Security and Resilience in eHealth

Security Challenges and Risks

www.enisa.europa.euEuropean 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 Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU 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 EU 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.

Authors

Dimitra Liveri, Anna Sarri, Christina Skouloudi, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We would like give special thanks to all the experts contributing to our study:
Franz Hoheiser-Pförtner, Vienna Hospital Association, Computer Department
Katrine Vedel, Health Innovation Centre of Southern Denmark
Mrs. Pia Jespersen, National eHealth authority of Denmark
Rünno Reinu, Estonian eHealth Foundation
Marina Mironova, Estonian Health Insurance Fund
Manuel Metz, ASIP Santé France
Eric Poiseau, INRIA and IHE Europe
Karima Bourquard, IHE-Europe and InteropSanté France
Andreas Grode, Gematik GmbH Germany
Dimitris Tsalikakis, 4th Regional healthcare Authority (RHA) Greece
Aidan Clancy, Department of Health Ireland
Fran Thompson, Health Service Executive Ireland
Hervé Barge, eSante, Luxembourg
Hrvoje Belani, Croatian Health Insurance Fund (CHIF)
Rui Gomes, SPMS - Portuguese Ministry of health shared services in Portugal
Emmanuel Andersson, Swedish eHealth Agency
Stéphane Spahni, Hôpitaux Universitaires de Genève (HUG)
Sang-Il Kim, eHealth Suisse
Walid Ahmed, Federal Office of Public Health of Swiss
Jeremy Thorp, Health and Social care Information Centre, UK

The study was conducted in cooperation with GNOMON, OtePlus and Vidavo Hellas and namely with Al. Berler, G. Makrodimitris (GNOMON); K. Panagiotakis, M. Legal (OTE Plus); El. Velidou, I. Pavlidou, P. Angelidis (Vidavo Hellas).

ISBN 978-92-9204-137-3, doi:10.2824/217830

Table of Contents

Executive Summary

Studies[1] have shown that cyber security incidents in eHealth systems can have a great societal impact. In a recent ENISA study, twelve out of eighteen Member States (MS) that participated in the survey- consider healthcare as a critical sector, therefore they should take all appropriate measures to protect their ICT systems and assets[2].

The scope and governance model of eHealth services may vary in the Member States (MS); it might be implemented as centralised or even decentralised and may be extended, offering cross-border services. Additionally, critical assets identification in the healthcare systems and infrastructures may be based on different criteria, such as business continuity, data security and integrity, services availability, eHealth security policy and legislation. Moreover usual practices, cyber security challenges, approaches to mitigate risks, and requirements for the eHealth infrastructures may converge, diverge or be inadequate.

The aim of this study is to investigate the approaches and measures MS take to protect critical healthcare systems, having as a main goal improved healthcare and patient safety. In that respect this study analyses:

- The policy context in Europe and the legislation of the Member States
- The perception of the Member States on critical assets in eHealth infrastructures
- The most important security challenges
- The most common security requirements
- Relevant good practices that have been deployed in the MS for eHealth security

Cyber security incidents affecting eHealth services and infrastructures cause great impact. As a result this study focuses on the availability, continuity and resilience of these systems and infrastructures. Issues like data integrity, data protection and data confidentiality are always important when we talk about eHealth, however this study aims at presenting another side of the same coin. It is important to analyse these systems from the availability and resilience angle to understand how great the societal impact could be should, for example, a network supporting 3-4 regional hospitals not be available.

To better understand the basic security challenges, features and applications in eHealth services, we focus on three basic use cases that are considered critical (based on a survey): Cloud Services supporting eHealth, Electronic Health Records (EHR)/Patient Health Records (PHR) and national eHealth services (i.e. ePrescription).

The following recommendations are targeted to Member State and Operators of critical eHealth infrastructures:

1. Member States should conduct an asset identification and a risk assessment to classify their critical eHealth infrastructures and services and develop a national catalogue.
2. Member States should introduce clear cyber security guidelines for the protection of their critical eHealth infrastructures and services.
3. Member States and healthcare organisations should perform an impact/cost benefit analysis of healthcare cyber security incidents and to use this as leverage for increasing investment on eHealth systems and infrastructures security.
4. Member States should develop incident response mechanisms to efficiently bring together the healthcare organisations with the national cyber security competent centres.

[1] http://www.healthcareitnews.com/news/4-5-health-orgs-hit-cyber-crooks

[2] ENISA survey on Critical Information Infrastructures https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

5. Member States and healthcare organisations should setup information sharing mechanisms to start exchanging knowledge and lessons learned on cyber security issues i.e. how they mitigate incidents, which are the security measures they take etc.
6. European Commission should encourage the development of baseline security measures for eHealth critical infrastructures and services. This should be done in coordination with the competent centres and the healthcare organisations operating the critical infrastructures.
7. Member States are encouraged to implement widely accepted security standards to achieve interoperability and provide the possibility to move towards a uniform European certification scheme.
8. Member States should invest in raising awareness of the citizens and healthcare organisations in providing cyber security training to personnel and users.
9. Member States' policy makers should make sure that eHealth is considered as a CIIP issue and should align with the national CIIP strategy and with the National Cyber Security Strategy (NCSS).

1. Introduction

New, more effective and efficient healthcare processes are being introduced. However, in the era of "digital Darwinism" (adapt to digital or lag behind) where technology, society and operation models rapidly evolve, the healthcare operation participant experience (professional, patient) is often suboptimal. Better healthcare for the patient at a highly controllable cost should be the main goal. The complexity of eHealth systems is very high, which renders information quality (completeness, integrity), accessibility and availability a very challenging task. Emerging healthcare data sharing schemes like EHR (Electronic Health Records) or PHR (Patient Health Records) as well as cross-border scenarios further complicate the technological challenges and respective protection requirements.

The term eHealth is widely used in academia, the private and public sectors, standardisation bodies, manufacturing organisations and vendors. eHealth systems extend from regional systems, where patients can access online basic data on their treatment, to national schemes like ePrescription services or cross border eHealth information sharing.

In this report, eHealth is defined as the use of electronic means to acquire, transfer or store healthcare related information and provide services used by health professionals and consumers[3].

Since 2006[4], many Member States, recognising the importance of this sector and the need for automation, have drafted national eHealth strategies which include important aspects for ICT adoption in the health sector; such as EHR, ePrescription, healthcare smart IDs, legal and security issues for eHealth systems, etc. In these strategies health information networks are considered a vital asset to protect; however in some cases no specific technical requirements, nor security measures nor controls have been formally established.

ENISA acknowledges the significance of eHealth not only as a major contributor to the societal and financial welfare of the EU, but more specifically as a critical information infrastructure and focuses for the first time on the security challenges and risks of ICT of the health sector in the Member States. Given that healthcare services have been recognized as a critical societal function[5], it is important to analyse the degree to which various eHealth systems and infrastructures are critical for the secure provision of healthcare services.

1.1 Policy Context

EHealth is a priority for the European Commission (EC): the overarching goals of the EC eHealth activities are:

- To improve citizens' health by making life-saving information available – between countries when necessary using eHealth tools.
- To increase healthcare quality and access by making eHealth part of health policy and coordinating EU countries' political, financial and technical strategies.
- To make eHealth tools more effective, user-friendly and widely accepted by involving professionals and patients in strategy, design and implementation.

In order to attain these goals, a set of policies have been put in place. Firstly, the EC has adopted the eHealth Action Plan 2012-2020, which offers a roadmap for attaining four operational objectives: (a) interoperability of eHealth services, (b) research, development and innovation, (c) uptake and wider deployment, and (d) international cooperation.

[3] http://www.who.int/trade/glossary/story021/en/
[4] http://ehealth-strategies.eu/
[5] EC directive on Critical Infrastructures (directive 2008/114/EC) http://ec.europa.eu/dgs/home-affairs/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf

Towards achieving the cooperation among the EU MS and the interoperability between electronic health systems, the eHealth Network was set up by the Directive 2011/24/EU. The eHealth Network consists of representatives from the 28 MS and its mission is to lead the cooperation among the MS, give direction to eHealth developments and adopt guidelines (such as the Guidelines on ePrescriptions Dataset for Electronic Exchange).

Further support to the issue of interoperability is provided by the Digital Single Market Strategy, which was adopted by the EC and defines eHealth as one of the critical sectors for which priorities for security and interoperability should be set for the benefit of patients, health professional, health systems and industry.

In the same context, the EC issued on 28th of July 2015 the Decision 2015/1302 on the identification of "Integrating the Healthcare Enterprise" (IHE) profiles for referencing the public procurement. This decision allows for the 27 IHE profiles to be identified as ICT technical specifications eligible for referencing in public procurement. The 27 IHE profiles are detailed specifications that optimise the selection of well-established standards describing the different layers of interoperability (i.e. protocol communication, technical, syntactical, semantic and application levels) with the aim to find interoperability solutions for exchanging or sharing health data. Hence, the IHE profiles have the potential to increase interoperability of eHealth services and applications to the benefit of patients and medical community.

Mobile health (mHealth) is a rapidly developing sub-segment of eHealth that covers medical and public health practice supported by mobile devices. It comprises a set of technologies which will bring a more innovative care access reducing healthcare costs at the same time. More specifically, mHealth includes the use of mobile communication devices for health and well-being services and information purposes as well as mobile health applications. The European Commission, having recognised the emergent role of mHealth in the transformation of healthcare, published in April 2014 a Green Paper on mHealth that considers existing barriers and issues related to mHealth deployment and analyses mHealth potential to maintain and improve patients' health and well-being and encourage their empowerment.

At the same time, according to the EC Directive on Critical Infrastructures[6], healthcare services have been recognized as a critical societal sector and therefore, healthcare systems are considered as critical infrastructures that should be protected by all types of threats, including cyber security attacks. Moreover, in the proposed NIS Directive, healthcare is considered as one of the critical sectors vital for the society.

1.2 Scope and objectives

This study focuses on eHealth information systems and infrastructures as well as on the relevant assets that are considered critical both for the society and the relevant stakeholder groups. As a starting point, this study aims to showcase how the MS perceive cyber security in their health systems, which are the specific approaches they follow and which are the measures they take to protect these systems. Examples of such systems are Healthcare information networks and systems, EHR, online ePrescription systems (supporting the drug prescription/dispensing/reimbursement cycle). Based on the criticality of these systems, the scope of this report narrows down to the availability, integrity of assets and continuity of the services.

ENISA takes stock of how Member States perceive eHealth security, which are the governance models and the specific requirements, and what are the measures they take to protect it. The aim of this study is to clarify the eHealth systems security perception in the MS; to identify the gaps and also to recommend, based on good practices, the next steps for the governmental authorities, the policy makers and specialists.

[6] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114

The objectives of this study are to:

- Identify national legislation on cyber security and eHealth, the governing authorities and the service provider organisation;
- Assess the perceived criticality of the relevant infrastructures and assets;
- Present the security priorities and challenges.

1.3 Methodology

The collection of information was conducted through two parallel activities: a desk research and a series of interviews accompanied by on-line survey process, to effectively acquire and validate the feedback.

- The desk research was focused on the use of ICT in eHealth, more specifically on cyber security risks, challenges and measures;
- The interviews with experts to collect analytical and granular information (country, regional briefs, strategy and governance issues, security requirements and measures, CIIP, use case scenarios)
- Additionally, the on-line survey targeted key experts of the field and was combined with the interviews, to get more specific information on good practices.

The stakeholders involved[7] (representing 18 EU MS and 2 EFTA countries) were either experts in cyber security related issues or academics conducting research or operators within the field of cyber security in eHealth with the following profiles:

- Public institutions responsible for eHealth strategy
- eHealth Competence centres
- eHealth platform Operators (CIOs, security officers, end points staff, system administrators)
- Academia
- User Associations – Networking organisations
- Standardisation Bodies
- ICT Industry (suppliers)

To better understand security risks the study assesses specific use case scenarios, seen from the CIIP point of view, based on the feedback received and the general perception. The study identifies actual instances of these scenarios which were validated by the respective stakeholders.

1.4 Target Audience

This report targets public sector experts in national authorities i.e. Ministry of Health, Ministry of State Affairs, competent Authorities (like eHealth national centres or cyber security centres) responsible for implementing the eHealth national strategy with or without mandate on cyber security and CISOs, as it offers recommendation on what are the steps to follow to protect their assets.

It is also useful for eHealth services providers (for the public sector), Operators i.e. hospitals and practitioners that use eHealth systems, as it provides advice on how they may implement security measures in their systems and what they need to do to comply with the requirements of a security policy.

[7] The specific contributions of each interviewee are intentionally left unmentioned, and the individuals are not directly quoted or linked to any given statement.

1.5 Structure

Following in chapter 2, an overview of policies and strategies on eHealth with specific reference to the Member States is presented. The criticality of eHealth infrastructures, examples of identified assets on specific use cases, as well as the security challenges related to these use cases, are presented in chapter 3.

Chapter 4 analyses the proposed Use Cases in terms of their criticality and security challenges faced. This Chapter also evaluates good practices in 3 uses cases that were assessed as the most prominent ones by the stakeholder's community. Chapter 5 present conclusions and elaborates some recommendations that could be seen either as input for future works or as issues that need to be properly addressed by the member states.

For the reader's assistance, a glossary of used terms is introduced in the Appendix. In Annex A, published as a separate document, the reader can see the country reports, with information on eHealth systems and infrastructures security in the 28 MS.

2. eHealth Security in the Member States

2.1 Overview of national legislation

The first step to understand the perception of eHealth in the MS is to identify the landscape and how Critical Information Infrastructure Protection (CIIP) is linked to eHealth. The approaches followed vary depending on the priorities of each country. We categorise them based on the existence of an eHealth strategy, on the specific legislation and on the way cyber security is included in the eHealth national framework.

In most countries an eHealth strategy exists, following the recommendation of the first EU eHealth Action Plan requesting the Member States to setup such policy documents to describe eHealth specificities, bodies involved and their responsibilities at a national level. Overall, eHealth infrastructures protection falls under the generic umbrella of CIIP. Currently, there is no specific regulatory framework on critical eHealth infrastructure protection. This information is presented in Table 1 (further information can be found in the annexed document named "Country Reports – Current Status on eHealth in the Member States" with references).

Table 1 Overview of eHealth legislation and policy in the 28 Member States

COUNTRY	RELATED LEGISLATION / STRATEGY / POLICY
Austria	• **Strategy:**"An information and communication strategy for a modern Austrian Health Care"(2006) • **Legislation**: Health Telematics Act (2012) / Electronic Health Record File Act (2012) • **eHealth and CIIP**: Austria has a specific legislation for Critical Infrastructure Protection. Healthcare providers should be compliant with the CIIP Act in order to participate in the eHealth Interexchange infrastructure
Belgium	• **Strategy:** eHealth Action Plan (2012) • **Legislation**: Law on the creation and organisation of the eHealth Platform (2008)
Bulgaria	• **Strategy:**National strategy for eHealth implementation (2006) • **Legislation**: The legislative act adopted in 2014 talks about implementing the eHealth card, the electronic reporting by healthcare providers and maintaining electronic health records. • **eHealth and CIIP**: eGovernment strategy of Bulgaria (2014-2020) describes eHealth as a critical sector
Croatia	• **Strategy:** National Health Care Strategy 2012-2020 (2012) and Strategic Plan for eHealth Development (2014) • **Legislation**: No eHealth specific legislation. Various aspects related to EHR are covered by legislation related to Medical practice and the protection of patient's rights. • **eHealth and CIIP**: In Croatia there is specific CIIP legislation is place. The mandate for eHealth CIIP lies within the Croatian Ministry of Health.
Cyprus	• **Strategy:** eHealth is being addressed in the overall eStrategy policy document of Cyprus • **Legislation:** There is no specific eHealth framework in Cyprus. The regulation of eHealth issues (such as EHR and ePrescription) is based on general health and data protection law. • **eHealth and CIIP**: Regarding cyber security issues, eHealth operators are overseen by the Cyber security Authority
Czech Republic	• **Strategy:** National eHealth Strategy (2008) • **Legislation:** No specific eHealth legislation. • **eHealth and CIIP**: In the law that focuses on Critical Information Infrastructures protection, eHealth systems have been classified as critical.
Denmark	• **Strategy:** National Strategy for Digitalisation of the Danish Healthcare Service (2011-2014). A new national public health and eHealth strategy for 2015-2018 is currently under preparation by the Ministry of Health.

COUNTRY	RELATED LEGISLATION / STRATEGY / POLICY
	• **Legislation:** There is no specific eHealth legal framework in Denmark. The legislative background for issues such as the exchange of healthcare information is provided by the General Healthcare Act and the Personal Data Protection Act. • **eHealth and CIIP:** The protection of critical eHealth infrastructure is covered by the general legislation on the protection of national critical infrastructures and the storage of critical data.

Estonia	• **Strategy:** The strategy is managed by the Ministry of Social Affairs in cooperation with the Estonian eHealth Foundation. The Foundation is updating the strategy currently and it is expected to be published by the end of 2015.
	• **Legislation:**
	  • Statute of Health Information System (establishes the ENHIS and regulates data protection aspects) (2008)
	  • Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents
	  • Types of Medical Images, Requirements of Information Technology therefor and Conditions and Procedure for Making them Available
	  • Overview of national laws on electronic health records. National report (2014)
	• **eHealth and CIIP:** eHealth is not mentioned as a critical infrastructure

Finland	• **Strategy:** eHealth Roadmap for Finland (2007), eHealth and eSocial Strategy 2015- 2020 / Growth and innovation strategy for the health sector, Genome strategy.
	• **Legislation**:
	  • Act on the Electronic Processing of Client Data in Social and Health Care Services (2007)
	  • Act on Electronic Prescriptions (2007)
	• **eHealth and CIIP**: KELA, the Social Insurance Institution of Finland, has internal documents for CIIP on ePrescription and patient data repository[8]

France	• **Strategy:** the eHealth strategy is led by the Health Ministry with all the national institutional actors (ministry of health, National insurance, national agencies). • **Legislation:** Projet de loi "Hôpital, Patients, Santé et Territoires" (2009), Projet de loi Santé (2015) • **eHealth and CIIP:** In France, health care is identified as a critical sector.

Germany	**Strategy:** German eHealth Strategy (2005)
	• **Legislation:**
	  • The "Act on safe digital communication and applications in the healthcare system" is expected to come into force on January 1st, 2016. The aim of this Act is to form the basis for profitable applications of the electronic healthcare card, the establishment and opening of the telematics infrastructure, the improvement of interoperability and the promotion of telemedicine applications.
	  • IT- Security Act (2015) – Act to implement security requirements like performing risk assessment, incident reporting, minimum security measures which applies to all critical sectors.
	• **eHealth and CIIP:** As healthcare in Germany is considered a critical sector, the above measures will affect the healthcare bodies. BSI will be the coordinating authority of this implementation.

Greece	• **Strategy:** eHealth roadmap (2006)
	• **Legislation:**
	  • Greek eHealth Policy (2014-2020) sets as priorities the restructuring of primary healthcare, pooling of financial resources, introducing new managerial and administrative methods, adopt cost effectiveness and monitoring mechanisms and developing policies for better resources allocation.
	  • Law 3892/2010 Electronic Recording of Prescription(2010) and 4328/2014 Network of Primary care(2014)
	• **eHealth and CIIP:** In Greece, the Ministry of Health is responsible for eHealth. IDIKA is the competent authority under the Ministry of Labor and implements the ePrescription services.

[8] http://www.kanta.fi/en/lainsaadanto

COUNTRY	RELATED LEGISLATION / STRATEGY / POLICY
Hungary	• **Strategy:** The key roadmap for eHealth was the "New Hungarian Development Plan 2007-2013", as it included the "Social Infrastructure Operational Programme" (TIOP) and the "Social Renewal Operational Programme" (TAMOP). Thereby, TIOP defined the physical infrastructure and development strategy as well as funds for health and eHealth, while TAMOP described the human infrastructure eHealth Roadmap. • **Legislation:** The applicable legal framework (act on the processing and protection of health care data and associated personal data) is currently being amended and once in place the National EHealth Services Platform shall be established.
Ireland	• **Strategy:** The eHealth Strategy for Ireland was published in December 2013 and the detailed implementation plan thereof is expected to be published within 2015. • **Legislation:** *Law on "national health identifier number for citizens, professionals and organisations"*
Italy	• **Strategy:** National eHealth Information Strategy (2011). • **Legislation:** Act 221/2012 defining the main principles on EHR
Latvia	• **Strategy:** eHealth Strategy (2006). • **Legislation:** Regulation No 134 on a unified health information system (2014)
Lithuania	• **Strategy:** "eHealth Strategy for 2007- 2015", E-health System Development Program for 2009 – 2015. • **Legislation:** The Law on Cyber Security (which entered into force on 1 January 2015) • **eHealth and CIIP:** In Lithuania eHealth is identified as a critical sector. The Ministry of Health is responsible for general supervision of the entire healthcare system.
Luxembourg	• **Strategy:** Luxembourg has a detailed eHealth Action Plan since 2006. • **Legislation:** The legal framework was defined in the Act of 17 December 2010 on the reform of health care.
Malta	• **Strategy:** The main national document addressing eHealth is the National Information Communication and Technology (ICT) Strategy for Malta of 2008 • **Legislation:** There is no comprehensive eHealth legislation in place.

Netherlands	• **Strategy:** no dedicated eHealth strategy document
	• **Legislation:**
	  • Code of Conduct Electronic Data Exchange in Health care
	  • Proposal on patient's rights with regard to electronic data processing (2013)
	  • Medical Treatment Contract Act
	  • General Administrative regulation with regard to the electronic exchange of data between healthcare providers. This is supplementary to the aforementioned and focuses in compliance.

Poland	• **Strategy:**The Plan of the Informatisation for eHealth for the years 2010-2015, Policy paper for the health care 2014-2020 • **Legislation:** Act on information system in the healthcare (2011). • **eHealth and CIIP:** In Poland eHealth is considered a critical information infrastructure thus making for all ehealth systems obligatory the implementation of the provisions required. The Minister of Health has the overall responsibility for healthcare and its organisation. The National Center for Health Information Systems is a unit in the MoH.
Portugal	• **Strategy:** Strategy for the National Electronic Health Record (2010) • **Legislation:** There is no comprehensive eHealth legislation in place. • **eHealth and CIIP:** In Portugal all eHealth infrastructures are critical. Software components are not the main issue in criticality, network availability and hardware and storage resilience is. Another issue that concerns criticality is that interdependence of IT systems main cause critical failures in other systems due to their

COUNTRY	RELATED LEGISLATION / STRATEGY / POLICY
	interconnection. In Portugal, most of the public sector ehealth system are operated by SPMS and offered as central systems to the healthcare providers. A working group has been set up within the cyber security authority in order to perform a gap analysis for security measures.
Romania	• **Strategy:** There is no eHealth specific strategy**.** • **Legislation:** Romania operates a central EHR system under the Health Reform Law 95/2006[9], that requires the Ministry of Public Health to establish an integrated information system for public health management.
Slovakia	• **Strategy:** ○ Strategic Goals of eHealth – key tool of public governance informatisation in the area of healthcare (2008) ○ eHealth Program in Slovakia (2008-2020) • **Legislation:** Act no. 153/2013 on the National Health Information System
Slovenia	• **Strategy:** ○ Strategy for informatisation of the Slovenian health care system 2005-2010 (Ministry of Health, 2005) ○ Resolution on the National Health Care Plan for the period 2008-2013 (Ministry of Health, 2008)
Spain	• **Strategy:** In Spain, there is no specific eHealth strategy at the national level. Issues pertaining to eHealth are indirectly addressed in the Avanza Plan and the National Health Plan. Furthermore, several regions in Spain have developed their own eHealth strategies.
Sweden	• **Strategy:** National eHealth – the strategy for accessible and secure information in health and social care (2010) • **Legislation:** ○ Patient Data Act ○ Act on Electronic Prescription
United Kingdom	• **Strategy:** United Kingdom pursues several distinct healthcare strategies, as NHS develops its own solutions in accordance with its respective legal framework. In fact UK has 4 independent NHS systems for England, Whales, Scotland and Northern Ireland.

2.2 Common deployment models in EU MS

Some MS are moving from the "healthcare data capture" stage to the "data analysis" and "data sharing" stage. The main goal is to improve healthcare via informed treatment decisions. As previously described, the "data sharing" stage involves the deployment of healthcare networks, which can securely retrieve patient data from various sources and make them available to the patient and the responsible healthcare professional. Relevant schemes like EHR and PHR, are currently trending in various MS. The eHealth models deployed in various MS vary, as analysed below:

Structural features of the model

National vs regional (or centralised vs decentralised) structures characterise eHealth in Europe. Moreover, hybrid models and loose connection (also called federation) of regional structures can be found. These features may influence both organisational and technological structures.

[9] http://legeaz.net/PdfDoc/legea-95-2006-actualizata-2012.pdf

In some MS the eHealth model is centralised with the mandated ministry assuming the overall responsibility, whereas in other MS part and/or the entire responsibility is assigned to regional authorities. It should be noted, that in a few MS, the regions develop their own eHealth legislation and/or eHealth systems.

Spain's decentralised/regional [1] eHealth system

Health care in Spain is highly decentralised among the 17 Regions. The Ministry is responsible to coordinate and to assure equality. The decentralisation of services, and the growing mobility of citizens make it necessary for services providers (Regions) to collaborate beyond their boundaries, to provide quality services focused on patient safety.

Spain has a regional deployment of e-prescription system [2], interconnected at the national level (47,5 mil. eDispensations performed in 2014 - 70% of dispensations). Spain also has a regional EHR deployment.

Spain's model incorporates a powerful central switching point allowing for the addition of services required to the national healthcare system, to ensure its sustainability and evolution.

Hospital-system driven

This approach, identified in one EFTA European country, puts in the driving seat one of the main eHealth stakeholders, the hospitals. In this case, the hospital developed its own eHealth infrastructure and eHealth application, including a PHR application.

Switzerland: Geneva HUG[10]

The university hospitals of Geneva deployed 'my medical dossier, an online electronic health record where all the health data that need to be exchanged between physicians, hospitals, laboratories and insurance companies are stored[3]. Hug was created in 1995, when all public hospitals in Geneva were merged and now hug covers the whole spectrum of outpatients and primary, secondary and tertiary inpatients care, including long-term rehabilitation and psychiatry. In 2013 60,000 admissions and over 900,000 outpatient visits took place, while 6,000,000 laboratory testing were done [4]. Mon dossier medical today includes clinical and non-clinical processes into a patient-centered care service and covers complete order entry for all orders including lab, drug, radiology, and care; unified clinical documentation; administrative information; access management; imaging; and laboratory information. Mon dossier medical itself is always the result of a real-time query of all relevant databases in the system [5].

Cross-border use cases

Cross-border use cases have been deployed within the EU-sponsored Large Scale Project (epSOS LSP). Pilot projects on specific use cases have been evolving to official & standardized healthcare information exchanges, gaining increased traction, through ongoing EU sponsored activities. In this case the deployment model is crossing European Countries, while certain services are deployed centrally (e.g. value coding and transformation services, required to provide semantic interoperability between MSs).

Cross- border e-Prescription and e-dispensing between Sweden and Finland[6]

Within the EPSOS project, **Finland** and **Sweden** developed a pilot service between pharmacies in Finland and pharmacies in Sweden. Around 10.000 user of the myKanta system in Finland gave their consent to participate in the pilot, which resulted in one of the more successful pilots of epSOS. The number of exchanged electronic prescriptions was quite moderate but many features and needs came up from this pilot, especially in the semantic domain where real case issues came up concerning drug substitution, active ingredient matching and others. Most of those problems are currently dealt under the project openMedicine, which will allow effective semantic interoperability amongst member states in the domain of electronic prescription.

[10] Exemplar case that is referenced throughout the report as good practice for eHealth services practices. CH is not EU but an EFTA country, which are also partly in scope of this report.

3. eHealth and Cyber Security

Nowadays incidents occurring in eHealth systems that affect their availability are common. As an example, the NHS in the England has suffered six data breaches every day since 2011[11] study states; hospital systems and networks can be affected as every other network by viruses[12] resulting into denial-of-service attacks and affecting for days all operations in the hospital, a common phenomenon[13]; malicious physical attacks can compromise data integrity and availability[14]; healthcare organisations are being targeted by sophisticated and highly organized cybercriminals who are showing every day how vulnerable the eHealth systems are[15]. And the situation keeps getting more difficult. Nations should realise how vital their national eHealth systems are and take all necessary measures to protect them.

Healthcare systems are becoming vulnerable to cyber security incidents due to various reasons; the volume of information and the connection with patients dictates the use of automation and IT; the diverse nature of healthcare information systems enables different devices to access the Internet (even though not designed for this) thus making them easy targets; many outdated applications and systems didn't include security as a priority requiring close attention of the information security officers and finally the exponentially increasing attack surface is making systems compromise an easier task. Combining these reasons with the fact that a breach of security can impact large parts of the population[16] makes eHealth a critical sector.

The analysis of the collected information is presented in this section: the most important reasons behind classifying eHealth systems as critical are described, as well as some of the most prominent security challenges.

3.1 eHealth as a Critical Information Infrastructure

Not all MS consider eHealth as a critical sector; in some cases eHealth services formulate a different category of emergency services and are not classified as critical, in other cases healthcare ICT services are not considered critical as the environment is considered so isolated that any incident would have small impact. Criticality of eHealth infrastructure is identified through three different perspectives:

a) The first perspective, healthcare business continuity, examines which assets (infrastructures and services) are required to ensure baseline functionality of the entire eHealth system and vitality to society. Under this perspective, central components and / or services that comprise the backbone of the eHealth system are considered as critical. These components may include health provider or patients' index service, document registries, medical databases, eHealth specific identifier services etc.
b) The second perspective is data security and integrity. It examines data storage components, 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). An analysis on specific assets for a given use case can be found in section 3.2.
c) The third perspective focuses on availability. For example, if the unavailability of a service is creating high impact to the society, such as loss of life, then this service is critical. In this perspective, applications like EHR are considered to be critical, whereas network availability is crucial. Additionally, systems and services

[11] http://www.computerworlduk.com/news/security/3586072/nhs-suffered-six-data-breaches-every-day-since-2011-study-finds/?intcmp=in_article
[12] Dynes, Information Security and Health Care: A Field Study of a Hospital after a Worm Event, Technical Report, Centre for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover, New Hampshire, 2006.
[13] http://www.volkskrant.nl/wetenschap/ziekenhuisapparatuur-slecht-beveiligd-tegen-computervirussen~a3946259/
[14] https://www.secnews.gr/90665/isma%CE%AD%CE%BA%CE%B8%CE%B5%CF%83%CE%B7-%CE%B1%CF%84%CE%BF%CE%BC%CE%B9%CE%BA%CF%8E%CE%BD-%CF%80%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CF%8E%CE%BD-%CE%B1%CF%80%CF%8C-%CE%BA%CE%BB%CE%BF/
[15] http://www.computerworld.com/article/2914741/cybercrime-hacking/researchers-hijack-teleoperated-surgical-robot-remote-surgery-hacking-threats.html
[16] www.computerworld.com/article/2975988/healthcare-it/more-than-80-of-healthcare-it-leaders-say-their-systems-have-been-compromised.html

that are directly linked to the patient's care as diagnostic systems and Intensive Care Unit (ICU) and the systems that aggregate information related to patient's care are considered as critical as well.

In this study, to depict the critical assets in eHealth systems, we follow the approach as described in the diagram below. First the critical eHealth service is identified. Then it is broken down to core applications, which are in turn broken down into CII assets. This is a common approach the MS could adopt to decide their focus when classifying eHealth infrastructures.

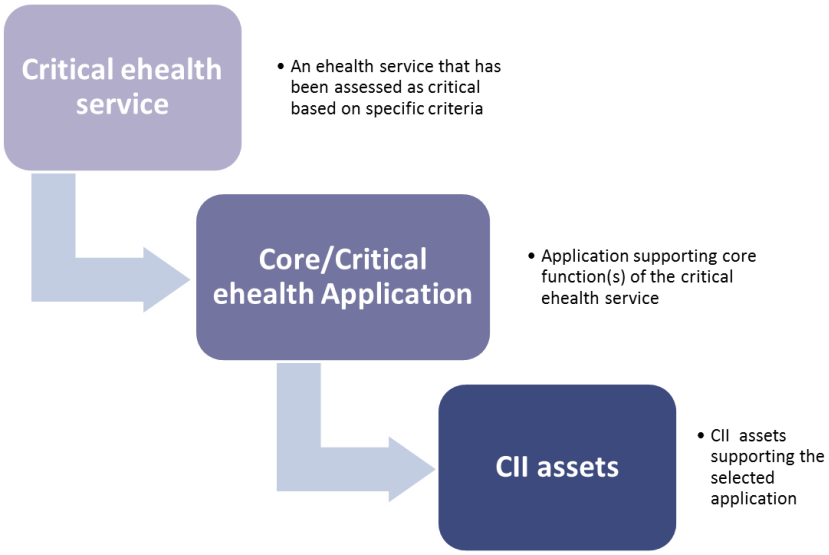

Figure 1 Steps to identify CIIs

However most MS have not developed a specific methodology, legislation or regulation for the identification of critical eHealth infrastructures[17]. Rather, the identification and protection of critical eHealth infrastructures is based on the general regulation and strategy for CIIP – wherever this is applicable.

As underlined during the stock taking, not all Member States have defined critical eHealth Infrastructures and identified relevant assets. Therefore, the process to protect the latter is based mainly on efforts of each healthcare Unit or system Operator.

3.1.1 National approaches

It should be noted that eHealth is not acknowledged as a critical sector in all Member States. In many cases, eHealth is identified as part of a critical sector such as Healthcare services and/or ICT.

Countries that identify eHealth as a critical sector address the protection of critical eHealth infrastructures according to the general legislation and guidelines that describe how national critical infrastructures should be protected and how critical data should be stored, protected and handled. In many cases infrastructure criticality is handled according to civil protection law, together with telecom infrastructure, transport communications, etc.

Austria's eHealth regulation

Austria's eHealth regulation is closely bound to e-government regulation (data protection act, CIIP law) as well as to civil protection law. Common practice is that central state administration bodies (e.g. ministries that are responsible for the critical sectors) identify the

[17] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/Methodologies-for-identification-of-ciis

critical infrastructures based on a defined process, maintain a database of critical infrastructures and prepare a risk analysis of the critical infrastructure.

In most cases, the CIIP mandate lies within the organisation that is responsible for CIIP in general, while in very few cases, an eHealth organisation has a CIIP mandate. If there is no such mandate, then the responsibility is assumed by the organisation that is overall responsible for the public healthcare sector, e.g. the Ministry of Health. If there is a national security agency, and no other competent authority has a mandate on cyber security, then a common practice is that they provide cyber security expertise horizontally in all sectors.

Examples of CIIP approaches

In **Greece** CIIP is handled horizontally via the civil protection legislation under action programs such as Perseas and Xenocratis. In other words this means that eHealth infrastructure is considered of critical impact if it becomes unavailable in case of emergency. However since Greece hasn't performed a national assets risk assessment, health care systems cannot be considered as critical information infrastructures.

In another example, **Estonia** has a nationwide approach concerning IT system security and defer the responsibility of eHealth CIIP to the Estonian eHealth Foundation. Although, eHealth is not considered as a CII in Estonia.

In **Finland**, the CIIs as well as all eHealth infrastructures are regulated by law: Act on the Electronic Processing of Client Data in Social and Health Care 159/2007.

In **Germany** the new IT Security Law includes security measures for all critical information infrastructures, ehealth services are considered critical. As BSI is the national security agency of Germany, they are the competent authorities to orchestrate the implementation of the provisions required by the law, and to monitor them, provide guidelines etc.

A third approach would be the one based on voluntary initiatives/ measures by healthcare units not aligned to any central or regional initiative (e.g. Geneva region EHR initiative leading the national EHR plan, 4th Greek RHA Healthcare Units initiatives).

From this information we conclude that there is no specific scheme when talking about critical information infrastructures protection governance, each country follows a model that is tailored to its needs. However it is very important to underline that identification of the assets and the infrastructures should be done through cooperation of the national authorities with the operators of the systems.

3.2 eHealth critical systems and assets

Having discussed the approaches followed in order to assess criticality, we present specific ICT assets which can be identified as critical for the proper operation of an eHealth system. Given that the scope of eHealth systems is very wide and the operational models and ICT implementations of a specific use case may vary, the attempt to analyse and identify assets is based on examples, to identify through them significant assets which can impact the proper operation of an eHealth system in case of failure.

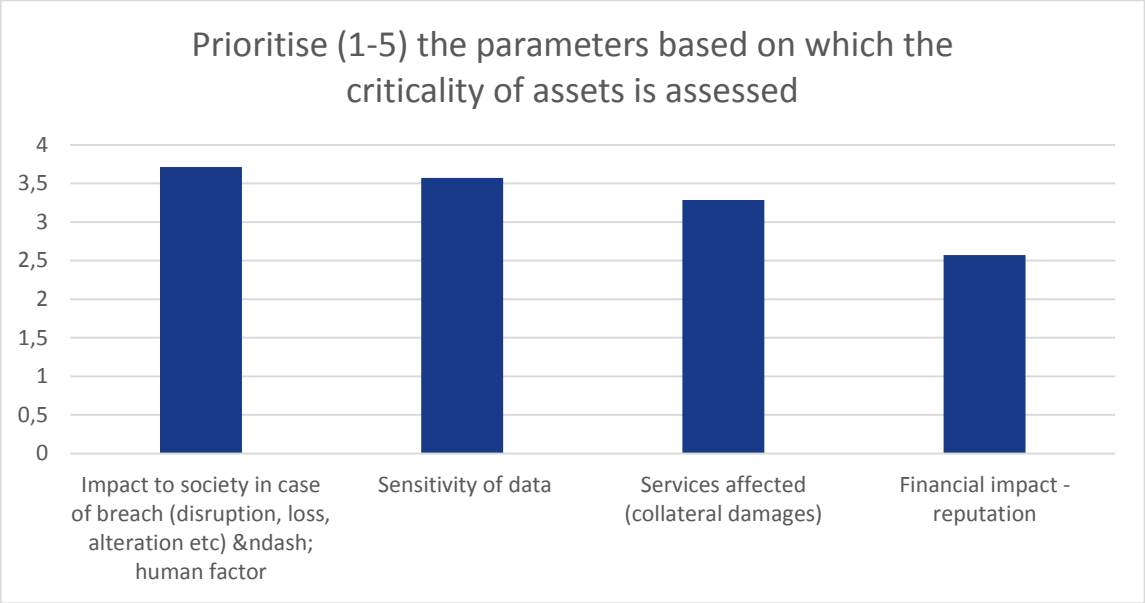

Figure 2 Criteria to assess criticality of assets

Operational models served by eHealth systems may vary in their functional aspects (e.g. a system may serve only e-prescription use cases, while another may serve both e-prescription & patient summary) and/or in legal aspects since they have to follow the legal framework and organisational model of each MS. Modern heavy duty information systems are characterized by a very high technical complexity and therefore technical implementation approaches vary. Moreover, alternative design models may be followed when implementing systems (e.g. EHR systems have been designed and implemented based on alternative ICT architectures with variant centralization degrees).

Based on the information received by the interviewees, assets considered as critical are:

- Health Information systems, i.e. the information networks in the hospitals;
- Clinical data repositories i.e. the databases in each hospital where information is stored locally;
- Authentication server i.e. to perform access control and authentication of users;
- Laboratory Information System (LIS)
- Radiology Information Systems (RIS);
- Picture Archiving and Communication Systems (PACS), i.e. transferring radiology results;
- Electronic Health Record components;
- Patient Health Record service;
- ePrescription service;

We present below two examples of systems that were reported critical by all our interviewees, the EHR system and the e-Prescription.

Example A: electronic health record (EHR) system

While there is sufficient support in academic literature and analysis, there is limited standardized architectural design of an EHR. It is stated that there are centralised and distributed architectural options. Architectural options are depicted in Figure 3. The HL7 EHR functional model (FM) defines a standardised model of the functions that may

exist in EHR systems. From the outset, a clear distinction between the EHR as a singular entity and systems that operate on the EHR – i.e., EHR systems is critical[18].

Even though many definitions exist for EHR, the official ones, according to ISO TR 20514 health informatics - electronic health record, are presented below.

> 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.

Several EHR architectures have been deployed throughout the world[19]. The most commonly recognized are: the centralised /fully integrated model, the decentralised/federated model and hybrids of the two models. As depicted in Figure 3, different architectural approaches are followed by those countries which have deployed EHRs. In the centralised model all the responsibilities, including cyber security, are in the mandate of one body, this might be the Ministry of health (MoH) or the national eHealth centre. They are also responsible for EHR, and all healthcare organisations (hospitals, GPs etc.) are directly reporting to them. On the other hand in the de-centralised scheme EHR is powered by the operator but instances exist in the several healthcare organisations.

In the EU, the NHS (UK) has deployed a centralised EHR architecture (called integrated EPR[20]). Germany, Denmark, Spain are deploying a decentralised EHR model based on a service oriented architecture, while the Netherlands are deploying a federated EHR model[21].

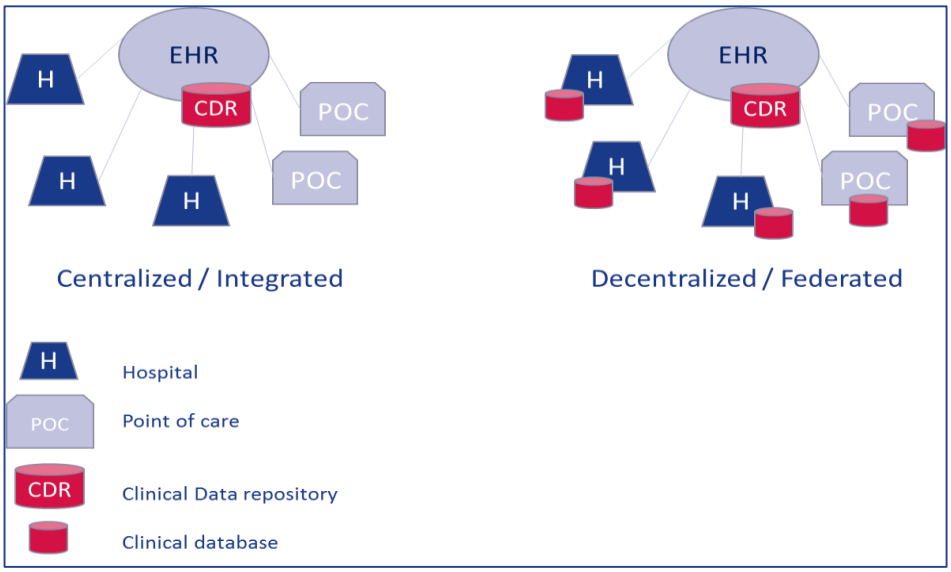

Figure 3 EHR architectural models (see glossary)

[18] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=18
[19] http://www.corepointhealth.com/geni/health-information-exchange-architecture-types
[20] http://mthink.com/article/federated-and-centralized-it-architecture-models-for-portable-ehrs/
[21] Bernd Blobel, Head, eHealth Competence Center, University Hospital Regensburg, Germany, Jahrestagung der HL7 Benutzergruppe Schweiz, Oktober 2012

An EHR focusing on continuity of the care record (containing various patient healthcare episodes of care and respective results throughout time) will need to extract data from many sources (e.g. healthcare unit databases, e-prescription systems, healthcare practitioner medical notes) as depicted conceptually in a very simplified mode in Figure 4 the 'assets analysis' below is based on the main ICT component categories.

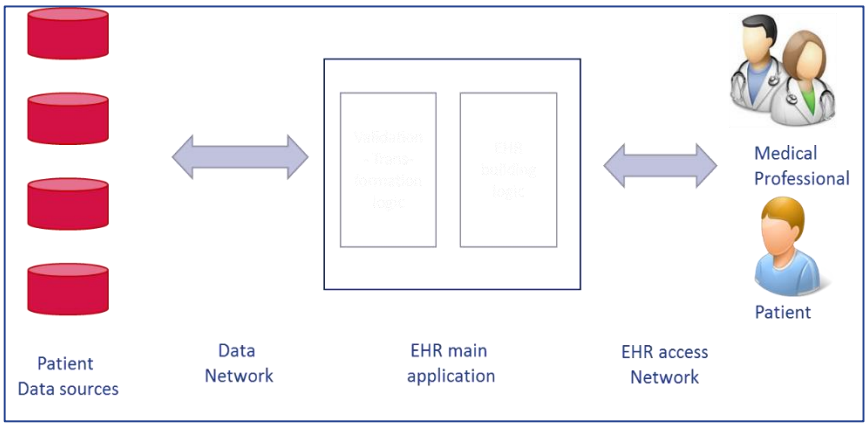

Figure 4 EHR data flow

When data are not persistently stored at the main EHR application, which is a common design option, then there is no single database asset involved. Therefore the resilience of the overall system is high, given that it depends neither on a single data source (several data sources are involved), nor on a single central database asset. Listed below are the critical assets that constitute the EHR system together with what will happen in case of failure and the impact an incident would cause.

ASSET	IMPACT IN CASE OF FAILURE
Components of network connecting the healthcare operators with the EHR system	Loss of availability (no access to the information)
Identity management system, for access control and authorization	Loss of availability (no access to classified information)
Web, Application and database servers	Loss of availability (no access application services)
Business process and Application logic assuring data integrity	Data integrity violation
Interoperability Enterprise Service Bus – document exchange interface	Loss of availability (no information exchange between point of care sites)
Databases and storage components	Loss of availability (no storage and retrieval of information)
Monitoring and logging of information exchanges	Confidentiality violation (unmonitored access to sensitive information)
User management and Patient consent application	Confidentiality & data integrity violation (misuse and illegal access to information)
Master Patient Indexes, Healthcare Providers registries	Data integrity violation

Table 2 EHR assets analysis

Example B: e-prescription / e-dispensing system

E-Prescription systems have been mentioned during the survey by MS stakeholders as a significant eHealth initiative.

An e-prescription / e-dispensing system serves the patient's need on the prescription and dispensing of medicine and automate/optimize the process, which is depicted in a rather simplified mode in Figure 5. 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.

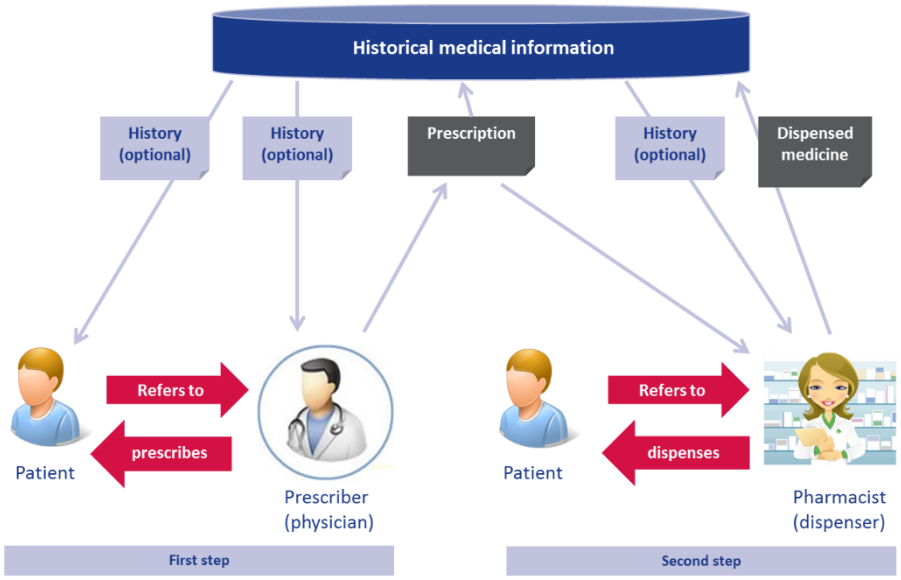

Figure 5 E-prescription / e-dispensing core cycle

An e-prescription / e-dispensing system may commonly be a web-based application. Usually, e-prescription systems are based on very thorough and analytical interoperability frameworks based on international standards that allow secure and quality proofed information exchange between the systems at the different points of care. Such real world examples are deployed in countries such as Denmark, Sweden, Greece, Croatia, Finland etc.

Even though actual ICT implementations are expected to differ, best of breed ICT approaches are commonly followed, namely: redundant components at all levels to enhance resilience (three-tier architectures/web/application/database tier), deployment of primary and secondary data centre sites, enhanced perimeter and internal security measures (e.g. several types of firewalling techniques, audit logging at many levels, SIEM tools).

Such a system may be serving tens of thousands of medical doctors and pharmacies, especially when deployed at a national level. Therefore it has to be highly resilient and scalable. Service outages though not life threatening, may cause serious distress to the society. Assets critical to its operation are depicted below.

ASSET	IMPACT IN CASE OF FAILURE
Components of network connecting the healthcare operators with the e-prescription system	Loss of availability (no access to the information)
Identity management system, for access control and authorization	Loss of availability (no access to classified information)
Web, Application and database servers	Loss of availability (no access application services)
Business process and Application logic assuring data integrity	Data integrity violation
Interoperability Enterprise Service Bus	Loss of availability (no information exchange between point of care sites)
Databases and Storage components	Loss of availability (no storage and retrieval of information), loss of data integrity
Monitoring and logging of information exchanges	Confidentiality violation (unmonitored access to sensitive information)
User management and Patient consent application	Confidentiality & data integrity violation (misuse and illegal access to information)

Table 3 ePrescription assets analysis

3.3 Security Challenges in eHealth

IT security in healthcare systems, services and applications is positioned as a major concern due to the high privacy and confidentiality requirements of sensitive healthcare data. EHealth faces many security challenges; the great majority of which are common to any critical infrastructure. In the interviews conducted for the purposes of the current report, the respondents were asked on which are the most important cyber security challenges in eHealth infrastructures and systems. The results are depicted below:

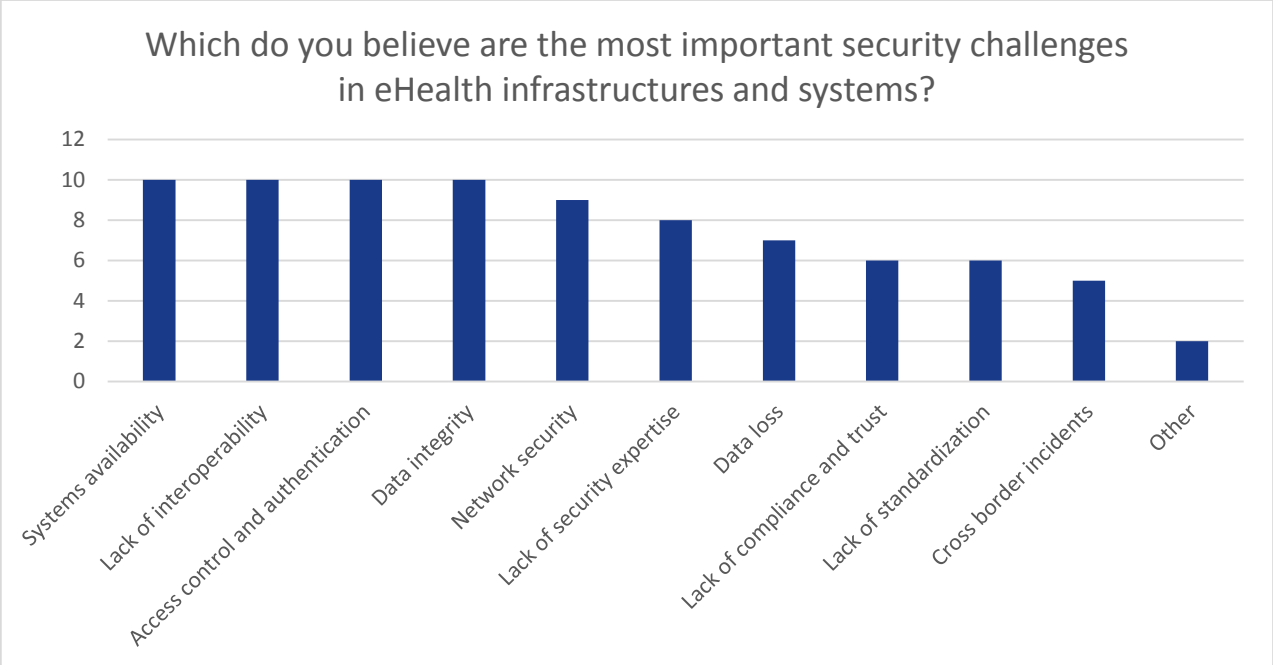

Figure 6 Security challenges

Systems availability

Systems availability is the basic feature for achieving continuity of electronic healthcare. It is about continuous accessibility of critical health information by authorized professionals in order to ensure the best healthcare services. Systems availability may relate to physical systems function (e.g. networks, storage) and affect significantly the healthcare delivery. In HUG (Hôpitaux Universitaires de Genève), if the network is down, the healthcare providers cannot access patient's data and cannot prescribe. Generally, the more digitized the health sector in a country, the more the health services are affected by interruptions in eHealth infrastructures. The HUG is highly digitized (documentation, imaging, laboratory systems, patient administration systems). Therefore, network and information system availability are considered to be very critical. Systems availability may also relate to the maturity of business continuity infrastructure and process in place, namely, systems integration. A violation of the processes protocol may lead to the interruption of services. A typical example is to experience an interruption because an operator might proceed to an update without following the protocol. In this case, the impact on the continuity of services can be really high. For example, in Estonia, if central services are interrupted, 1600 healthcare providers are affected. Another parameter which may affect business continuity is the type of the model that is used in eHealth services. In case this model is not patient-centric, a patient may easily have hundreds of separate, overlapping records in various systems and this limits the availability of information[22], a condition which affects patient safety and leads to unnecessary duplication of tests and investigations, so it increases the cost of the services[23]. Under the umbrella of systems availability falls also the application security for

Lack of interoperability

EHealth infrastructures include many diverse systems and applications interconnected at various scales i.e. a medical device collecting clinical data can be linked in the same network that a computer uses to access Internet. A core issue for an effective and secure use of these services is to ensure a high level of interoperability and guarantee that

[22] Access Control and Integration of Health Care Systems: An Experience Report and Future Challenges, Lillian Røstad, Øystein Nytrø, The Second International Conference on Availability, Reliability and Security, 2007

[23] Developing National eHealth Interoperability Standards for Ireland: A Consultation Document, Health Information and Quality Authority, Ireland, 2011

information is transmitted safely through individual information systems, health service institutions, healthcare providers and patients[24] and, on the other hand, that the recipient's system is able to use the information received in order to proceed in various actions[25]. For example, the vocabulary used in EHR, namely the terminologies, the classifications, the metadata[26], or the cloud services among different cloud service providers, local or external clouds, must be based on universally applied standards and an agreed-upon framework or some open protocols/APIs for secure information exchange and services integration[27].The lack of interoperability may also affect the security updates in an eHealth services network. For instance, some healthcare providers in Estonia still used Windows XP until the previous autumn, while all the software companies were about to stop producing updates for this operating system, so this was a significant obstacle to take all the necessary security measures for the stakeholders. In the current report, 25% of the survey respondents claimed that there is no interoperability framework in place at their organisation.

Access control and authentication

A recent study by KPMG[28] showed that among the greatest vulnerabilities in data security is sharing data between third parties and insiders (breaches by employees). This finding indicates access control and authentication as key security features in eHealth infrastructures. Authentication is the initial stage of the users' validation in order to determine their identity which is necessary to ensure that they are authorized to access the system. Once authenticated, the information level that they are allowed to view or share for organisational purposes is defined by an access control policy[29]. Access control is one of the main safeguards for ensuring data privacy and integrity[30]. A centralised system (e.g. an HIS) with limited external connection has a specific perimeter which needs to be safeguarded. In such a case, internal user access control becomes a higher challenge than external access control. On the other hand, a distributed EHR or a mHealth chronic disease management system needs to prevent unauthorized access on data over the network. Apart from enforcing authentication and access control, the need to retain at the same time a user-friendly system is of great importance since it helps avoiding errors introduced by the user. Additionally, with respect to the prevention of inappropriate or illegal disclosure it is crucial for providers of health data to be sure that parties who consume data enforce, in turn, access constraints conformant to the purposes under which that data was provided. Therefore the definition and enforcement of access rules for health data and services throughout clinical workflows is a precondition for any cooperative patient treatment[31].

Data integrity

One of the most common cyber security challenges in eHealth is ensuring quality and integrity of the data that are stored and exchanged for clinical and administrative purposes. Examples include clinical laboratory test results, patient demographics, medication related information, radiology reports and images, pathology reports, hospital admission, discharge and transfer dates, etc. Data integrity is crucial, as errors in personal or clinical data may affect a person's medical treatment, insurance or employability[32]. These errors are often related to incorrect entry by staff,

[24] e-Health Cloud: Opportunities and Challenges, Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi, Future internet, 2012
[25] E-QUALITY IN E-HEALTH, Stakeholders' reflections on adressing e-health, Health First Europe, 2010
[26] Data Integrity in an Era of EHRs, HIEs, and HIPAA: A Health Information Management Perspective, AHIMA, Dan Rode, MBA, CHPS, FHFMA Vice President, Advocacy and Policy,2012
[27] Developing National eHealth Interoperability Standards for Ireland: A Consultation Document, Health Information and Quality Authority, Ireland, 2011
[28] Health care and cyber security: Increasing Threats Require Increased Capabilities, KPMG, 2015
[29]Privacy Oriented Access Control for Electronic Health Records, Randike Gajanayake, Renato Iannella, Tony Sahama, In Data Usage Management on the Web Workshop at the Worldwide Web Conference, ACM, Lyon Convention Centre, Lyon, France, 2012
[30] Access Control in Healthcare Information Systems, Thesis for the degree of Philosophiae Doctor (PhD), Norwegian University of Science and Technology, Trondheim, January 2009
[31] http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf
[32]Ensuring Data Integrity in Health Information Exchange, AHIMA Thought Leadership Series, American Health Information Management Association, 2012 p.2

incorrect conversion from a paper-based filing system to electronic health records[33] [34] and improper or insufficient use of standard based healthcare information exchange protocols[35] [36] [37].

Network Security

A fundamental challenge in securing eHealth infrastructures is considered to be network security, and according to the interviewees, this is highly related to many security incidents. Network security becomes critical when the security of other critical assets relies on the security of the network. This is a top priority when the eHealth system is network based (e.g. EHR/PHR, cross border eHealth). Recent reports indicate that one of the main vulnerabilities of an eHealth network are the inadequate firewalls by 27% and place the external attackers as one of the major threats by 65%[38], while the 81% of health care executives surveyed claim that their organisations experienced attacks by at least one malware, botnet or other cyber-attack during the past two years and only half feel that they are adequately prepared to prevent attacks[39].

Security expertise and awareness

A critical parameter for achieving and maintaining a high security level in eHealth systems and networks appears to be the security expertise. The security practices by personnel are considered a source of potential problems and appear to be a significant challenge, as in some countries, like Austria, the human factor is considered the most important cause of security incidents. Thus, ensuring that the security architecture and all the respective procedures and measures that must be followed are well designed, understood and applied by all relevant stakeholders in an organisation is of high importance. A critical factor which contributes to awareness raising is the appropriate, adequate and sufficient organisational structure and especially the role of a security officer. Nowadays 20% of healthcare providers don't have a leader solely responsible for information technology security[40] and -in some countries, like Estonia- a security officer placement is an organisational structure mandatory by law only for public sector. Therefore many concerns are raised for the private sector security practices, since the lack of this asset may lead to misuse of security standards and a gap between security policy and work practices[41] [42]. Finally, another major concern regarding the lack of security expertise is that the 23% of organisations do not have a security operations centre to identify and evaluate threats[43].

Data loss

The digitalization of information and the high level of eHealth services penetration in the healthcare sector mean that a significant amount of vital, personal and confidential data are stored in digital format. In this framework, the protection of the data from loss is considered to be very important. On the other hand, sometimes it is impossible to avoid ending up in such a critical situation (e.g. software and hardware faults, network faults, security attacks, and natural disasters), so data recovery and the timeframe that it can be achieved is closely related to data loss. Common causes of data loss are unauthorised access to clinical patient data by IT vendors and by healthcare organisations personnel and the back-up policy[44]. A European Hospital Survey on benchmarking the deployment of

[33] http://www.aaos.org/news/aaosnow/dec14/managing8.asp
[34] http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/E/Electronic-Health-Records-Security-and-Privacy-Concerns.aspx
[35] http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049675.pdf
[36] http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_WP_HITStdsforHIMPratices_Rev1.0_PC_2015-06-19.pdf
[37] http://www.ihe.net/Technical_Framework/upload/IHE_ITI_White-Paper_Enabling-doc-sharing-through-IHE-Profiles_Rev1-0_2012-01-24.pdf
[38] HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities, KPMG, 2015
[39] http://www.kpmg.com/us/en/issuesandinsights/articlespublications/press-releases/pages/81-of-healthcare-organizations-have-been-compromised-by-cyber-attacks-in-past-2-years-kpmg-survey.aspx
[40] HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities, KPMG, 2015
[41] Williams, P.A.H. (2008). When trust defies common security sense. Health Informatics Journal
[42] Adams, A. and Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. International Journal of Human-Computer Studies, 63 (1-2), 175-202.
[43] Health care and cyber security: Increasing Threats Require Increased Capabilities, KPMG, 2015
[44] http://www.rendta.com/portfolio-item/the-true-cost-of-clinical-data-loss/

eHealth services showed that 73% of the hospitals have an archiving strategy for long-term storage and disaster recovery, while 23% don't and only 14% are able to proceed to an immediate recovery and 42% in less than 24 hours[45].

Standardisation, Compliance and trust

One of the main concerns in attaining security in eHealth infrastructures is the proper use and persistence to create, maintain and enforce an interoperability framework so that integrated systems contributes to cost reduction in eHealth[46]. Some experts expressed concerns around the applied security policy from the third-party providers. The European Commission has foreseen this need and thoroughly studied it during the HITCH and ANTILOPE projects. In some countries, like Estonia, providers from the private sector are not obliged to comply with a specific and detailed security standard. Additionally, eHealth professionals in Estonia find the requirements defined in the data protection act to be abstract, something that results in problems in practice.

Cross-border incidents

Cross-border eHealth services play a significant role, especially in the European framework of free mobility for citizens across the EU, since it is one of the main instruments to reach globally the public health objectives ensuring the safety of emergency care and the continuity of non-emergency care. The challenges that shall be tackled in order to facilitate transferability of data in cross-border healthcare are mainly related to building a common interoperability and access control and authentication framework[47]. For example, the Estonian ID-card is issued only to citizens and residents of Estonia. The Mobile-ID requires activation with an Estonian ID-card; consequently Mobile-ID is also available for Estonian residents only and there is no support for qualified certificates issued by other countries[48]. The European Commission has invested substantial human and financial resources to prevent cross border incidents from happening. The extensive use of integration profiles such as IHE ATNA, provide effective logging of information exchange that minimise the case of cross border incidents.

Incidents management

Incidents management is a major challenge in eHealth security. Although 75% of the respondent's implement security policies in their eHealth systems and/or infrastructures, there are incidents that can be neither anticipated nor avoided. Security incidents root causes include, human errors, natural phenomena, malicious actions (DDoS attack, MITM attacks, etc.) and system failures (including third party failure, i.e. hardware failure). System failures and human errors account equally for the majority of the incidents reported. Deliberate human intervention to disrupt the workflow (i.e. malicious actions) also accounts significantly for jeopardizing security, whereas the impact of natural phenomena accounts for a small only portion of the reported security incidents. It has to be noted that human factor may also relate to malicious actions, from the perspective of causing system holes by negligence or oversights, which could lead to system inefficiencies and thus make the infrastructures vulnerable to possible attacks. Human error also includes incorrect security practices by personnel which may result in security

Figure 7 Common root causes of security incidents

[45]European Hospital Survey: Benchmarking Deployment of eHealth Services
[46]Developing National eHealth Interoperability Standards for Ireland: A Consultation Document, Health Information and Quality Authority, Ireland, 2011
[47]E-QUALITY IN E-HEALTH. Stakeholders' reflections on adressing e-health: challenges at the European level, Health First Europe, 2010.
[48]eID Interoperability for PEGS: Update of Country Profiles study Estonian country profile

incidents, so, apart from implementing cyber security measures, awareness raising and training are very important to building a secure system. Therefore, eHealth organisations need to have an incident response capacity, in order to timely identify incidents and restore and reconstitute systems and services in a trusted manner. Apparently, there is a need to develop an eHealth specific incident reporting, classification and alerting mechanism in pan European level. International good practices could be consulted towards this direction.

3.4 Information security requirements for eHealth

Security requirements, which the operators have to meet, are drawn from the legal framework of each EU MS, as well as the EU directives which have been transposed in the MS. The legal framework requirements are sometimes described at an abstract, non-technical level. Thus operators have to assess risks and security options and deploy appropriate measures, depending on ICT architecture and technology deployed.

Generally, the security objectives in eHealth, according to the interview respondents of the current report, are shown in the graph below.

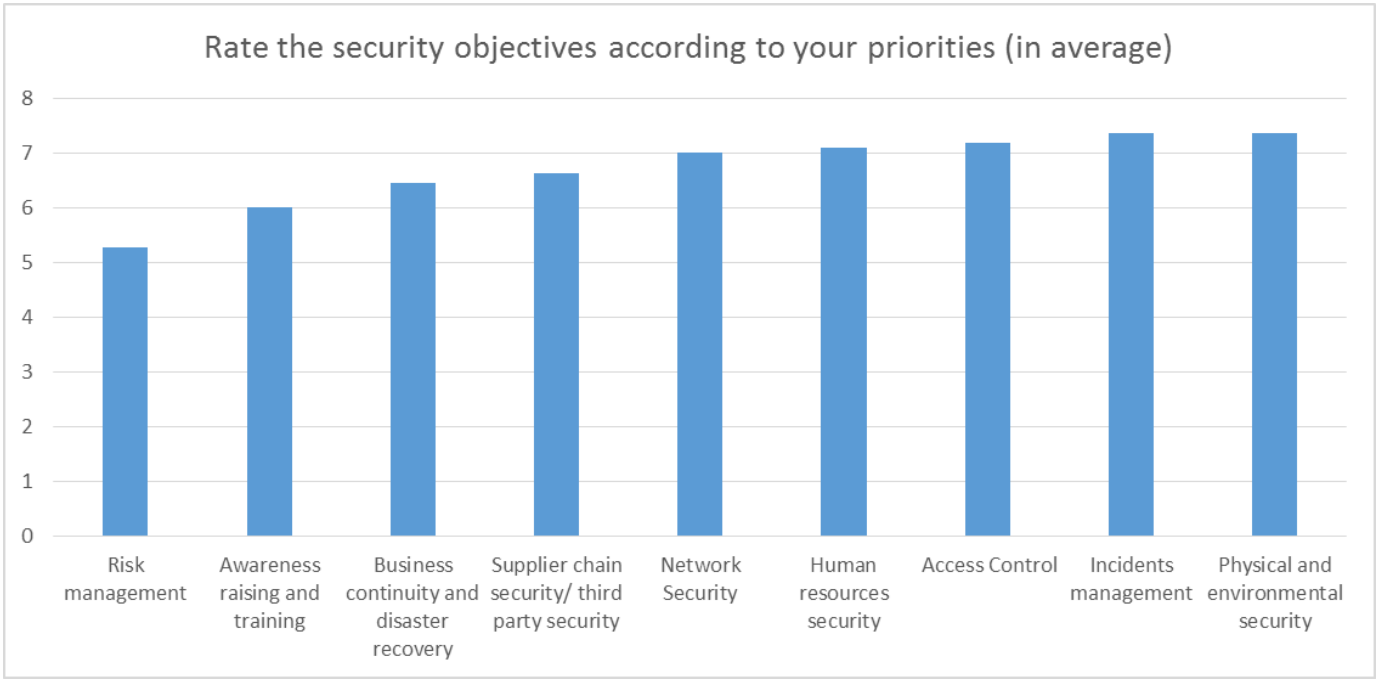

Figure 8 – Security Objectives

Incidents Management

According to the findings of the conducted surveys and interviews, one of the top priorities in security appears to be the management of incidents. Many countries pointed that incident reporting is the key for improving security planning and measures. Some countries have already built helpdesks or reporting mechanisms. For example, in Ireland, there are regional incident helpdesks and the incidents are usually managed by the vendors, while the establishment of a single virtual helpdesk is planned. In Estonia the security officer of the eHelath Foundation reports to the Foundation's management board and Ministry of Social Affairs reports directly to the CERT Estonia. In France, the eHealth authorities report directly to the security officer of the Ministry of Health. However, although there is an established mechanism for reporting and resolving incidents in these countries, there isn't in place a regulatory framework and the action plan is based on informal guidelines. Furthermore, in Greece, the external eHealth services providers are contractually obliged to report incidents.

Physical and environmental security

The second top security requirement in eHealth is considered to be the physical and environmental security, which is usually included in the acts covering the protection of the national infrastructures in each country. This is a very wide subject which may refer either to the protection from physical disasters or to the mechanisms that protect infrastructures from intruders and control the entrance to restricted areas where they can gain access to specific information. A basic principle for the physical protection of data is to ensure that file servers are located in secure areas safeguarded from unauthorized access and environmental threats such as fire, flood, loss of power etc. Additionally, all equipment used to store or process critical data may be recorded and any movements tracked to ensure that any theft or loss is detected in time[49]. In the UK, the physical security technologies that are used to control the entrance in restricted areas and use IT systems and communication over IP networks can be divided into three types: (a) Automatic Access Control Systems (AACS) (b) Closed Circuit Television (CCTV) (c) Intrusion Detection Systems (IDS)[50].

Network security

The network architecture and the network equipment (e.g. switches, routers, firewalls, anti-malware / anti-virus servers, security patches and updates servers, domain controllers, application servers, workstations, support laptops, event logging systems etc.) should be sufficient and meet the operational security requirements. On the other hand, network security also relates to secure data transmission. Therefore in many countries a secure connection platform is established exclusively for e-government or eHealth network. For example, in Ireland a platform was built for the exchange of health data, named Healthlink Online. It utilizes 128-bit SSL encryption and digital, client and server, certificates are required to initialize a TLS session. Data sent via a TLS connection is protected by encryption. It also employs the use of V-LANs, multiple firewalls and VPNs to ensure the data remains as secure as possible.

Access control

A very significant priority for ensuring security in eHealth appears to be access control, as it is the instrument to control data protection –both in terms of integrity and privacy- and ensure that the user who has access to a specific information is well-trained and able to use it efficiently for the appropriate purpose. Some of the main requirements for a secure access to patients' data include[51]:

a) The use of a unique identifying reference for each patient (the NHS number or similar);
b) Access to the system permitted only where there is a "legitimate relationship" between the system user and the patient;
c) Registration of all users with a central authority to obtain a smartcard and a pass code (chip and pin). For example, in Estonia there is a three-level authentication system used (notably): (i) knowledge-based authentication, where the server identifies the clients by their user names and passwords (ii) device-based authentication, where the server identifies the client using a specified object, such as a chip card, magnetic card or key (iii) biometrical authentication, where the server identifies clients by the voice, face, fingerprint or retina.
d) Strict prohibitions on the sharing of access cards and passwords;
e) "Role based" access for every registered user which defines the extent to which information can be accessed and amended. Staff will only be able to access as much information as is needed for the purpose of their role, for example, a clinic clerk may only have access to administrative information;

[49] Information Security Policy of Scotland, NHS in Fife http://www.nhsfife.org/nhs/index.cfm?fuseaction=nhs.policydisplay&p2sid=4F3677D5-E613-00B6-CEBF46733EC2AD2E&themeid=E44C37C3-5056-8C6F-C003CD63C15D8FF0&objectid=9E398034-9B81-470D-8C3F113B70249902

[50] Physical Security over Information Technology, Guidance Document by the CPNI(Centre for the Protection of National Infrastructures), March 2014 http://www.cpni.gov.uk/documents/publications/2014/ps%20over%20it%20issue%201%20final.pdf?epslanguage=en-gb

[51] Electronic health records: data protection issues in Europe By Clare Sellars and Dr Amanda Easey IPM&T Group, McDermott Will & Emery UK LLP, issue of BNAI's World Data Protection Report, April 2008

f) Introduce continuous manual or automatic auditing mechanisms of accesses made by staff as a requirement i.e. did the doctor really have a patient relationship while accessing the patient information?
g) Data classification according to access levels. In Finland, the health information systems are separated into two groups: Group A can access the central eHealth hub after certification; Group B cannot access national services, but the system manufacturer must still make a self-declaration of compliance with guidelines, while compliance of Group A systems is checked by a third-party certification authority accredited to do so by the Finnish Communications Regulatory Authority. In Switzerland, there are three data classes, administrative data that can be seen by all professionals, utility data that can be seen by all healthcare providers (e.g. weight, laboratory test results, special follow-ups) and health data which are classified into three subcategories: (i) basic data, which can be seen by the healthcare providers to whom the patient has granted access (ii) stigmatizing data which can be seen only by healthcare providers, provided the patient has given his consent (iii) secret data, which also can be seen only by clinicians, provided the patient has given his consent;
h) An audit trail (accountability) whereby records are kept of all instances of access to a patient's care record, with alerts triggered when access is not justifiable. Specific individuals will be responsible for reviewing such alerts and taking appropriate action;

Business continuity and disaster recovery

As the continuous provision of health services to patients is a major concern, it is very important to ensure systems availability and recovery from incidents. In order to achieve business continuity in eHealth, organisations should meet several requirements:

i. Regular data and software back-up procedures in order to provide contingency backup;
ii. Back-up copies of operational configuration files for the I.T. infrastructure including server and networked equipment (IP address ranges, firewalls, etc.) should be kept in a secure place. This will allow the quick recovery of the infrastructure if a disaster occurs[52].
iii. The option not to deploy a central EHR repository in order to reduce the risk of illegitimate large scale data availability (e.g. Austrian ELGA approach).

Supplier chain/third party

The supplier chain/third party security is a common major concern in information security which also affects eHealth security. Several countries establish SLAs with ICT integrators, where security level requirements and incidents reporting are included.

Awareness raising and training

Also, awareness raising and training of the personnel is of high priority in order to enforce the knowledge on the information security processes and data protection procedures and consequently reduce human errors. In this direction, a very prevalent security measure is the placement of an IT security officer in every healthcare organisation. For example, HUG (Hôpitaux Universitaires de Genève) started employing a security officer five years ago. Appropriate training on the permitted use of patient information according to the relevant requirements of data protection law.

[52]Information Security Policy of Scotland, NHS in Fife http://www.nhsfife.org/nhs/index.cfm?fuseaction=nhs.policydisplay&p2sid=4F3677D5-E613-00B6-CEBF46733EC2AD2E&themeid=E44C37C3-5056-8C6F-C003CD63C15D8FF0&objectid=9E398034-9B81-470D-8C3F113B70249902

Risk management

Risk management turns out to be a significant objective in eHealth security, as it includes, firstly, the identification of critical assets and potential threats and, secondly, the risk analysis and impact evaluation of potential incidents on healthcare delivery and patients' safety[53].

Further requirements

Furthermore, various approaches have been also stated, aiming at augmenting security:

- Compliance with international standards. The use of ISO standards and relevant security measures, have been referenced (i.e. ISO 27000 series and ISO 80001), especially in the deployment of internal information systems (such as HIS/CIS). IHE security measures (e.g. IHE ATNA, etc.) have been mentioned, especially in distributed use cases.
- Internal and external security audits on a regular basis, in order to monitor the application of the security measures and the traces of the access in personal data. Government eHealth Agencies may be mandated to review Healthcare Operators and decide whether the latter need to take further protective ICT measures. For example, in France, hospitals are audited every 2-3 years by an independent organisation, named High Health Authority, in order to verify that their operation complies with the general and IT security standards. If a hospital does not follow the security requirements, then it is not able to acquire the security certification and has to stop accepting patients. In England, there is no specific framework for auditing, however there is a licensing program in place and the hospitals/GPs are obliged to mark their progress (self-assessment) to show that they comply with guidelines and policies (national toolkit).

[53] eHealth for Safety Impact of ICT on Patient Safety and Risk Management, European Commission, October of 2007

4. eHealth Use Cases

4.1 Overview of Use Cases

This study identified several Health IT implementation scenarios (i.e. use cases) taking into account current trends in eHealth[54], European Union policies in the domain[55] and deployment models that are either widely accepted by the eHealth community or they are expected to emerge in the near future. The basic scope of those use cases is to study the impact of data integrity, data availability and resilience of eHealth infrastructures. Those use cases are presented in the following table.

Table 4: eHealth's Use Cases

USE CASE	SHORT DESCRIPTION	RESILIENCE AND DATA INTEGRITY
Cloud services in healthcare	Sharing information and medical processes within a healthcare stakeholders' network by establishing public, private or hybrid cloud infrastructures.	Public Sector entities usually have very secure network facilities. In most cases Private clouds are established with high access credentials, encryption and logging operating services
Big data and healthcare analytics for public health	Healthcare management needs statistics about the patient's history and anonymized patient data for public health and health policy needs	Usually Health Data are not part of open data schemes. Thus, indirect use of data for healthcare analytics run on complex de-identification scenarios taking into account patient consent policies.
Smart Hospitals	Intra-hospital wide access to the current healthcare information (administrative, transactional, medical)	Usually, hospital infrastructures are closed networks restricted for administrative and clinical support. Many establishments envision the use of web and social media to interact with patients. Currently such services are either in pilot phases or under future considerations.
eHealth services (ePrescription, Patient summary, referrals)	Region/Nation-wide access to transactional patient health information for multiple purposes (patient summaries, electronic prescription, patient consent management, electronic orders and referrals, etc.)	This type of services have been introduced in most 21st century eHealth roadmaps, so that immediate e-services can be provided to citizens and patients. Those services often use the web as the networking protocol as they rely mostly on interoperability of systems and users. Such Interoperability assets are of great importance. In most of the cases widely accepted standards are proposed for example HL7, IHE, DICOM, etc.
mHealth and telemonitoring applications	Sharing information about the medical background and history of a patient by a healthcare professional via remote access medical devices and mobile applications	MHealth seems to be closely assessed at policy level, mostly as it allows to shift healthcare systems from healthcare delivery (illness treatment) towards wellness and prevention (manage health quality). Both certification and health technology assessment are now in the focus before solving the resilience of such eHealth services.
EHR/PHR operations	An EHR is a systematic collection of health history and status of a citizen. It can provide	EHR and PHR facilities are also widely defined as milestones in national and regional eHealth

[54] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63383,
[55] Antilope Project: http://www.antilope-project.eu/front/index.html

	information on administrative, financial or statistical nature and quality control. There are many definitions and interpretations for the meaning of EHR. The basis of a worthy EHR is the quality of information it collects. Health care providers can improve the quality, accuracy and availability of information by increasing the speed of processing claims, and by improving productivity. Personal health records (PHRs) contain the same types of information as EHRs — diagnoses, medications, immunizations, family medical histories, and provider contact information — but are designed to be set up, accessed, and managed by patients.	roadmaps and currently such services are either operational or under development. Data integrity and resilience issues are considered very important for the operations of those services. Interoperability standards are used to solve the operation equation (covering also security and monitoring of data) so that those services can be provided to the appropriate end users.
Cross Border Healthcare	Sharing information about the medical background and history of a patient by a healthcare professional in another country	Cross border healthcare has been introduced in EU as required to secure universal quality of service delivered across MS. Those settings are currently operated on a pilot basis and will be established until 2020 via the Connected Europe Facility Programme. Security specifications are based on commonly approved interoperability standards to secure data integrity.

Respondents ranked the level of criticality of these Use Cases, from low, medium low, high and very high, according to their experience and the contribution of these systems to their everyday job. The purpose of this criticality assessment is to identify the Use Cases that are most valuable to the eHealth community and therefore focus our future efforts in terms of research, good practices and recommendations.

The result of this qualitative analysis is depicted in the following diagram:

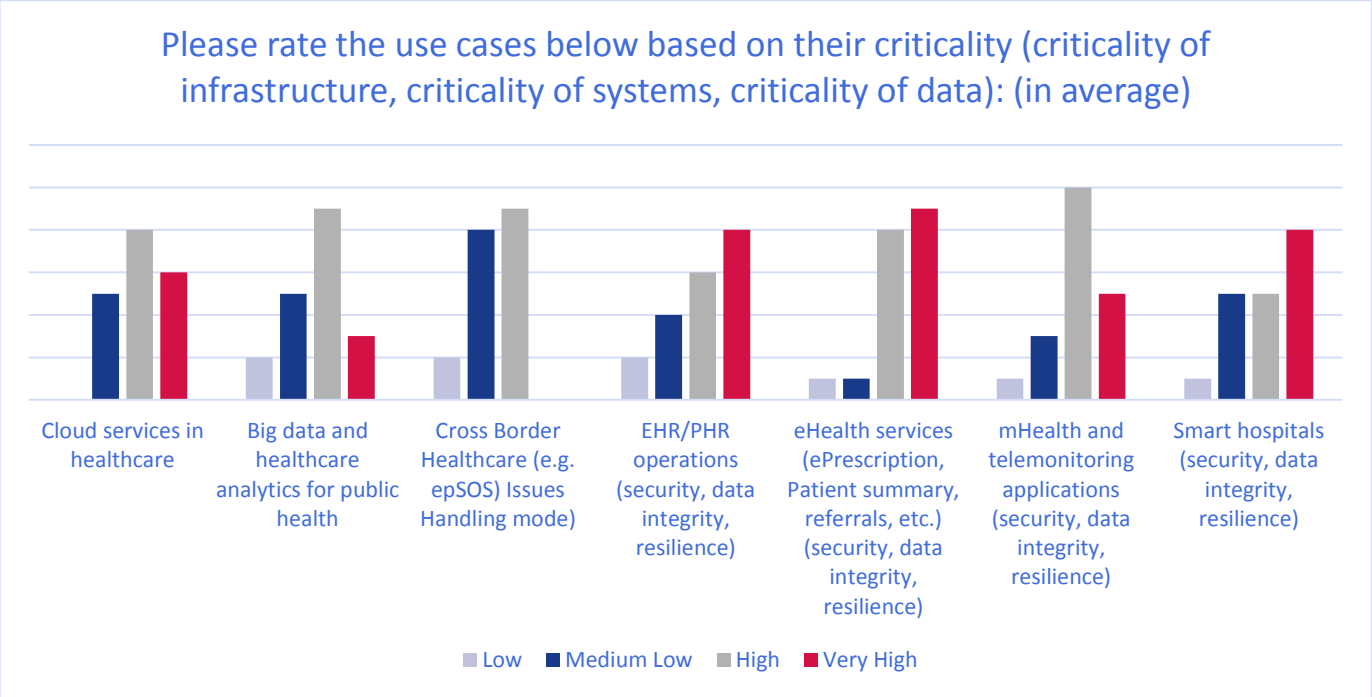

Figure 9–Criticality of Use cases

The diagram above establishes some initial conclusions on the existing and future deployment models in eHealth:

1. Criticality is noted as of most importance in cases where services are already deployed or under deployment, i.e. EHR/PHR operations, eHealth services, smart hospitals.
2. Criticality is correlated mostly to point of care delivery systems
3. Many respondents noted that some use cases may become dominant in the future but still have a lot of procedural, legal and administrative issues to be solved. This is the case for cloud services, mHealth and telemonitoring, cross border healthcare and big data and healthcare analytics.

Based on the above results, 3 uses cases are further analysed as interesting study cases that need to be assessed for security and data resilience. Those use cases are the ones that are already in use or have an important impact in matter of data integrity and resilience. The rest of the use cases are valid, but they are either expected to become prevalent in a medium to long term timeframe, or they have already established data integrity and resilience strategies from well-established protocols on which, end users and security officers have already specified countermeasures and security policies.

Those use cases are:

1) Cloud services in healthcare: Cloud services are a new phenomenon in healthcare. Disruption of those services may create discomfort, nevertheless, denial of service is usually not life threatening. Most respondents ranked this use case of high or very high impact in terms of criticality
2) EHealth services (ePrescription, Patient summary, referrals): Lack of eServices operation may create discomfort to end users. Most of the time those processes are transactional processes that deal with further value added services and administrative tasks (reimbursement, etc.). Most responders noted the high or very high importance of this use case, since such services are now the cornerstone of many national or regional health IT strategies.
3) EHR/PHR operations: EHR/PHR act as a supportive mechanism to point of care information systems. Many EU countries have deployed (for example, Luxembourg, Denmark, Finland, Estonia, France, Romania and other) or

are in the process of deploying such services (for example, Greece, Cyprus, Italy and other) aiming at providing value added services to citizens, healthcare providers and the public health policy. As such, they are gradually gaining recognition in the end user communities and they are considered critical information infrastructures while they acquire and reuse healthcare information.

4.2 Use Cases analysis

In this section, three use cases are analysed in detail. For each one of them, purpose and relevance are included. The study also reflects the domains where those use cases have been or could be potentially applied, the scale (cross border, national, regional or local deployment), the information that is exchanged and used and the key users, stakeholders that actively take part in each case. Additionally, security parameters are mentioned such as potential risks, security requirements, eHealth assets, and criticality. Finally, proposes some references of existing good practices in each use case.

Cloud Services in Healthcare

TITLE	CLOUD SERVICES IN HEALTHCARE
Purpose	Sharing information and medical processes within a network of healthcare stakeholders by establishing public, private or hybrid cloud infrastructures.
Relevance	Healthcare professionals need access to the patient's information. They are using smart technology via open networks, mostly targeting at accessing securely pre-existing e-services. Other type of cloud services incorporates use of social media or other technologies to create open services with healthcare orientation (allocation of medical practices, second opinion services, comparison of diagnostic protocols, transfer and translation services of health data, geolocation, civil protection and other related services). Cloud services usually focus on open data services especially for public cloud.
Domains	• Medication • Laboratory • Radiology • Patient Summary • Referral and Discharge reporting • Participatory healthcare • Telemonitoring • Multidisciplinary consultation
Scale	Cross Border, National/regional, inter-organisational
Information	• Patient Summary • Patient consent • Healthcare transactions • Patient discovery • Healthcare documentation retrieval • Providers registries
Participants / stakeholders	• Healthcare professional (HCP) all categories • Patients
Potential eHealth Assets	• EHealth data centre /data room • Web Service (e.g. for ePrescription, eDispensation, patient summary, patient cross-referencing) • EHR Socket-based service (e.g., HL7 MLLP) • EHR Service (either socket or web service) deployed in a physically unsecure environment • Usage of unsecure communication channel in Hospital (e.g., unencrypted message exchange in Wi-Fi networks) • eHealth information database • eHealth portal

	• epSOS NCP to NCP WAN network • PKI infrastructure • Tele-surgery application & network • Cloud based application to store measurements and auto-alert the patient • Cloud based Clinical information system (CIS) • eHealth Web Service

Potential Risk	• Network security
	• Systems availability
	• Lack of standardisation
	• Lack of interoperability
	• Lack of security expertise
	• Access control and authentication
	• Data loss
	• Other
	  ○ Data privacy
	  ○ reliable network infrastructure (especially mobile)
	  ○ Health IT has a lack of funding, which may lead to substandard quality levels. Moving to high-quality managed services such as the Cloud may be harder. The cost of moving may offset the cost benefit of the economies of scale. [56]

Security Requirements	• Health care providers must have a service level agreement in place with their cloud service provider in order to
	  ○ Meet cloud service availability requirements
	  ○ be obliged to follow state privacy and security laws
	  ○ adhere breach notification requirements
	  ○ meet appropriate back-up and disaster recovery provisions
	  ○ meet performance requirements[57]

Criticality	High (cloud services is a new paradigm in healthcare. Disruption of those services may create discomfort but denial of service is usually not life threatening), Most experts ranked this use case as high to very high though.
Additional Remarks and Challenges	This use case is not a high priority in the Member States. Some Countries have noted that they foresee to use cloud based services for supportive and administrative tasks (document management, etc.) and some of them foresee to assess the private cloud model in a very restrictive and controlled way to secure sensitive data. This use case is highly regulated from upcoming EU guidelines, recommendations and futures directives. Most countries will wait for those to be established before incorporating this use case in their strategy. Nevertheless, mobile and web technological hype distinguish this use case since seed capitals, investment funds and other evangelists foresee a fast growth of demand on such services. This would require that this market be regulated to secure patient data integrity and avoid misuse of sensitive information. Challenges noted by experts include the need to properly define what cloud computing is in healthcare, the needed legal background for the proper use of sensitive information, regulate the ICT market in the domain to protect from illegal or improper use of information. Many experts clearly noted that, as things are today, they would not invest in creating cloud based services. So technology is present but business scenarios need to be validated both from an ethical point of view and a legal point of view. One such business scenario that has been excessively validated is the chronic disease management using telemonitoring services. This is a typical IoT - cloud based service scenario where sensor data are aggregated, processed and distributed over the cloud. Telecom operators' value-added service departments have recently started piloting on such services.
Current practices	Cloud computing is an emerging use case in Europe. Nevertheless some member states have envisioned the use of such approaches. For example SPMS, the Portuguese eHealth competence centre is using cloud based services for document managements and document processing. Cyprus intend to create a private cloud for the implementation of the electronic healthcare record. In Greece the Greek Research & technology network is implementing a cloud computing repository of health data.

[56] COCIR eHealth Toolkit, Integrated Care: Breaking the silos, Fifth Edition,European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, May 2015

[57] http://www.covingtoneHealth.com/2015/04/moving-to-the-cloud-some-key-considerations-for-healthcare-entities/

EHR/PHR Operations

TITLE	EHR/PHR OPERATIONS
Purpose	An EHR is a systematic collection of health history and status of a citizen. Moreover, it can provide information on administrative, financial or statistical nature and quality control. There are many definitions and interpretations of the meaning of the EHR. The basis of a good EHR is the quality of information it collects Health care providers can improve the quality, accuracy and availability of information, increasing the speed of processing claims, and thus improving productivity. Personal health records (PHRs) contain the same types of information as EHRs—diagnoses, medications, immunizations, family medical histories, and provider contact information—but are designed to be set up, accessed, and managed by patients.
Relevance	The EHR/PHR can provide instant access to information such as medication history, clinical picture over time and decision support, such as allergy alerts, and more. It can also be a registry of allocated repositories of analytical medical information securely stored at the point of care, within the existing information systems used there for care delivery and data storage.
Domains	• Medication • Laboratory • Radiology • Patient Summary • Referral and Discharge reporting • Telemonitoring • Multidisciplinary consultation
Scale	National/regional
Information	• Diagnoses, medications, immunizations, family medical histories, and provider contact information Patient Summary • Patient consent • Discharge Letters • Links to other more analytical healthcare information (medical imaging, doctor reports, etc.)
Participants / stakeholders	• Healthcare professional (HCP) • Patient
Potential eHealth Assets	• EHealth data centre /data room • EHR Socket-based service (e.g., HL7 MLLP) • EHR Service (either socket or web service) deployed in a physically unsecure environment • Private Healthcare Information (PHI) database • eHealth portal • PKI infrastructure • Cloud based Clinical information system (CIS) • eHealth Web Service
Potential Risks	• Network security • Systems availability • Lack of standardisation • Lack of interoperability • Lack of security expertise • Access control and authentication • Data loss • Data integrity(data breaches, correct conversion from a paper-based filing system to electronic health records, incorrect data entry by staff, cut-and-paste data entry, inadequate updating) • Other

	○ Computer crashes resulting in data loss and access problems[58]
Security requirements	• Build service availability via component redundancy • Enhance administrative controls ○ Update policies and procedures ○ Guide employees through the stringent privacy and security training process ○ Run background checks on all employees • Monitor physical and system access ○ Create physically inaccessible systems to unauthorized individuals ○ Have exigencies in place for data recovery or restoration ○ Provide identification and verification requirements to all system users ○ Access the list of authorized users ○ Supply passwords and personal identification numbers (PINs) ○ Provide automatic software shutdown routines[59]
Criticality	EHR/PHR act as a supportive mechanism to point of care information systems. As such criticality is Medium to High. Most experts ranked this use case as very high
Additional Remarks and Challenges	This use case is one of the dominant use cases now implemented at regional or national level. Some examples have been further described in other sections of this document and further information are provided in the annexes (country briefs). It is important to note that this use case is highly moderated by interoperability standards and well established integration profiles such as the ones proposed by IHE. Some of those profiles have a strong security and resilience approach to secure data privacy, data availability and non-repudiation. In addition 27 of those profiles have been adopted as EU standard specifications under the 1025/2012 EU regulation.
Current Practices	Most EU member states have incorporated EHR and or PHR approaches in their eHealth strategy. Some examples (non - exhaustive) in this domain are: 1. the myKANTA pages and Patient data repository in Finland managed by KELA 2. the Dossier MédicalPartagé - DMP in France managed by ASIP Santé 3. the myDSP (dossier des soins partagé) from Luxembourg 4. the myHUG electronic health record of the Geneva University Hospitals

EHealth Services

TITLE	EHEALTH SERVICES (EPRESCRIPTION, PATIENT SUMMARY, REFERRALS, ETC.)
Purpose	Region/Nation-wide access to transactional patient health information for multiple purposes (patient summaries, electronic prescriptions, e-referrals, billing, etc.)
Relevance	Healthcare professionals need an accurate and actual overview of the patient's continuity of care record and specific administrative or medical procedures that are distributed in more than one point of care setting.
Domains	• Medication • Laboratory • Radiology • Patient Summary • Referral and Discharge reporting • Multidisciplinary consultation
Scale	National/regional
Information	• Medication Lists • Referral lists

[58] http://www.aaos.org/news/aaosnow/dec14/managing8.asp
[59] http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/E/Electronic-Health-Records-Security-and-Privacy-Concerns.aspx

	• Patient summary aggregates • Patient registries • Healthcare encounter reports
Participants / stakeholders	• Healthcare professional (HCP) • Pharmacist • Patient
Potential eHealth Assets	• eHealth data centre /data room • Web Service (e.g. for ePrescription, eDispensation, patient summary, patient cross-referencing) • EHR Socket-based service (e.g., HL7 MLLP) • EHR Service (either socket or web service) deployed in a physically unsecure environment • IHE XDS registries and repositories • Usage of unsecure communication channel in Hospital (e.g., unencrypted message exchange in Wi-Fi networks) • Private Healthcare Information (PHI) database • eHealth portal • PKI infrastructure • Cloud based Clinical information system (CIS) • eHealth Web Service
Potential Risks	• Network security(secure access to databases online)[60] • Cross border incidents • Systems availability • Lack of compliance and trust • Lack of standardisation • Lack of interoperability • Lack of security expertise • Access control and authentication • Data loss • Data Integrity(reliability of data acquisition)
Security Requirements	• Build service availability via component redundancy • All staff implementing a relevant project should be provided with clear written instructions on how to use the system appropriately in order to prevent security risks and breaches; • Suitable arrangements should be made for using prescription storage and archiving systems to protect the data against unauthorised access, theft and/or partial/total loss of storage media; • Data format standardisation • For data exchange, secure communication protocols and end-to-end security must be adopted; • Special attention must be paid to adopting a reliable and effective electronic identification system that provides the appropriate level of assurance (of both participating staff and patients) in compliance with eHealth Network decisions; • The system must be able to correctly record and track in an auditable way the individual operations that make up the overall data processing; • Unauthorised data access and/or changes should be prevented when the back-up data is transferred and/or stored; • In emergency situations, any access should be logged and subject to audit.[61]
Criticality	High (lack of eServices operation may create discomfort to end users. Most of the time though those processes are transactional processes that mostly deal with additional value added services and administrative tasks (reimbursement, etc..) so those service are no prerequisite to delivery of care at the point of care. Most experts ranked this use case of very high criticality
Additional Remarks and challenges.	This use case is the most dominant one in all EU member states as they all have included the implementation of eHealth services in their strategy either at a national level or at a regional level. As a consequence, this is a use case requires further attention and support by providing guidelines and recommendations on handling network security issues.

[60] http://homes.esat.kuleuven.be/~decockd/slides/20130601.privacy.and.security.concerns.ehealth.pdf
[61] GUIDELINES ON ePRESCRIPTIONS DATASET FOR ELECTRONIC EXCHANGE UNDERCROSS-BORDER DIRECTIVE 2011/24/EU

	EHealth services rely on establishing thorough connectivity and interoperability at all levels to secure information handling and exchange from one healthcare facility to another. Most end users and experts currently use integration profiles techniques extensively, as the one proposed by IHE (between systems) and Continua Healthcare Alliance (between devices). The European Commission has already validated this path to provide quality interoperability services over network infrastructures and has accepted 27 IHE profiles as part of the accepted specifications procurement under regulation 1025/2012. Basic challenges here remain such as having adequate and trusted registries of information based on commonly accepted terminologies and techniques. Appropriate solutions have been tested and have been put in practice in many countries and regions such as Luxembourg, Greece, Italy, Portugal, Spain, France, Denmark, Finland, etc. In general eHealth critical infrastructures do not massively differ from normal eGovernment or other basic CIIs. Healthcare has additional requirements in data privacy and patient consent domain (legal regulations) that may disrupt the value chain of services in favour of security and not the end service. This in some cases means that some services are so securely established that end user experience is tampered. Further analysis should be proposed in assessing technologies, standards, and methodologies that would securely enhance end user experience.
Current Practices	Most EU member states have incorporated eHealth services approaches in their eHealth strategy. Some examples (non-exhaustive) in this domain are: 1. The MedCom messages – digital exchange of health data network in Denmark 2. The Sundhed.dk – the official web portal of the public health services in Denmark 3. The ePrescrition system in Sweden managed by Swedish Health Agency 4. The ePrescrition system in Greece managed by IDIKA SA 5. The National Healthcare Information system managed by the Croatian Health Insurance Fund

5. Recommendations

5.1 Recommendations

Based on the information presented in this study and given the status of eHealth security in the MS, we conclude by providing the following recommendations for further work in this area.

Recommendation 1: Member States should conduct an asset identification and a risk assessment activity to classify their critical eHealth infrastructures and services and develop a national catalogue.

Identification of critical eHealth infrastructures and assets is a process to evaluate several eHealth services (use cases) and supporting infrastructures, as well as to determine which ones are critical. Definition of several Criticality levels may also be an option. ENISA's 2014 report on CII identification, having taken stock of practices followed in EU, provides alternative methods towards reaching this goal. [62]

It is critical to achieve a uniform and adequate security level throughout critical eHealth infrastructures. The determination of such infrastructures and assets at a national level shall enable the systematic protection of the latter, based on national rules to be followed uniformly. Moreover this approach may lead to the concentration of protection efforts to the most critical eHealth infrastructures, based on a prioritisation scheme.

Defining what is critical can be a complex issue and the result may be disputable, given interdependencies between services and infrastructures. MS may start with a simple approach in the identification of critical eHealth infrastructures and follow an evolution process towards higher maturity. ENISA has made a good first step in this report and listed some of the assets that should be considered critical.

Recommendation 2: **Member States should introduce clear cyber security guidelines for the protection of their critical eHealth infrastructures and services.**

Define the minimum requirements for the protection of eHealth infrastructures and assets classified as critical and include them in clear cyber security guidelines. Such guidelines may refer to specific use cases and technical infrastructures and assets commonly deployed, in terms of their protection measures. Combined with the previous recommendation, these guidelines could form the basis for the development of a standard protection level for the critical eHealth Infrastructures and identified relevant assets.

Guidelines may not be observed due to budgetary limitations, lack of management commitment to eHealth security as well as limited training & skills. However clear incentives can help bypassing these obstacles.

Recommendation 3: Member States and healthcare organisations should perform an impact/cost benefit analysis of healthcare cyber security incidents and to use this as leverage for increasing investment on eHealth systems and infrastructures security.

Senior management echelons need to be motivated to increase budget for investing on cyber security and assets protection. The best way to explain this is to present the cost benefit analysis of the security incidents classified by root causes, to indicate how big the loss is. The healthcare organisations should provide statistical analysis based on actual facts, incidents that have caused also financial impact to the organisation, to convince higher management that security should be considered a priority regardless of the national legal framework.

[62] ENISA, Methodologies for the identification of Critical Information Infrastructure assets and services, Dec. 2014

Recommendation 4: Member States should develop incident response mechanisms to efficiently bring together the healthcare organisations with the national cyber security competent centres.

An eHealth incident reporting mechanism, potentially part of a clinical incident reporting and alerting system, may improve patient safety. Moreover, by effectively sharing such information at various levels nationally, organisationally and clinically, collaborative efforts can be made to improve critical eHealth infrastructure protection and patient safety. In practice, an eHealth focused Computer Emergency Response Team should be created, which could potentially collaborate with the national CERT on incident handling. Feedback directly to the eHealth service users (e.g. clinicians) is extremely important for their continued engagement. A culture that encourages reporting and information sharing is needed.

In terms of eHealth incident handling and hazard control, further steps need to be taken:

- Systems for reporting and analysing incidents both locally and nationally,
- A good in-depth analysis process to establish root causes for selected individual incidents and aggregate incident reviews, thus enabling learning,
- A process to ensure that actions are implemented and corresponding improvements in eHealth safety can be demonstrated,
- Redefinition of compensation systems (punitive or non-punitive) and their impact on the patient safety culture and achievements.

Recommendation 5: Member States and healthcare organisations should setup an information sharing mechanism to start exchanging knowledge and lessons learnt on cyber security issues i.e. how they mitigate incidents, which are the security measures they take etc.

Information sharing is a very important component when building frameworks at a national level. Bringing stakeholders from the private and public sector, the users, the general practitioners, associations of pharmacists etc. would result in better depicting the current situation in the country, the gaps, the needs and thus developing concrete security requirements for the security and resilience of eHealth systems and services.

Recommendation 6: European Commission should encourage the development of baseline security measures for eHealth critical infrastructures and services. This should be done in coordination with the competent centres and the healthcare organisations operating the critical infrastructures.

To offer assistance to the healthcare practitioners and bodies, baseline security measures could be set by competent European authorities (national regulators, national security agencies etc.). Depending on the existing frameworks, these could be binding and mandatory through ad hoc legislation (thus requiring monitoring and auditing mechanisms to be in place) or through non-mandatory guidelines. Depending also on the maturity levels the security measures should be able to cover all different levels of sophistication in the systems.

Recommendation 7: Member States need to implement widely accepted security standards to achieve interoperability.

Define a set of must have integration profiles to establish secure connections over the network, specifically in the domains of audit logs, data encryption, TSL assertions, access rights policy, eID, healthcare providers' registries, and many more related to data integrity and resilience of systems.

Having a common guideline on the way to ensure correct interoperability will gradually increase end user experience and acceptance of new type of services that are meant to run over open networks and not in closed and restricted networks.

Recommendation 8: Member States should invest in raising awareness of the citizens and healthcare organisations in providing cyber security training to personnel and users.

One of the greatest gaps identified in this study is the lack of expertise and knowledge on cyber security, with consequent risks for the people involved in healthcare. Officers working in the competent authorities and the healthcare units (hospitals, clinics etc.) should understand the concepts of cyber security risks to be able to protect the critical assets.

Recommendation 9: Member States policy makers should make sure that eHealth should align with the national CIIP strategy and with the National Cyber Security Strategy (NCSS).

The NCSS is the policy document that describes the activities the country should take to enhance cyber security at a national level in the public, private sector and citizens. One of the most important objectives of the NCSS is Critical Information Infrastructures Protection (included in 90% of the existing EU NCSS[63]). As healthcare is considered a critical information infrastructure, any ehealth strategy should be aligned with the national policy documents and activities. This applies to all MS the ones that have already a strategy and the ones in process of creating one, including this way ehealth systems security and protection in the national priorities.

5.2 Future work

In more detail, the study identified also several areas where future work needs to be done:

1. Guidelines need to be created concerning CIIP in eHealth since many countries do not have a specific policy in the domain.
2. Further analysis on the factors which govern the criticality of eHealth services and infrastructures (e.g. the nature of interdependencies). Goal is to produce a guideline on methods to apply in order to formally identify critical eHealth infrastructures.
3. Further drill down on specific eHealth use cases of interest (review the technology and architecture used, the specific threat and risk mitigation measures to be taken). More specifically to thoroughly study the Cloud implementation in healthcare, presenting the related challenges and opportunities.
4. As eHealth is a prominent sector for automation and it can be supported by Smart solutions, a specific analysis on the Smart Hospitals pilots from the cyber security perspective should be considered.

[63] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

6. Appendix - Glossary of Terms and Acronyms

6.1 Acronyms

ACRONYM	DESCRIPTION
ASIP Santé	Agence des Systèmes d'Information Partagées de Santé
CCR	Continuity of care record
CDA	HL7 Clinical Document Architecture Standard (i.e. CDA R2, Level3, etc.)
CDR	Clinical Data Repository
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CPR	Computer based patient record
DMP	Dossier Médical Personnel /Partagé
eEIF	eHealth European Interoperability Framework
EHR	Electronic Healthcare Record
EHR QTN	Thematic Network on Quality of Electronic Health record systems
eID	Electronic Identification
eIDAS	Electronic identification and trust services
ePHR	Electronic Personal Health Record
EPR	Electronic Patient Record
epSOS	European Patient Smart Open Services – EU project
HIS	Hospital Information System
HITCH	Healthcare Interoperability Testing and Conformance Harmonisation
HL7	Health Level Seven
ICT	Information and Communication Technologies
IDA	Interchange of Data between Administrations

IHE	Integrating the Healthcare Enterprise
IHE ATNA	IHE Profile – Audit Trail and Notification Node
IPSec	Internet Protocol Security
IS	Information System
ISA	Interoperability Solutions for European Public Administrations
ISO	International Standards Organisation
ISO/IEC	International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC)
IT	Information Technology
LIS	Laboratory Information System
MOH	Ministry of Health
MPR	Medical Patient Record
NCP	National Contact Point
NeHIF	National eHealth Interoperability Framework
NHS	National Healthcare System
openNCP	Open source Reference Implementation of the epSOS project for an NCP
PAT	Project Athon
PHC	Primary Health Care
PHR	Personal health care record
PHR-S FM	Personal Health Record System Functional Model
PKI	Public Key Infrastructure
POC	Point of Care
PS	Patient Summary
RIS	Radiology Information System
SOAP	Simple Object Access protocol
TLS	Transport Layer Security

UC	Use Case
VPN	Virtual Private Network
WHO	World Health Organisation
WS	Web Service
WSDL	Web Service Definition Language
XAML	Extensible Application Mark-up Language
EHR-S FM	Electronic Health Record System Functional Model

6.2 Glossary of basic terms

TERM	MEANING
Cross-border healthcare	means healthcare provided or prescribed in a Member State other than the Member State of affiliation
Clinical data management system	Is a tool used in clinical research to manage the data of a clinical trial. This exists in research institutes, laboratories or university hospitals and not only.
Clinical data repository	is a real time database that consolidates data from a variety of clinical sources to present a unified view of a single patient.
eHealth Interoperability	is a characteristic of an ICT enabled system or service in the healthcare domain that allows its user to exchange, understand and act on citizens/patients and other health-related information and knowledge in a commonly interpreted way. In other words, it is a means of crossing linguistic, cultural, professional, jurisdictional and geographical border in eHealth.
e-Services in healthcare	are all electronic services together comprise integrated ICT supported health services to citizens. Examples of such services are electronic identification, authentication and authorisation services, telemonitoring, access to electronic health records, ePrescribing, e-dispensation and e-reimbursement.
Healthcare	means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices
Interoperability	The ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems. It is also the capability to communicate, execute programs, or transfer data

	among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units (ISO/IEC 2382-01).
Laboratory	is a place equipped for making tests or doing experimental work. A clinical laboratory is specialised laboratory for examination of materials derived from the human body (such as fluids, tissues, or cells) for the purpose of providing information on diagnosis, prognosis, prevention, or treatment of disease. Usually clinical laboratories are equipped with a Laboratory Information Management System (LIMS), sometimes referred to as a Laboratory Information System (LIS) or Laboratory Management System (LMS). It is a software-based laboratory and information management system with features that support a modern laboratory's operations. Key features include — but are not limited to — workflow and data tracking support, flexible architecture, and data exchange interfaces, which fully "support its use in regulated environments.
Prescription	means a prescription for a medicinal product or for a medical device issued by a member of a regulated health profession within the meaning of Article 3(1) (a) of Directive 2005/36/EC who is legally entitled to do so in the Member State in which the prescription is issued.
Radiology	is the science of radioactive substances and high-energy radiations and a branch of medicine that deals with diagnostic images of anatomic structures made through the use of electromagnetic radiation or sound waves and that treats disease through the use of radioactive compounds. Radiological imaging techniques include x-rays, CT scans, PET scans, MRIs, and ultra-sonograms. Radiology departments in healthcare institutions operate radiology information systems (RIS). An RIS is a computerized database used by radiology departments to store, manipulate, and distribute patient radiological data and imagery. The system generally consists of patient tracking and scheduling, result reporting and image tracking capabilities. RIS complements HIS (Hospital Information Systems), and is critical to efficient workflow to radiology practices.
Telemonitoring	is defined as the use of information technology to monitor patients at a distance. It is the ongoing assessment of a condition—in particular cardiac arrhythmias and/or other objectively measurable indicators of disease (e.g., heart failure)—by sensors attached to the patient, signals from which are ported wirelessly to a central station or “node” where abnormalities will trigger a response by healthcare workers.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
VassilikaVouton, 700 13, Heraklion, Greece

Athens Office

1 Vass.Sofias&Meg.Alexandrou
Marousi 151 24, Athens, Greece

Catalogue Number TP-04-15-824-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-137-3
doi:10.2824/217830