces incident reporting (for security incidents) and security measures to be implemented for medical devices.

Directive on the application of patients' rights in cross-border healthcare[14]

This directive aims to improve the functioning of the internal market and the free movement of goods, persons and services by achieving harmonisation and a high level of protection of human health across the EU Member States, taking account in particular of any new development in the healthcare area.

General data protection regulation[15]

The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her. The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

[13] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745

[14] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

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

GDPR is an important piece of legislation in the area of healthcare, as personal data concerning health are considered as sensitive and therefore need to be treated in a particular way.

eIDAS Regulation[16]

This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

eIDAS provides services and tools that are important for the healthcare sector, especially in the context of the eHealth initiative, which aims to provide seamless, secure access to medical data for patients and doctors.

NIS Directive[17]

The Network and Information Systems Security Directive is the first legal act of the EU setting up a global approach at Union level covering common minimum cybersecurity capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers, therefore allowing an effective response to the challenges of the security of network and information systems. The NIS Directive is being transposed to national law, usually taking account of other, existing laws on cybersecurity.

In Annex II of the NIS Directive Healthcare sector is included putting in scope operators that offer healthcare services in the Member States.

Draft EU Cybersecurity Act[18]

This document in its current form stipulates that cybersecurity certification plays an important role in increasing trust and security in ICT products and services. The digital single market can only thrive if there is general public trust that ICT products and services provide a certain level of cybersecurity assurance.

“Electronic medical devices” are mentioned in the proposal as an example of sector in which certification is already widely used or is likely to be used in the near future.

[16] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[17] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[18] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency" [..], and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act''), COM/2017/0477 final - 2017/0225 (COD) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0477:FIN

5. Healthcare Information Technology security

5.1 Assets

The assets of smart hospitals have been identified in a previous ENISA study[19] in 2016. They characterize well the information technology related assets of the whole healthcare sector. We distinguish among them:

- **Remote care system assets**
  Medical equipment for remote monitoring and diagnosis – heart rate monitors, glucose meters; drugs dispensing equipment etc.
- **Networked medical devices**
  Implantable or wearable devices like insulin pumps, cardiac pacemakers; stationary devices like MRI or X-ray equipment, chemotherapy dispensers.
- **Identification systems**
  Systems to authenticate and track patients, staff and equipment – RFID tags and systems, bracelets, smart badges, biometric tags
- **Networking equipment**
  IT equipment used in healthcare establishments – network devices (routers, switches), cables, wireless equipment; computers
- **Mobile client devices**
  Laptops, smartphones, tablets and applications working on them
- **Interconnected clinical information systems**
  Specific systems deployed in healthcare establishments, like Laboratory Information Systems, Radiology Information Systems, Blood Bank Systems etc.
- **Data**
  One of the more important assets of healthcare sector, subject to various regulations. It includes administrative patient's data, clinical data (health records, test results, medical history), research data (clinical trials results) etc.
- **Physical facilities**
  Buildings of healthcare establishments, electricity supply, air conditioning etc.

5.2 Threats

There are several categories of threat that can affect healthcare IT systems, which in fact consist of various elements and technologies. Healthcare devices are highly interconnected, having even the ability to connect automatically to other devices, therefore a proper threat analysis is complex. The ENISA study on Smart Hospitals proposed a taxonomy of threats to which various types of assets are exposed:

- **Malicious actions**
  Under this category fall a variety of potential threats – malware (viruses, worms, trojans, rootkits), hijacking, DoS attacks, device tampering, social engineering (phishing), theft of device, theft of data, skimming
- **Human errors**
  They are due to involuntary human actions, resulting in damage to healthcare systems

[19] Cyber security and resilience for Smart Hospitals, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

- **System failures**
  They can have different causes, the most common are: software or firmware failures, device failure, network failure, insufficient maintenance, overloading.
- **Supply chain failure**
  This threat can be caused by cloud provider, network provider, power supply provider or by the manufacturer of medical devices, not putting adequate care in his supply chain integrity.
- **Natural phenomena**
  They include fires, floods, earthquakes and other natural disasters that can cause interruption of normal services.

5.3 Security requirements for healthcare products and services

Because of a lack of homogeneity of healthcare information technology systems, consisting of many functional and technical parts, developing a concise set of security requirements needs a look into all building blocks. Basing on assertions in Section 3, we can distinguish the following distinct components in scope of this study:

- Semiconductors – chips used in medical equipment
- Medical devices – all medical equipment, from glucose meters and insulin pumps to sophisticated hospital equipment, interconnected by Internet of Medical Things
- Electronic services – using traditional IT systems and cloud technology

In November 2017, ENISA published the Baseline Security Recommendations for IoT[20]. In February 2018, the NIS Cooperation Group issued a document on security measures for operators of essential services[21]. Finally, in November 2018 the German Federal Office for Information Security (BSI) published a recommendation on Cybersecurity requirements for network-connected medical devices[22]. Also the MDR (Medical Devices Regulation) Cybersecurity Task Force is expected to produce guidelines (including security requirements) for manufacturers and hospitals. Based on these studies, common high level functional security requirements for the healthcare sector can be elaborated as below. These requirements should be evaluated during the certification process. [P] denotes requirements for manufacturers of products, [O] for operators of services.

Security by design

- Consider the security of the whole system from a consistent and holistic approach [P, O]
- Ensure the ability to integrate different security policies, technologies and methods [P, O]
- Security must consider the risk posed to human safety; carry out a risk assessment in relation to the specific application area [P, O]
- Designing for power conservation should not compromise security [P]
- Design architecture by compartments to encapsulate elements in case of attacks [P]
- Test plans to verify whether the product or service performs as it is expected (like penetration tests) [P, O]

[20] Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[21] CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643
[22] Cyber Security Requirements for Network-Connected Medical Devices, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.pdf?__blob=publicationFile&v=3

- Code review during implementation to reduce bugs [P]

Personal data protection / privacy by design

- Make personal data protection and privacy an integral part of the design of a system or product or service [P, O]
- Perform personal data protection / privacy impact assessments [P, O]
- Establish and maintain asset management procedures and configuration controls [P, O]
- Identify significant risks using a defence-in-depth approach [P, O]
- Identify the intended use and environment of a given device [P]
- Follow a layered approach recognising the importance of treatment of healthcare data as sensitive personal data, which calls for different measures than those taken for other general types of data. [O]

Organisational measures

- Put in place and implement an effective security policy [P, O]
- Carry out security a risk assessment regularly [P, O]
- Ensure appropriate business continuity and disaster recovery plans [P, O]
- Establish a secure development life cycle [P]
- Develop a full end-of-life strategy [P]
- Offer effective and secure patch management [P]
- Use proven solutions, i.e. well known communications protocols and cryptographic algorithms [P, O]
- Establish procedures for security incident handling [P, O]
- Participate in information sharing and coordinated vulnerability disclosure [P]
- Ensure the personnel is trained in privacy and security [P, O]
- Cybersecurity roles and responsibilities are established [P, O]
- Develop policy for processing of data by a third-party [P, O]
- Adopt cyber supply chain risk management policies [P, O]
- Make broad use of recognised solutions to known issues, even when it is not mandated by legislation e.g. eIDAS [P]

Technical measures

- Meet baseline security requirements for IoT, listed in Annex A [P]
- Carry out a risk assessment regarding the specific application area and complete it with suitable mitigation measures [O]
- The use of recognised solutions to known issues, even when it is not mandated by legislation e.g. eIDAS or Medical Devices Resolution for the management of administrative data, is desirable as healthcare systems require a high level of assurance. [P, O]
- Ensure appropriate configuration of ICT systems and their segregation [P, O]
- Deploy cybersecurity measures to protect data at rest, in use and in motion [P, O]
- Apply appropriate traffic filtering [O]
- Use state-of-the-art cryptography and key storage methods [P, O]
- Put in place effective identity and access management [P, O]
- Ensure correct IT security maintenance [P, O]
- Develop policies for physical and environmental security [P, O]

- Deploy early warning/detection systems [P, O]

5.4 Additional considerations

Non-conforming products, services or devices can result in hasards for both patients and medical personnel, delay or hold up a medical protocol form applying, risking life and wellbeing of patients and significantly increase costs for the healthcare system as a whole. In response, such risks lead providers of health care services to rely on conformity assessment systems. By the same token it is necessary to have the ability to assess safety, health, environmental and cost effectiveness risks associated with health care products and services. Requirements for medical devices are based on a risk assessment linked to the device's intended use and profile. The MDR expands on the existing risk profile framework for classification of devices. It is the responsibility of appropriate Notified Bodies to conduct such conformity assessments.

There are several issues with security of healthcare ICT systems. Problems include fragmentation (for example many hospitals have different ICT systems and use different data formats) and potential lack of privacy (emergency messages are sent in clear text, including potentially sensitive data). Electronic Health Records are driven by vendors, which creates a lock-in situation. Interoperability of systems is one of biggest issues in the area of healthcare, however there are initiatives towards harmonisation[23], aiming at creating EHR profiles.

There is no open, standardised format of EHR, which would allow the exchange of EU medical data between healthcare providers, institutions and medical staff. There are some national initiatives – in 2008 Estonia was the first country in the world to introduce a "birth-to-death" EHR. The eHealth Action Plan[24] published by the European Commission in 2012 underlines the necessity to work on three crucial components – EHRs, e-Prescriptions and telemedicine. The eGovernment Action Plan also aims to support Member States in the development of cross-border solutions.

There are challenges at the EU level when it comes to cross-border access and portability of personal health data. Further work, however, should start with harmonization of interoperable connectivity at the national level. In its Communication[25], the European Commission sets out its intention to take action in three areas – assure secure access to and sharing of health data across borders, assure better data for medical research and empower citizens with digital tools for personal-centred care. Respondents of a public consultation[26] carried out in 2017 gave priority to development of new EU standards for data quality, reliability and cybersecurity, EU standards for electronic health records and better interoperability through open exchange formats.

An obvious need for the healthcare community is to close the gaps in standardisation and harmonize various ICT systems.

In the healthcare sector safety issues prevail over ICT security. Convergence of safety and security is important especially where human lives are endangered. For example, while in other areas an IoT device in front of critical fault can just shut down, a heart pacemaker has to enter safe mode, in the context of fail-

[23] http://www.hl7.org/implement/standards/index.cfm?ref=nav
[24] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4188
[25] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628
[26] https://ec.europa.eu/info/consultations/public-consultation-transformation-health-and-care-digital-single-market_en

safe operation. However, security should be built-in in the devices, and manufacturers should obey security-by-default rules.

For medical devices, apart from traditional IoT security requirements, additional ones concerning privacy and data protection have to be observed. Many devices are shared among patients (like hospital glucose meters), what creates additional complications. Privacy should be correctly perceived. Appropriate training should be mandatory in order to exercise certain functions.

Also access rights to data have to be correctly set for users, doctors and administrators. Different levels of authentication have to be foreseen – for example to access to the configuration settings of a pacemaker, or to data from heart rate monitor.

Other requirements concern integrity of software used by components and devices, their authenticity and sets of data that they exchange in the network. Functional security requirements have to be collected for all building blocks (component level, device level etc.) – as pieces of a puzzle. Identifying them properly is very important; predicting possible misuse cases is necessary. These issues are in scope of the MDR task force on cybersecurity for medical devices.

6. Healthcare certification

6.1 Overview

In April 2018 the European Commission has published the "Communication from the Commission […] on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society"[27] and an accompanying "Commission staff working document"[28]. They underline the importance of further work on digital healthcare solutions in order to promote their usability and harmonization.

As stated previously, healthcare is a complex area, where various building blocks need to be assessed separately. Fragmentation of the healthcare market and issues like lack of Electronic Health Records interoperability, make the discussion about potential certification schemes very challenging.

Medical devices are already subject to certification, during which evaluation of safety and functional requirement is carried out. Also service providers (i.e. operators of medical clouds) have to undergo certification procedures, evaluating methods of handling and processing of data, and being based on ISO standards from series 27000 and 20000.

This section will review the situation in reference standards for requirements identified in Section 5 and discuss possibilities of establishing a certification scheme in the area of healthcare.

6.2 Healthcare standards

When discussing reference ICT security standards related to the healthcare sector, it's important to repeat that it is not a homogenous area. On the one hand, as mentioned in section 5, there are at least three different areas that must be considered separately – semiconductors, medical devices and electronic services. On the other, there are different types of requirements – security by design, privacy by design, organisational requirements and technical requirements. Additionally, from the practical point of view, healthcare systems are used by various groups of users – doctors, patients, hospitals, pharmacies, governmental agencies and insurance companies – having their own needs and requirements. Integrating all these factors is a big challenge for standardisation organisations.

Standards Developing Organisations are dealing with standards related directly or indirectly to ICT security in the area of healthcare. The following work is being carried out by the bodies recognised by the Regulation 1025/2012 on European standardisation[29]:

- **International Standards Organisation – ISO**
  ISO has established a technical committee TC 215 – Health informatics. It deals with standardization in the field of health informatics, to facilitate capture, interchange and use of health-related data, information, and knowledge to support and enable all aspects of the health system.
- **CEN-CENELEC**

[27] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628
[28] https://ec.europa.eu/digital-single-market/en/news/staff-working-document-enabling-digital-transformation-health-and-care-digital-single-market
[29] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF

There are various technical committees dealing with medical devices, mainly from the safety point of view (so outside of scope of this study, covering a wide variety of topics, ranging from electrical medical equipment, syringes, ophthalmic optics and dentistry to air ambulances, in vitro diagnostic medical devices and sterilizers).
A technical committee at CEN has been established to develop European standards harmonised and consistent with the existing international framework - TC 251, "Health informatics". Its scope ranges from Electronic Health Records architecture and Health Informatics Service Architecture, to Detailed Clinical Modelling.

- **ETSI**
  ETSI has established the "EP (ETSI Project) eHealth", which co-ordinates its activities in the Information Communication Technology related to eHealth. Its duties include among others collecting and defining the Health ICT related requirements from relevant stakeholders and informing the concerned ETSI Technical Bodies, identifying gaps where existing ETSI standards do not fulfil the Health ICT requirements and suggesting further standardization activities to fill those gaps.
- **International Telecommunication Union – ITU**
  Within its Study Group 16 – "Multimedia coding, systems and applications", the ITU is dealing with several items related to eHealth applications – identification of users' requirements, multimedia framework (in particular for telemedicine, roadmap for e-health standards, generic architecture for e-health applications etc. Some parts of healthcare related activities related to telebiometrics are also undertaken by Study Group 17 – "Security".
- **International Electrotechnical Commission – IEC**
  IEC is currently working on the new 80001 series for medical devices information security.

There are several standards that could potentially be used for ICT security certification in the area of healthcare – published by traditional Standard Developing Organisations as above, or industrial ones. They relate either to specific medical devices, or more broadly, to technologies used in this sector, like IoT or cloud. Traditional standardisation processes, however, can be time-intensive, potentially causing delays in the application of necessary standards and interoperability. Solutions to improve this situation include the support of European industry and best practices as precursors. Full analysis and identification of gaps should be subject to a separate study, but one of the major technical problems concerns the lack of appropriate standards for ICT interoperability.

ENISA analysed the standards related to IoT in 2018[30]. Results of this work can be partially extended to IoMT.

The simplified analysis is yields that there is no significant standards gap – every security requirement can be met by an existing standard. The problem is that this is neither the correct nor the expected answer. Standards exist for many different elements of making a device or service secure. However, when referring to IoT, one refers to an ecosystem of not only devices and services. Moreover, the context of use of IoT, its high scalability and other particularities further complicate the field and require more generic and flexible approaches. Therefore, for example the gap in IoT device standards for security is that the standards are not treated holistically so it is possible to deliver a device to the market that can authenticate its user, that can encrypt data it transmits, that can decrypt data it receives, that can deliver or verify the proof of integrity, but which will still be insecure. Similarly, the organisation developing the IoT product or service

[30] IoT Security Standards Gap Analysis, publication expected in January 2019

may have the development processes defined in management guidelines such as those of ISO-27000 but still delivers an insecure product.

6.3 Opportunities for certification

The previous discussion on ICT security requirements and reference standards supports the statement that it is impossible to certify the healthcare sector as a whole. There are different requirements for semiconductors used in medical devices, devices themselves, the Internet of Medical Things, medical clouds' various sets of data. A solution to overcome this situation would be to establish a segregated scheme, providing links between other schemes. Synergies across various "certifiable" areas should be used to a large extent to reduce the amount similar certification approaches.

The baseline requirements for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication and authorization, should set reference levels for trusted IoMT solutions, which could be evaluated in a certification process. They should become effective in the networked architecture and value chain as a whole: from components of simple devices up to complex systems. Common principles should be based on scalable robustness requirements (including security controls and mechanisms), reference security architectures, basic functionalities, and security certification of embedded security services. This would need an adaptation of the existing interoperability and security testing framework to new requirements related to healthcare sector.

Although Common Criteria[31] based certification covers the highest assurance and security levels, certain components of healthcare area do not require full evaluation; nevertheless they still need appropriate security levels and the require vulnerability assessment of security solutions. Vulnerability disclosure is a good choice for healthcare, as there is public interest associated with the potential loss of human life to support the argument in favour of the potential, additional burden it may entail. The vigilance system introduced in the Medical Devices Regulation is one approach to this issue, while industry-led efforts, such as the Manufacturer Disclosure Statement for Medical Device Security (MDS2), are also focusing on the topic. Industry stakeholders often call for a good definition of medium assurance level, as the most appropriate for IoT components. "Lightweight" certification would be attractive for the development of modern applications and agile development methodologies, for products with short life cycle or low cost. Such certification should use standardized security requirements for connected devices as reference.

6.4 Recommendations

Concrete considerations for certification in the area of healthcare, collected through a series of interviews, include:

- It is important to certify semiconductor components of devices (including medical devices), but final products should also be evaluated. The use of certified components in the medical product should become a requirement.
- Evaluation of components should include assessment of full traceability of manufacturing, integrity of supply chain, design, security features, lifecycle etc.
- With exceptions (like against IEC 62304 or the IEC 80001 series), currently mainly hardware is subject to certification. Certification of software should be envisaged, in particular security features of the firmware – key management, storage of data, secure booting.
- ICT security certification of IoMT devices should differ from IoT.

[31] ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security, https://www.iso.org/standard/50341.html and further

- The assurance level of certification should be linked to the risk associated with the concrete product or service. Depending on the risk assessment, the same technological aspects do not have to be evaluated in the same way.
- In medical equipment, safety prevails over cybersecurity, but both have to be evaluated at the same time for certification.
- For online healthcare services, confidentiality and integrity of data is of utmost importance, therefore stress should be put on data storage and processing.
- Healthcare is an area in which a vulnerabilities disclosure obligation could work out best, as there is sufficient public interest (as it relates to human life) to ensure that known vulnerabilities of components are sufficiently communicated and mitigation measures have been taken against them. The Medical Devices Regulation includes appropriate consideration of this matter.
- Certification needs to be based on a sound risk assessment of risks perceived in the specific application area in question.
- In healthcare at data level it is important to gravitate towards robust solutions as all personal data is potentially sensitive one with very few exceptions.
- In the same vein solutions regarding the privacy of personal data in transit (e.g. managed on a health care cloud, transmitted across networks etc.) needs to offer a high level of assurance.
- The use of recognised solutions to known issues, even when it is not mandated by legislation e.g. eIDAS for the management of administrative data, is desirable as healthcare systems require a high level of assurance.

7. Bibliography

Standards

ISO/IEC 17067:2013 Conformity assessment -- Fundamentals of product certification and guidelines for product certification schemes, https://www.iso.org/standard/55087.html

ISO TR 20514 Health informatics – Electronic health record – Definition, scope and context, https://www.iso.org/standard/39525.html

ISO/IEC 15408-1:2009 Information technology – Security techniques – Evaluation criteria for IT security, https://www.iso.org/standard/50341.html and further

Legal acts

Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

Regulation (EU) 1025/2012 of the European Parliament and of the Council on European standardisation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012R1025&from=EN

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

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0745

Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R0746

Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007 amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32007L0047

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011L0024

ENISA and European Commission studies

Baseline Security Recommendations for IoT, https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Cyber security and resilience for Smart Hospitals, https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Infineon – NXP – STMicroelectronics – ENISA Common Position On Cybersecurity, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/infineon-nxp-st-enisa-position-on-cybersecurity

Indispensable baseline security requirements for the procurement of secure ICT products and services, https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services

IoT Security Standards Gap Analysis, publication expected in January 2019

CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53643

European Commission, eHealth Action Plan
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=4188

European Commission, *Study on Big Data in Public Health, Telemedine and Healthcare*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/bigdata_report_en.pdf

Communication from the Commission […] on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society
http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51628

Commission staff working document https://ec.europa.eu/digital-single-market/en/news/staff-working-document-enabling-digital-transformation-health-and-care-digital-single-market

Other publications

Cyber Security Requirements for Network-Connected Medical Devices, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_132E.pdf?__blob=publicationFile&v=3

Deloitte Center for Health Solutions, *Medtech and the Internet of Medical Things – How connected medical devices are transforming health care*, https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html

Healthcare Information Systems: A Look at the Past, Present, and Future, https://www.healthcatalyst.com/insights/healthcare-information-systems-past-present-future

Deloitte – Medtech and the Internet of Medical Things, https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html

Annex A: Technical security requirements for IoT

The following requirements were identified in previously mentioned ENISA study *Baseline Security Recommendations for IoT*. Appropriate reference standards for each requirement were matched in ENISA study *IoT Security Standards Gap Analysis.* The list below lists general requirements for IoT.

- Employ a hardware-based immutable root of trust
- Use hardware that incorporates security features to strengthen the protection and integrity of the device – for example, specialised security chips / coprocessors that integrate security at the transistor level, embedded in the processor, providing, among other things, a trusted storage of device identity and authentication means, protection of keys at rest and in use, and preventing unprivileged from accessing to security sensitive code. Protection against local and physical attacks can be covered via functional security
- Trust must be established in the boot environment before any trust in any other software or executable program can be claimed
- Sign code cryptographically to ensure it has not been tampered with after signing it as safe for the device, and implement run-time protection and secure execution monitoring to make sure malicious attacks do not overwrite code after it is loaded
- Control the installation of software in operating systems, to prevent unauthenticated software and files from being loaded onto it
- Enable a system to return to a state that was known to be secure, after a security breach has occurred or if an upgrade has not been successful
- Use protocols and mechanisms able to represent and manage trust and trust relationships
- Any applicable security features should be enabled by default, and any unused or insecure functionalities should be disabled by default
- Establish hard to crack, device-individual default passwords
- Personal data must be collected and processed fairly and lawfully, it should never be collected and processed without the data subject’s consent
- Make sure that personal data is used for the specified purposes for which they were collected, and that any further processing of personal data is compatible and that the data subjects are well informed
- Minimise the data collected and retained
- IoT stakeholders must be compliant with the EU General Data Protection Regulation (GDPR)
- Users of IoT products and services must be able to exercise their rights to information, access, erasure, rectification, data portability, restriction of processing, objection to processing, and their right not to be evaluated on the basis of automated processing
- Design with system and operational disruption in mind, preventing the system from causing an unacceptable risk of injury or physical damage
- Mechanisms for self-diagnosis and self-repair/healing to recover from failure, malfunction or a compromised state
- Ensure standalone operation - essential features should continue to work with a loss of communications and chronicle negative impacts from compromised devices or cloud-based systems
- Ensure that the device software/firmware, its configuration and its applications have the ability to update Over-The-Air (OTA), that the update server is secure, that the update file is transmitted via a secure connection, that it does not contain sensitive data (e.g. hardcoded credentials), that it is

signed by an authorised trust entity and encrypted using accepted encryption methods, and that the update package has its digital signature, signing certificate and signing certificate chain, verified by the device before the update process begins

- Offer an automatic firmware update mechanism
- Backward compatibility of firmware updates. Automatic firmware updates should not modify user-configured preferences, security, and/or privacy settings without user notification
- Design the authentication and authorisation schemes (unique per device) based on the system-level threat models
- Ensure that default passwords and even default usernames are changed during the initial setup, and that weak, null or blank passwords are not allowed
- Authentication mechanisms must use strong passwords or personal identification numbers (PINs), and should consider using two-factor authentication (2FA) or multi-factor authentication (MFA) like Smartphones, Biometrics, etc., on top of certificates
- Authentication credentials shall be salted, hashed and/or encrypted
- Protect against 'brute force' and/or other abusive login attempts. This protection should also consider keys stored in devices
- Ensure password recovery or reset mechanism is robust and does not supply an attacker with information indicating a valid account. The same applies to key update and recovery mechanisms
- Limit the actions allowed for a given system by Implementing fine-grained authorisation mechanisms and using the Principle of least privilege (POLP): applications must operate at the lowest privilege level possible
- Device firmware should be designed to isolate privileged code, processes and data from portions of the firmware that do not need access to them. Device hardware should provide isolation concepts to prevent unprivileged from accessing security sensitive code
- Data integrity and confidentiality must be enforced by access controls. When the subject requesting access has been authorised to access particular processes, it is necessary to enforce the defined security policy
- Ensure a context-based security and privacy that reflects different levels of importance
- Measures for tamper protection and detection. Detection and reaction to hardware tampering should not rely on network connectivity
- Ensure that the device cannot be easily disassembled and that the data storage medium is encrypted at rest and cannot be easily removed
- Ensure that devices only feature the essential physical external ports (such as USB) necessary for them to function and that the test/debug modes are secure, so they cannot be used to maliciously access the devices. In general, lock down physical ports to only trusted connections
- Ensure a proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of data and information (including control messages), in transit and in rest. Ensure the proper selection of standard and strong encryption algorithms and strong keys, and disable insecure protocols. Verify the robustness of the implementation
- Cryptographic keys must be securely managed
- Build devices to be compatible with lightweight encryption and security techniques
- Support scalable key management schemes
- Guarantee the different security aspects -confidentiality (privacy), integrity, availability and authenticity- of the information in transit on the networks or stored in the IoT application or in the Cloud
- Ensure that communication security is provided using state-of-the-art, standardised security protocols, such as TLS for encryption

- Ensure credentials are not exposed in internal or external network traffic
- Guarantee data authenticity to enable reliable exchanges from data emission to data reception. Data should always be signed whenever and wherever it is captured and stored
- Do not trust data received and always verify any interconnections. Discover, identify and verify/authenticate the devices connected to the network before trust can be established, and preserve their integrity for reliable solutions and services
- IoT devices should be restrictive rather than permissive in communicating
- Make intentional connections. Prevent unauthorised connections to it or other devices the product is connected to, at all levels of the protocols
- Disable specific ports and/or network connections for selective connectivity
- Rate limiting. Controlling the traffic sent or received by a network to reduce the risk of automated attacks
- Risk Segmentation. Splitting network elements into separate components to help isolate security breaches and minimise the overall risk
- Protocols should be designed to ensure that, if a single device is compromised, it does not affect the whole set
- Avoid provisioning the same secret key in an entire product family, since compromising a single device would be enough to expose the rest of the product family
- Ensure only necessary ports are exposed and available
- Implement a DDoS-resistant and Load-Balancing infrastructure
- Ensure web interfaces fully encrypt the user session, from the device to the backend services, and that they are not susceptible to XSS, CSRF, SQL injection, etc
- Avoid security issues when designing error messages
- Data input validation (ensuring that data is safe prior to use) and output filtering
- Implement a logging system that records events relating to user authentication, management of accounts and access rights, modifications to security rules, and the functioning of the system. Logs must be preserved on durable storage and retrievable via authenticated connections
- Implement regular monitoring to verify the device behaviour, to detect malware and to discover integrity errors
- Conduct periodic audits and reviews of security controls to ensure that the controls are effective. Perform penetration tests at least biannually

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number: TP-07-18-077-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-276-9
DOI: 10.2824/939028