Security and Resilience in eHealth

Annex A: Countries' Report

DECEMBER 2015

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

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and 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.

Current status of security in eHealth information systems in the Member States

A.1 Austria

Healthcare Governance Model

Principle laws are in the responsibility of the Federal Ministry of Health which is the supervisory authority on national issues; the implementation of the legal provisions in the healthcare system is in the responsibility of the federal provinces (nine Länder) following a decentralized model. The Federal ministry is supported by subordinated authorities such as the Federal Office for Safety in the Healthcare system.

National eHealth Strategy and Legislation

The Austrian policy paper for eHealth "An information and communication strategy for a modern Austrian Health Care" was developed in 2006 and focuses on the following issues:

- Portability and interoperability aspects, such as standardisation;
- specific eHealth applications, e.g. telemedicine and eCards;
- legal aspects regarding data protection and patient access.[1]

Furthermore, there are two main laws that apply to eHealth-related issues: (a) the Health Telematics Act (2012) and (b) the Electronic Health Record File Act (2012). The eGovernment legislation also applies to

EHealth Services and Infrastructures

The central element of the Austrian eHealth model is the so called ELGA, the electronic health record (EHR) but also the body that coordinates the project of EHR in Austria**.** ELGA is based on a federated architecture (each federal province is in charge of managing the ELGA and also report to the Ministry of Health) wherein no patient data is stored outside of the host infrastructures (hospital, physician practice etc.) located in the country. ELGA allows Austrian healthcare professionals to share information relevant to a patient's healthcare treatment over a secure network, and thus makes their work simpler.

Austria has a national health ID card that is issued to all citizens. This smart card is the "patient identifier" addressing master patient indexing (MPI). All information is backed up locally to regional MPIs thus information exchange is accomplished. Patient information is queried via a physician portal. ELGA is connected with the national health ID, but is not creating a complete patient record. Instead, ELGA can query and present discharge summaries, radiology reports, lab reports and medications.[2]

Network infrastructures are based on the Healix: the e-Health Interexchange. Healix is a specific communication network for eHealth professionals and bodies. Strong regulation applies and only healthcare providers can use it after proving compliance against national regulation (requirements like existence of a business continuity plan, focus on ISO 27000 series compliance, yearly reviews, CIP Act regulation, etc.) both private and public healthcare providers can participate. Healthcare systems' interoperability is based on achieving and be compliant to specific IHE profiles proposed by ELGA as the central eHealth agency in Austria. There is also another network architecture layer called GOVIX for governmental bodies only.

[1] European Commission, DG Information Society and Media (2010), Austria Country Brief eHealth Strategies.
[2] https://www.chilmarkresearch.com/2015/01/27/a-sneak-peek-at-austrias-elga/

The Austrian eHealth model is based on classification of assets and on specific security requirements per class. For example the baseline is the eHealth framework requirements level where requirements like compliance to national laws, standards, access control based on roles etc. are included. In the second level, the one of the eHealth infrastructure requirements like archiving, pseudonymisation are included. One step further the eHealth applications are described leaving in the most important level the electronic health records.

Security Requirements related to eHealth Services

In Austria healthcare is considered a critical sector which means that national law applies to the critical systems. Security measures are mandatory by law and linked to civil protection guidelines. Given that ELGA is based on a federated architecture, no patient medical data is centrally stored anywhere. While this eliminates the ability to perform any type of analytics, it provides an added level of security that hybrid and centralized architectures cannot match.

In terms of data privacy, ELGA is an opt-out system wherein a patient has to formally request that their records not be available through ELGA. Access to ELGA and a patient's record is strictly limited to the attending physician and the patient. Physician uses the patient's smart card and must have justifiable need to gain access to data. Other physicians, government agencies, payers (they are part of government), employers, etc. do not have access to patient's data.

A.2 Belgium

Healthcare Governance Model

Since 1980, part of the responsibility for healthcare policy in Belgium has been devolved from the federal Government to the regional governments, with the Federal Ministry of Health to be the responsible body. The federal authorities determine the general legislative framework for the health system by issuing laws and by determining the annual budget. They regulate and finance the compulsory health insurance; determine accreditation criteria; finance hospitals and so-called heavy medical care units, and register and control pharmaceuticals. The regional governmental structures (Flemish community, French community and Brussels) are responsible for health promotion and preventive healthcare; maternity and child health services; different aspects of elderly care; the implementation of hospital accreditation standards.[3]

National eHealth Strategy and Legislation

In December 2012, a group of stakeholders proposed an eHealth Action Plan, which was approved by the federal and regional ministers competent for healthcare policy in April 2013. The Plan sets out concrete objectives that the Belgian and regional governments as well as the different stakeholders intend to pursue between 2013 and 2018. The objectives are aimed at stimulating the electronic exchange of data from patient files in the areas of healthcare and health insurance. The plan is based on five pillars: develop data exchange between caregivers on a common architecture, achieve a greater engagement and better knowledge of eHealth by the patients, develop a terminology of reference, simplify and improve efficiency of administrative tasks and establish a flexible and transparent governance structure in which all authorities and relevant stakeholders will be involved.

[3] European Commission, DG Information Society and Media (2010), Belgium Country Brief eHealth Strategies

EHealth Services and Infrastructure

In August 2008 Belgium adopted the law on the creation and setup of the eHealth Platform[4] .The eHealth Platform is an interoperable technical platform for safe and reliable electronic information exchange, based on a service-oriented architecture, with common basic services, and using technical and semantic interoperability standards. The use of eHealth Platform is optional. The eHealth Platform gives special attention to information security and data protection:

- end-to-end encryption of exchanged personal health data
- very thorough preventive access control
- specific guidelines for health data exchange
- logging of electronic services performed (who, what, about whom, when –not exchanged personal health data)

A meta-database (a database of databases) interlinking all governmental services Crossroad Bank, is created by a private provider keeping information like social security number and linking them to social services information.

Security Requirements related to eHealth Services

Specific security requirements for the eHealth platform are obliged by law and concern access control, end to end encryption, exchange protocols, safety measures. Specific provisions are made to avoid central storage of personal healthcare data, safe electronic data exchange between all actors,

A.3 Bulgaria

Healthcare Governance Model

Bulgaria has a centralized governance model for the healthcare sector, with the Ministry of Health performing the state healthcare policy and implementing the National Healthcare Strategy. The structure of the MoH comprises of 28 regional centers for Healthcare, a National Information Centre and an Executive Agency of Pharmaceuticals. In 2013, the Center for eHealth and Innovation was setup based on the UniBIT University of Sofia.

National eHealth Strategy and Legislation

The National strategy for eHealth implementation was approved in March 2006. The main goal of the strategy is to transform the healthcare system so that it becomes convenient for citizens through implementation of ICT and to establish an information infrastructure for patient oriented healthcare services. Priority tasks are: the creation of central electronic health record to be accessed through the eHealth portal, the implementation of e-Cards, provision of on-line healthcare services and development of a modern ICT infrastructure and of Information Networks in the healthcare system. However the strategy lack implementation.

The legislative act adopted in 2014 talks about implementing the eHealth card, the electronic reporting by healthcare providers and maintaining electronic health records. In the eGovernance strategy a sectorial approach is described, including eHealth as a critical sector and take the obligation to create a specific strategy.

EHealth Services and Infrastructure

The need to create a sector specific strategy emerges in the eGovernment strategy of Bulgaria (2014-2020). In Bulgaria eHealth is considered a critical sector so the assets supporting the healthcare information system are also critical and security is an objective. The fundamental elements of information infrastructures are considered the

[4] https://www.eHealth.fgov.be

data centers, the communication channels, information systems, operating systems, interoperability of used resources etc.

Security Requirements related to eHealth Services

Security is a priority for all eGovernment services so security requirements like access control, authentication, network security, continuous monitoring, resilience etc. however these are not linked directly to eHealth systems and infrastructures.

A.4 Croatia

Healthcare Governance Model

The healthcare system in Croatia is controlled centrally. The state owns hospitals and the regional authorities are in charge of the medical centres. The Ministry of Health has the overview. It is responsible for legislation, the annual national health plan, monitoring health status and health care needs, modifying standards in healthcare facilities, supervising training, hygiene inspections, setting the quality of food and drugs and raise citizens awareness. The ministry also holds the CIIP mandate for eHealth services.

National eHealth Strategy and Legislation

Croatian National Health Development Strategy for the period 2012-2020[5] is published. Among the declared ultimate purposes of informatisation of the healthcare in Croatia is to achieve full availability of the healthcare services to patients through quick and secure access to their own health record, as well as to information on health services. A specific legal framework for eHealth is also out since 2014, the Strategic Plan for eHealth Development[6].

According to the decision on the determination of the critical sectors, eHealth spans over several services ranked by criticality: communication and information technology (electronic communication, data transmission, and information systems), health (3 levels of criticality based on the activity), finance (insurance and payment systems), public sector (emergency medical services).

EHealth Services and Infrastructure

While the legal/regulatory framework for CIIs already exists in Croatia, the identification of critical assets is still underway. However the following information systems are key to ICT infrastructures for Croatia eHealth:

- The CEZIH (Central Healthcare Information System of Republic of Croatia) is the main eHealth infrastructure in Croatia. The services and systems covered are Electronic Health Records, e-Prescription, e-Referral and Patient portal. The system is owned by the Croatia Ministry of eHealth, which has authorised the Croatian Health Insurance Fund to be the eHealth platform operator.
- The Croatian Certification Authority that issues the eHealth Cards. Each healthcare professional has a smart card providing his ID data and certification. The IDs are assigned by the Croatian National Institute of Public Health.
- eHealth Card for the insured citizens in Croatia, assigned by the Croatian Institute for Health Insurance, with limited use for administration purposes.
- Health Insurance registry created by the Croatian Health Insurance Fund.

[5] http://www.zdravlje.hr/programi_i_projekti/nacionalne_strategije/nacionalna_strategija_zdravstva
[6] www.zdravlje.hr/content/download/15949/118543/version/2/file/Strate%C5%A1ki+plan+razvoja+eZdravlja.pdf

Security Requirements related to eHealth Services

Specific security requirements are set by the responsible authority of each system, for example for the Health Insurance registry/ information system the Croatian Health Insurance Fund has enforced a strict information security policy including rules and procedures for all employees and partners. There is a strict backup and restore procedure, encryption mechanisms, strong peripheral security etc.

A.5 Cyprus

Healthcare Governance Model

Primary healthcare is organised on a national level, supervised by the Ministry of Health. MoH has under its supervision all the eHealth projects. The Ministry is involved in the technical documents and tenders. The goal is to digitalize all the hospitals, to create an interoperability platform for e-folders of the patients. The Ministry is a public institution responsible for eHealth strategy in collaboration with the e-services sector.

The Cyber Security Authority is responsible for information security in the eHealth operators. DITS is the department of the government responsible for the security of all ministries. It has also established committee with internal audit and penetration tests.

National eHealth Strategy and Legislation

Cyprus lacks a specific strategy and / or policy regarding eHealth. eHealth issues are addressed in the overall "Digital Strategy of Cyprus"[7] policy document, whereas the regulation of eHealth issues (such as EHR and ePrescription) is based on general health and data protection law. The Ministry is also the main authority that is responsible for implementation of the strategy.

Cyprus has however a regulation on Critical Information Infrastructures protection and eHealth is considered a critical sector. The critical assets are the hardware and the software that can affect the availability of the system.

EHealth Services and Infrastructure

eHealth System, which will allow the electronic management of patient records in state hospitals, is expected to be implemented within two years[8]. However, similar systems are already in place in the private hospitals. eHealth services offered or in supervision:

- Hospital Information System (i.e. administration needs, management of operational aspects, etc.)
- Laboratory Information System (i.e. blood tests etc.)
- Radiology Information system (i.e. MRI, CAT scan etc.)
- Electronic Health Records (i.e. personal health information)
- Patients Health Record (i.e. information on patients)
- Telemonitoring/Telemetry
- ePrescription

Security Requirements related to eHealth Services

Specific security requirements are described in the "Digital Strategy of Cyprus" and apply to the eHealth infrastructures and systems which are:

[7] http://www.mcw.gov.cy/mcw/dec/digital_cyprus/ict.nsf/3700071379D1C658C2257A6F00376A80/$file/Digital%20Strategy%20for%20Cyprus-Executive%20summary.pdf
[8] http://in-cyprus.com/ministry-one-step-closer-to-e-health/

- Compliance with national regulation. Implementation of security measures obliged by law and the internal policy for both devices and systems
- Implementation of internal security policy for devices and systems, internal audits and security incidents reporting

Cyprus is about to implement private cloud solution hosted in the country to store eHealth data. Security requirements are based mostly on national regulations.

A.6 Czech Republic

Healthcare Governance Model

Healthcare is organised on a national level, coordinated by the Ministry of Health. Main actors involved are the Czech national eHealth center, the Regional Public Health Authorities, and the Regional Institutes of Public Health.

National eHealth Strategy and Legislation

The Czech Republic's current national eHealth strategy document was created in 2007 and was made public in 2008 by the Interdepartmental Committee for eHealth that is responsible for the coordination of eHealth projects. The areas specified in the document are:

- electronic documentation
- ePrescription
- eID for insures and healthcare professionals
- electronic payments
- national registries
- data interface
- classification systems of diseases
- health technology assessment
- systems of decision support
- standards
- clinical protocols
- electronic data exchange among (including foreign) health insurance companies
- internet portal for eHealth
- health information portal for citizens including data about quality of provided care.

The Czech national eHealth Center has launched a project in 2012 on telemedicine services

eHealth Services and Infrastructure

In the Czech Republic there is a law focusing on Critical Information Infrastructures protection. During the assets identification process, eHealth systems have been classified as critical. However no specific regulation on eHealth infrastructures protections exists.

There is an application in place for Electronic Health Record, which contains per patient: a history of all prescribed medicines; hospitalisation records and reports; vaccines; lab test results; administrative data: reimbursement, civil status, etc.

Security Requirements related to eHealth Services

The optimal goal of eHealth services in CZ is to enhance the availability of data in continuous mode online and provide a secure access to these data. To achieve this interoperability between all the systems and services of eHealth is required. Some security requirements set for these services are: security in general in the forms of authentication, access control, auditability for data and for transactions, back up and services continuity.

A.7 Denmark[9]

Healthcare Governance Model

The healthcare sector has three political and administrative levels: the state, the five regions and 98 municipalities. The regions are following a decentralized governance model; regions are responsible for hospitals and GPs, and municipalities are partially financing healthcare. Each year the regions and municipalities make an agreement with the ministry on the priorities to be followed. They make recommendations and guidelines on several eHealth aspects (not only security).

The task of the state in healthcare provision is to initiate, coordinate and advise on national health policy at a general level. The Ministry of Health, in its capacity of the principal health authority, is responsible for setting up the overall national health policies and legislation on healthcare.

The National eHealth Authority is the regulatory authority. Other roles the National eHealth Authority has is that they are responsible for standards, drafting the eHealth strategy and provide national service platforms for hospitals to use. The National eHealth authority drafts also specific guidelines for IT security for the region, GPs and hospitals, etc. but compliance is not mandatory.

The five regions in Denmark are the main service providers in the Danish health care system. Their responsibilities include all hospital and psychiatric treatment and parts of the primary health care system (general practitioners, private practicing specialists, dental services, physiotherapy). The municipalities are responsible for home nursing and homes for elderly people with care facilities and associated care staff, public and school health care, child dental treatment, general disease prevention and rehabilitation.

National eHealth Strategy and Legislation

- National Strategy for Digitalisation of the Danish Healthcare Service (2011-2014)[10]. A new national public health and eHealth strategy for 2015-2018 is currently under preparation by the Ministry of Health.
- 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 Services and Infrastructure

No critical assets assessment has taken place in national level. The National eHealth Authority has performed internally a risk assessment for the national systems they provide. Between these are the national service platform (The National service platform is a CI component and then there is a network that is connects all in the eHealth services), the network that interconnects all eHealth services like:

- Sundhed.dk (”health”.dk): the official Danish health website providing access to information for citizens, patients and health care professionals. The portal features on-line services for the general public, who can find general health information, book appointments with their GP and renew prescriptions, as well as gain access to their own medication data, for instance. For the healthcare professionals, sundhed.dk features include on-line services for access to laboratory test results and to data stored in electronic patient records.
- MedCom (a network that through a central db GPs and hospitals are connected and sharing info) and the common medicine systems for ePrescription and medicine handling (all activities are registered). In the last one hospitals, GPs and authorities (regional bodies and municipalities) have access. No mandate on CIIP, no

[9] Danish Ministry of Health (2012), “eHealth in Denmark”S
[10] http://www.ssi.dk/~/media/Indhold/DK%20-%20dansk/Sundhedsdata%20og%20it/NationalSundhedsIt/Strategi/Digitalisering%20med%20effekt.ashx

responsible authority in Denmark. There is also no regulated methodology for CIIs identification in national level, however each region has conducted an asset identification (and assessed based on criticality).

- "e-Journalen": digital access to electronic medical records at hospitals. It gives patients and health care professionals' digital access to information on diagnoses, treatments and notes from EHR systems in all public hospitals. 30–40% of the hospitals also provide access to information on medicine and sample results from laboratories. By the end of 2011, the system contained health data on more than 85% of the Danish population.
- Shared Medication Record ("Fælles Medicinkort"): a central database containing information on all Danish citizens' medicine dispensed during the previous two years as well as an updated list of every patient's current medication.
- Laboratory information system (used for very specific analysis done only there),
- ePrescription (common medicine chart for ePrescription).

Security Requirements related to eHealth Services

A unique personal identifier is issued to all Danish citizens at birth, and a software-based PKI digital signature is widely used, instead of the hardware-based chip card. To create this infrastructure the specific security requirements as documented are:

- Access Control (only the bodies that need the information will have access to the data –classification of data i.e. privileged users have been abusing their privileges.
- Business continuity and disaster recovery.
- Supplier chain security/third party security

A.8 Estonia

Healthcare Governance Model

The ministry of Social Affairs is responsible for the coordination of whole eHealth domain in Estonia and has created the eHealth Strategy (with the cooperation of MoH). The ministry is the accountable body responsible for any legal frameworks, and in charge of the development and setup of the whole eHealth system in a national level. Other bodies are created to implement the provisions of the strategy.

The Estonian eHealth Foundation is the body in charge of EHR in Estonia. The HIS (Health Information System) is the central database in EE (hosted and maintained by the eHealth Foundation) and it provides also software modules for patients and smaller health care service providers (patient's portal, doctor's portal, portal for expertise doctors). The authorized body from a technical level is the eHealth foundation, which is developing, hosting and maintaining the eHealth systems.

The Estonian Health Insurance Fund was registered in 2002 and is dealing with compulsory health insurance. The organization has under its supervision the implementation and the operation of ePrescription platform. The purpose of health insurance in Estonia is to cover the costs of health services provided to insured persons, prevent and cure diseases, finance the purchase of medicinal products and medicinal technical aids and provide the benefits for temporary incapacity for work and other benefits.

National eHealth Strategy and Legislation

The strategy is managed by the Ministry of Social Affairs. The Ministry is updating the strategy currently. All government bodies have to follow a specific security standard ISKE (Estonian Three-level IT baseline security system) (based on the BSI framework). This includes classification of assets and specific measures per asset class. This applies to the public healthcare providers.

Data protection law is higher level act/framework than ISKE but is mandatory for all medical data processors, also for private sector. Other laws that exist in Estonia and apply in eHeatlth:

- "The Law of coordinating health care services" establishes requirements for data exchange[11]
- Statute of Health information system[12]
- Also by law, State's databases have to exchange data over secure layer called x-road (authenticated end point systems, encrypted information)[13]

In sum, it can be stated that the general eHealth concept in Estonia is built around the idea that all information about patient health should be 1) available to patients and health professionals on request and 2) collected once and managed centrally, so that multiple and variable secondary uses are enabled. The patient has the right to decide how personal information should be handled by state authorities and health service providers.

eHealth Services and Infrastructure

Since 2005, the countrywide eHealth approach encompasses four pillars: Electronic Health Records (EHR), Digital Registrations, Digital Imaging and Digital Prescriptions.

The central eHealth project is EHR (Electronic Health Record), which is part of the Health Information Exchange platform. Its main goal is to enable the exchange of information between doctors by connecting IT systems for health services. The EHR gives doctors the possibility to see a defined selection of a patient's health information and provides time critical information to ambulance services.

Security Requirements related to eHealth Services[14]

The security arrangements adopt five principles:

1. Secure authentication of all users (users authentication via biometrics or knowledge based, device authentication). Estonia's ID card is an effective security device. Its primary task was the digital signature but the same mathematical method and device can be successfully used for each kind of secure authentication.
2. Maximum accountability and transparency, with all actions leaving an unchangeable and non - removable secure trail
3. Separating personal data from medical data, the so-called coding of personal data
4. Database encryption that minimises the confidentiality risk from the technical administrators
5. Effective monitoring for all actions and the corresponding counter-measures both organisational and technical.

Other Security requirements:

- Compliance with national regulation, laws and security standards
- Implementation of security measures, external auditors
- Certification against national or international standards
- Security incidents reporting to competent authorities and incident management
- Separation of duties
- Risk management, awareness raising and training, access control, network security, business continuity

[11] https://www.riigiteataja.ee/akt/115042014007#para59b1lg3
[12] https://www.riigiteataja.ee/akt/110052014031
[13] https://www.ria.ee/x-road/
[14] ProeHealth, Estonian EHR Case Study

A.9 Finland

Healthcare Governance Model

In March 2014, the Finnish government decided that the responsibility to organize healthcare will be the task of five special responsibility areas (ERVA) following a regional approach. The ministry of Social Affairs and Health is currently preparing a new strategy for information management in health and social care.

The Ministry of Health defines the data protection guidelines through legislation. Legislation includes provisions for certification of systems connected to the national KanTa services and defines the rules for information access. Finnish Cyber Security Authority (Finnish Communications Regulatory Authority) provides general cyber security guidelines, also applicable to eHealth. Population Register Centre is responsible for designing the certificate infrastructures and certification policies.

National eHealth Strategy and Legislation

- eHealth Roadmap for Finland (2007): The roadmap sets the country's strategic objectives on eHealth. These aim at secure access to information for those involved in healthcare regardless of time or place, together with increased citizen access to high quality health information. The focus of the strategy is the development of a national eArchive record repository and ePrsecribing service.
- eHealth and eSocial Strategy 2020 (2015)[15]. The objective of the strategy is to support the renewal of the social welfare and health care sector and the active role of citizens in maintaining their own well-being by improving information management and increasing the provision of online services.
- Regulation on the Use of Electronic Social and Healthcare Client and Patient Information (Client Data Act, 2007)**:** From 2011, the law requires all public healthcare units as well as private healthcare units that do not use paper-based archives, to be incorporated into the electronic archiving system. Article 11 of the Act specifies that a medical record should consist of at least a so called General Medical Record (GMR) and a patient consent record. One GMRshould be kept for every patient by the general practitioner in charge of the patient's treatment. The Act also states that the national eArchiving service for electronic patient records will be maintained by the Social Insurance Institution (Kela), using a unique number per patient. The archive will be accessible to all physicians who are involved in the provision of care to the patient, after obtaining consent. Individuals have access to their own patient records, are entitled to see the access log of their care record and to obtain a copy.
- Genome strategy [16]
- Act on the Use of Electronic Prescription (2007)

eHealth Services and Infrastructure[17]

The main eHealth Infrastructure of Finland is "KanTa - National Archive of Health Information". KanTa includes all the national information services for healthcare. The services provided include:

- ePrescription service
- National pharmaceutical database
- Patient data repository

[15] http://urn.fi/URN:ISBN:978-952-00-3575-4 (in English)

[16] http://stm.fi/en/article/-/asset_publisher/suomesta-voi-tulla-genomitiedon-hyodyntamisen-mallimaa

[17] Jarmo Reponen (2014), "eHealth status in Finland", Danish eHealth Observatory, 2nd Oct 2014, Nyborg, Denmark

- Portal for patient's own data
- Patient data management (patient consent management and patient summary management)[18]

For ePrescription and Patient data repository, there are internal documents for CIIP, internal to KELA, on how to protect systems and data certification requirements are public for access to central systems. Group A of information systems can access the central ehealth hub after certification[19]. Group B cannot access national services, but the system manufacturer must still make a self-declaration of compliance to guidelines. Compliance of Group A systems is checked by a third-party certification authority accredited to do so by the Finnish Communications Regulatory Authority.

ePrescription and Patient Data Repository can be seen as a public cloud service provided to citizens. Patient data are centrally inserted and accessed, third party devices are connected to the central services, so back bone is in the public cloud

Security Requirements related to eHealth Services

Security measures are mandatory by law. They ensure the security level with Compliance with national regulation, Implement security measures, certification against national or international standards, through service level agreements, internal audits and security incidents reporting. There should be a regulatory framework for cross border services, possibly but not necessarily the use of ISO standards. Some of the security requirements are mentioned above but the most important ones are access control, authentication, network security, compliance with national legislation etc. For example the Client Data Act from 2007, covers archive services, encryption and certification services as well as the patient's access to data. The Client Data Act provides the patient with a right to a medical record, carefully updated and safely stored by the health professional. Medical records need to be kept in electronic format.

A.10 France

Healthcare Governance Model

The Ministry of Health along with the ASIP Santé have the supervision and provide guidelines for security and protection in healthcare. French Ministry of Health and Social Affairs is responsible for the national health plan. In terms of healthcare provision, France is following a regional approach through the Regional Health Agencies (27 regions). Financial responsibilities are delegated to the health insurance/social security system.

ASIP Santé is a government agency under the supervision of the Ministry of Social Affairs and Health, which is responsible for the development of information systems in the healthcare sector. As such, ASIP Santé could be categorized primarily as an eHealth competence centre and partly as a public institution responsible for eHealth strategy and as a standardization body. ASIP Santé is one of the bodies helping define health information security policies for healthcare organisations. The regional health agencies are collaborating with ASIP Santé. The agency is responsible for issuing guidance for the healthcare actors on several topic like information security, authentication, access control[20] etc.

[18] http://2014.e-sundhedsobservatoriet.dk/sites/2014.e-sundhedsobservatoriet.dk/files/slides/Jarmo%20Reponen,%20E2%20slides.pdf
[19] http://www.kanta.fi/en/lainsaadanto
[20] http://esante.gouv.fr/pgssi-s/espace-publication

National eHealth Strategy and Legislation

"Projet de loi "Hôpital, Patients, Santé et Territoires" (2009): it sets the key conditions for the eHealth infrastructure and notably the further development of the French EHR project Dossier Medical Personnel (DMP) and the associated pharmaceutical care record.

The Ministry of Health sets the guidelines for the definition of eHealth strategy. However, there is no unified guidelines for all, but different smaller guidelines depending on the type of the organizations. In terms of security policy, there are three activities/issues to be mentioned:

Certification process[21] : Hospitals are audited by an independent organization (High Health Authority) every 2-3 years, in order to verify that their operation is safe enough. Network security is one of the issues that are checked during those audits; however, information system security is a rather new dimension and the audit questionnaire is rather 'light' in this aspect (in case the hospital is not certified it has to stop accepting patients).

Digital hospital[22] : This involves a questionnaire to be answered and be kept up to date, by the hospitals. Different maturity levels included. Depending on the extent to which hospitals comply with certain rules, there might be a financial incentive. Those rules include, among others, security-related issues such as authentication, business continuity plans, files storage and backup, non –repudiation, accreditation etc.

Global security policy[23] : This is a document about best practices in information systems security. Some parts of this document are expected to be incorporated in the related legislation in the next years as information system security in the health sector is very new for hospitals.

eHealth Services and Infrastructure

In France Healthcareis considered a critical information infrastructure. Most important infrastructures and services in France:

- Electronic health record (DMP): Launched in January 2011, the DMP is being gradually rolled out across the French territories through voluntary adoption by patients and healthcare professionals. It will form the infrastructural and technical base for numerous eHealth services, whether proposed by public authorities or private sector.
- Sesame Vitale eHealth card has improved the efficiency of the French social security system and significantly simplified administrative workflows.

Security Requirements related to eHealth Services

The ASIP Sante has issues recommendations to be used for healthcare professionals to protect their systems and services, like the guide to developing and implementing a security policy for their systems. Specific documents on network security, authorisation policy and access control, data security (policy on how to destroy data), certification of services, risk assessment etc. are already published.

A.11 Germany

Healthcare Governance Model

A fundamental characteristic of the German political system in general and the health care system in particular is the sharing of decision-making powers between the states and the federal government. Legislation takes place at the federal and the states level; implementation of legislation is mostly through the various bodies of health system

[21] http://www.has-sante.fr/portail/jcms/fc_1249882/fr/certification-des-etablissements-de-sante
[22] http://www.sante.gouv.fr/le-programme-hopital-numerique.html
[23] http://esante.gouv.fr/pgssi-s

self-administration (cooperation of social health insurance associations, statutory medical and dentists associations, pharmacy association, patient representatives) and, with respect to hospitals, at states level.

Gematik is the authority in charge of introducing, maintaining and developing the electronic health card and its infrastructure in Germany, to coordinate and to ensure interoperability with components. Germatik is founded under the umbrella of the German healthcare system. Gematik cooperates closely with BSI at the national level, in order to define the eHealth security aspects.

National eHealth Strategy and Legislation

- German eHealth Strategy (2005)
- eHealth initiative of the Federal Government (2010)
- "Planning study Interoperability" (2014) and establishment of "eHealth council" to promote interoperability of IT systems
- eHealth Act – 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. As healthcare in Germany is considered a critical sector, these measures will affect the healthcare bodies. BSI will be the coordinating authority of this implementation.

eHealth Services and Infrastructure

- eGK (National electronic eHealth card): As well as being used to reimburse health costs, eGK offers users access to their health records online, at a national level. It has been designed so that it can be used for several other optional eHealth services, some of which are still in development, and all of which will be subject to the patient's consent:
- E-prescriptions: patient cards will be able to transmit prescriptions electronically to pharmacies with the necessary equipment;
- Emergency medical data: allergies, intolerances, current treatment, organ donation information, and the details of the patient's doctor can all be registered directly on the card, so that they can be easily accessed in the case of an accident;
- Treatment history and any treatment currently underway;
- A messaging and document sharing service for doctors, for discharge letters, notes, X-rays with reports, and test results, following identification via the "Elektronischer Heilsberufsausweis", the German equivalent to France's healthcare professional card (CPS);
- Access to the patient's electronic medical record if it exists. Each regional government is responsible for rolling out these records.

Security Requirements related to eHealth Services

As described in the newly published IT Security law, the specific requirements that should apply to all ehealth systems and services:

- Designing and implementing specific security standards
- Identifying critical infrastructures
- Implementing incident reporting
- Conduct mandatory auditing and reporting
- Collaboration and information sharing with operators

A.12 Greece

Healthcare Governance Model

In Greece, the Ministry of Health MoH Ministry of Health has the overall responsibility for eHealth. IDIKA is the competent centre under the Ministry of Labour and implements the ePrescription services but has extended to other eHealth priorities.

National eHealth Strategy and Legislation

- eHealth Roadmap (2006)
- 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 and 4328/2014 Network of Primary care
    - Obligation to submit prescription and dispense medications electronically; duties of doctors and pharmacists; access rights including for Patient access to own information;
    - Obligation to provide citizens with electronic medical records; obligatory inclusion of a minimum PS data set; doctors are responsible for the creation and maintenance of eHRs; access rights including for Patient access to own information

eHealth Services and Infrastructure

In Greece there has been no identification of national critical information infrastructures, so ehealth systems are not defined as critical per se. However services and infrastructures exist that could affect the social well fare of the community if an outage occurs, and these are:

- ePrescription system
- Hospital Information System
- Laboratory Information System
- Telemedicine: one pilot in behavioural mental health. Most telemedicine in Aegean and Crete.

Security Requirements related to eHealth Services

No specific security requirements for eHealth systems are identified.

However there are some common obligations that we meet when procuring ehealth services, such as: SLAs for the contractors (IT providers/integrators), obligation to report security incidents etc. But again these are not obligatory and not set by the government.

A.13 Hungary

Healthcare Governance Model

The overall responsibility for state social welfare and healthcare provisions are assigned to the national level while the responsibility for local health services is assigned to local governments.

National eHealth Strategy and Legislation

There is no eHealth strategy in Hungary. 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 (2006).

eHealth Services and Infrastructure

ACT CLXVI of 2012 on the assignment and the protection of the critical infrastructures of Hungary and the subsequent decrees for the transport, energy, agriculture and law enforcement sector define the process of identification of CII. The method has only been applied in the aforementioned sectors.

Security Requirements related to eHealth Services

No relevant information has been identified.

A.14 Ireland

Healthcare Governance Model

The primary responsibility for primary care policy lies with the Health Services Executive for operational matters.

The Department of Health is responsible for the overall policy. However, HIQA - The Health Information and Quality Authority – is strongly involved as the independent authority that drives continuous improvement in Ireland's health and social care services. The Authority has various activities: Regulations, setting of standards, provision of guidance, assessing health technologies and promoting the efficient and secure collection, use and sharing of health information.

Department of Health and Health Service Executive are responsible overall for the hospital information systems, the laboratory information systems and the radiology information systems. At the national level, there is only PACS; all other systems are provided by more than one supplier. However, it is expected that a national laboratory system will be in place in a timeframe of 4-5 years.

National eHealth Strategy and Legislation

- "eHealth Strategy for Ireland" was published in December 2013. The detailed implementation plan thereof is expected to be published within 2015. One of the things foreseen in the eHealth strategy is the establishment of an independent dedicated entity called eHealth Ireland.
- The legislation for a "national health identifier number for citizens, professionals and organisations" was published with the strategy.

eHealth Services and Infrastructure

There is no separate authority that has a mandate on eHealth CCIP. However, it could be said that the Department of Health has the overall responsibility although this is not legally defined. Even though there is no CCIP strategy in place, one could say that the most critical eHealth assets are those that have a direct impact on the patient's care such as diagnostic systems and ICU and then the systems that aggregate information related to patient's care.

Security Requirements related to eHealth Services

The following security objectives were mentioned as priorities: (a) physical and environmental security; (b) access control in terms of data protection and application security; and (c) business continuity and disaster recovery. To what concerns incident management, there are regional incident helpdesks and the incidents are usually managed by the vendors. However, the establishment of a single virtual helpdesk is planned.

A.15 Italy

Healthcare Governance Model

In Italy, healthcare is the responsibility of the regions, the policy is decided on the national level and implemented on the regional. In 2010 there were 146 Aziende Sanitarie Locali (ASL) (local health centers) and 178 Aziende Ospedaliere (AO) (hospitals) (Ministry of Health 2011). The Ministry of Health sets national directives and guidelines

on eHealth for ASLs to implement new ways of organizing and providing services, rationalize investment and create synergy within a single institutional-strategic eHealth framework.

National eHealth Strategy and Legislation

- The National eHealth Information Strategy was published in November 2011. The following were defined as priority areas: (a) health services booking system, (b) eHealth Record, (c) telemedicine, (d) e-prescription, and (e) e-Certificates.
- Act 221/2012 defined the main principles on EHR.

eHealth Services and Infrastructure

NSIS: New Health Information System: a health information network, making standardised information available to regional actors throughout Italy. It includes data on healthcare service interactions by citizens as well as financial data on healthcare facilities. Within the framework of European epSOS project, focuses on patient summaries and e Prescription (IPSe).

There are also regional systems that are operating independently like the implementation currently in use in Lombardia, composed of a patient eID implementation, an EHR back-end and a complex health data network interlinking healthcare providers throughout Lombardia.

Security Requirements related to eHealth Services

The Italian National Agency for Digital Administration (CNIPA) issues technical frameworks such as guidelines and recommendations for the implementation and management of administrative information systems and security, interoperability and service delivery.

A.16 Latvia

Healthcare Governance Model

The Ministry of Health is the leading governmental institution in the health sector in Latvia.

National eHealth Strategy and Legislation

An eHealth strategy was developed in 2005 (Government of Latvia, 2005). The Latvian NHS is responsible for implementation of the strategy and the establishment of the necessary infrastructure.

On April 2014, the Government of Latvia approved the Regulation No 134 On a unified health information system (Government of Latvia, 2014). According to the regulation, the eHealth system shall be fully operational by 2016. This is an ambitious target because the system will include e-receipts, eHealth records, e-bookings, e-referrals and an e-portal, which will provide general information to the public and which will have a restricted area accessible only by patients and medical doctors, summarizing all relevant information (eHealth records, e-receipts etc.). [24]

eHealth Services and Infrastructure

The Latvian approach to CI doesn't rely on specific critical sectors; rather, any infrastructure found to meet the criteria of criticality can be designated as critical. This designation must then be approved by the government

[24] http://www.hspm.org/countries/latvia08052014/livinghit.aspx?Section=4.1%20Physical%20resources&Type=Section#1Theimplementationofe-healthisadvancingdespiteopposition

cabinet before infrastructure becomes critical infrastructure. However no significant eHealth services and infrastructure are defined as critical.

Security Requirements related to eHealth Services

The National Security Law includes a specific act on cyber security, the law on Security of Information Technologies, which the framework to set specific security measures to be implemented for the infrastructures and the services designated as critical. Direct legal responsibility for the security and functioning of CII lies with the owner, and he is required to define security measures based on the identified risks, to document these measures, present them to the Constitution Bureau and get validation.

A.17 Lithuania

Healthcare Governance Model

The Ministry of Health is responsible for general supervision of the entire healthcare system. It is strongly involved in drafting legal acts and issuing the consequent regulation for the sector and also develops the public healthcare infrastructure. National Patient Fund at the Ministry of Health and five Territorial Patient Funds provide services to all 10 counties of Lithuania.

National eHealth Strategy and Legislation

- "eHealth Strategy for 2007- 2015" with the objectives to keep the balance in currently implemented and newly developed IT and communication solutions, to promote eHealth development, ensuring effectiveness, quality and accessibility, to create an effective eHealth system able to provide information for comprehensive administration and clinical decision-making.
- E-health System Development Program for 2009 – 2015.

eHealth Services and Infrastructure

The Law on Cyber Security (which entered into force on 1 January 2015) introduces the definition of critical information infrastructure (CII) in national level. In addition to setting of organization, management and control of the national cyber security system. In Lithuania eHealth is a critical sector.

Security Requirements related to eHealth Services

The security requirements are set by the CII owners and they are responsible for cyber security of their critical infrastructures and implementation of the measures. However some specific measures are described in the law: incident reporting and incident management, business continuity plans, indicate contact points for cyber security cases, information sharing.

A.18 Luxembourg

Healthcare Governance Model

The Ministry of Health and the Ministry of Social Security are co-responsible for primary healthcare. Agence eSante is the national agency for information sharing in the health sector, created in 2010 by the reform of the Luxembourgish healthcare sector.

The eHealth Agency is an Economic Interest Group (EIG) which includes the following members: (i) State jointly represented by the Ministries of Health and Social Security, (ii) the National Health Fund (Caisse Nationale de Santé - CNS) (iii) the Public Centre for Social Security (Centre Commun de la Sécurité Sociale - CCSS) (iv) the Association of Doctors and Dentists Doctors (Association des Médecins et Médecins Dentistes - AMMD) (v) the Luxembourg Federation of Hospitals (Fédération des Hôpitaux Luxembourgeois - FHL) (vi) the Union of Pharmacists (Syndicat des

pharmaciens) (vii) the Luxembourg Federation of Medical Analysis Laboratories (Fédération Luxembourgeoise des Laboratoires d'Analyses Médicales - FLLAM) (viii) the Confederation of Organizations and Providers of Aids Care (Confédération des Organismes Prestataires d'Aides et de Soins - COPAS) (ix) the Patientevertriedung. The hospital is obliged to apply a governance policy which follows a decentralized policy.

National eHealth Strategy and Legislation

- Law 2010 on the reform of healthcare systems.
- Luxembourg has a detailed eHealth Action Plan since 2006. (Plan d' action eSante, dated July 5th 2006).
- Luxembourg's national eHealth agency is operational since September 2012 and its main missions defined by law are the development and implementation of:
    - A national eHealth services platform for the exchange and sharing of medical data
    - A national strategy to promote and enhance interoperability between healthcare information management systems

The eHealth strategy includes the establishment of a platform for sharing and exchange of data in the health field and a national strategy for interoperability of health information systems, which will allow different health systems to interact smoothly. Its members are highly experienced in eHealth Strategy and Regulation, CIIP, Cyber Security Policy and NIS implementation in eHealth. The legal framework was defined in the Act of 17 December 2010 on the reform of health care but doesn't cover all of the infrastructures. It is planned to implement a medical data repository.

eHealth Services and Infrastructure

- eHealth services Platform
- DSP- Dossier de Soins Partagé

Security Requirements related to eHealth Services

No specific security requirements set by law.

A.19 Malta

Healthcare Governance Model

The Ministry for Health, the Elderly and Community Care is responsible for primary healthcare in Malta.

National eHealth Strategy and Legislation

The main national document addressing eHealth is the National Information Communication and Technology (ICT) Strategy for Malta of 2008. Health data exchange is regulated by the Data Protection Acti and the Professional Secrecy Act. There is no specific national "ehealth legislation" yet.

eHealth Services and Infrastructure

- Electronic Case Summary system: in house system for electronic discharge letters.
- National Patient Summary system: automatic aggregation of data from online registries and from electronic case summary.

Security Requirements related to eHealth Services

No specific security requirements set by law.

A.20 Netherlands

Healthcare Governance Model

The Netherlands is a decentralised unit state. Policy making happens at national, regional (12 provinces) and local (around 500 municipalities) level. Policy implementation is decentralised to the lower levels, unless it can be done more efficiently at the national level. Regarding the healthcare sector, the Ministry of Health, Welfare and Sports (VWS) is responsible for legislation, policies and budgets, whereas the Ministry and local authorities are jointly responsible for primary healthcare.

The Agency on standardisation and eHealth (NICTIZ) was founded in 2002. 2. NICTIZ sets the legal framework for the exchange of patient information and for communication between GPs and other health providers (in terms of the national infrastructure, electronic messages, and safety). It also coordinates the implementation of health IT projects and provides a level of national support, including training, a helpdesk, and maintenance of Web-patient portals. They provide the AORTA system which is used for exchange of information. Efforts on the creation of the national electronic health care record have taken place but the project is still in infancy.

There are mainly two supervisory authorities responsible for EHRs: The Dutch DPA and the Dutch Healthcare Inspectorate.

National eHealth Strategy and Legislation

Netherlands has no dedicated eHealth Strategy document. Regarding legislation the main documents are the following:

- Medical Treatment Contract Act
- Code of Conduct for Electronic Data Exchange in Health care: self-regulation by several umbrella healthcare organisations. It applies to information systems that are used for exchanging personal data between healthcare providers. I lays down requirements with regard to 1. Rights of the data subject, 2. Informed consent, 3. Authorisation of healthcare providers and patients with regard to health data and 4. Information security and logging. This code is not legally binding. However the supervisory authorities refer to this document when executing supervisory responsibilities.
- Proposal on patient's rights with regard to electronic data processing (2013)
- General Administrative regulation with regard to the electronic exchange of data between healthcare providers. This is supplementary to the aforementioned and focuses in compliance.

eHealth Services and Infrastructure

- AORTA is the national standardized infrastructure for exchanging and consulting medical records. The responsibility lies in the NICTIZ and the association for care providers and care communication. This platform facilitates exchange of medical data and it makes it possible for the patient to consult their medical records. The law requires the de-centralised storage of medical records and this is dealt in the National Healthcare Information hub.
- In Netherlands there is e-prescription system (EVS).
- eConsultation

Security Requirements related to eHealth Services

There is no specific legislation with respect to the requirements on institutions hosting EHR data. However national legislation provisions apply.

A.21 Poland

Healthcare Governance Model

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. The mission of the unit is to support IT systems which will enable to optimize financial allocation on healthcare system and to model and monitor the IT system in healthcare, including interconnections between stakeholders.

National eHealth Strategy and Legislation

- Act on information system in the healthcare (Journal of Law 2011, No 133).
- The Plan of the Informatisation for eHealth for the years 2010-2015
- Policy paper for the health care 2014-2020

eHealth Services and Infrastructure

In Poland eHealth is considered a critical information infrastructure thus making for all ehealth systems obligatory the implementation of the provisions required.

- Platform for sharing services and resources of digital medical records with on-line business
- Electronic Platform for Collection, Analysis and Sharing of Digital Medical Records

Security Requirements related to eHealth Services

Some of the main strategic targets of “Poland e-Health strategy for 2004-2006” cover:

- Safety and security of medical data
- Availability of telemedicine services

In addition to this policy document, the National Critical infrastructure Program includes national priorities, objectives, requirements and standards to ensure the smooth functioning of critical infrastructure.

A.22 Portugal

Healthcare Governance Model

The central Government, through the Ministry of Health, is responsible for developing health policy and overseeing and evaluating its implementation.

Portugal has an independent cybersecurity authority. A working group for ehealth has been created now performing a gap analysis for security measures.

National eHealth Strategy and Legislation

There is no formal ehealth strategy. Existing strategies are formulated at regional level to be upgraded at the national level by the Ministry of Health Shared Services. The Ministry documentation encompasses also security oriented specific requirements and measures.

eHealth Services and Infrastructure

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 interconnection. In Portugal, most of the public sector ehealth system are operated by SPMS and offered as central systems to the healthcare providers.

- The services are Hospital Information System, Electronic Health Records, Patients Health Record, Patients Summary and ePrescription.
- SPMS has an MS Office 365 installation as a document process system for the healthcare sector domain which also acts as a community server.
- Efforts in the domain are located in supporting the creation of HL7 Portugal and IHE Portugal as soon as possible, SPMS provides to third party software and tools for workflow integration.

Security Requirements related to eHealth Services

Access control and authentication, interoperability and standardisation, monitoring, information exchange. However there is no regulated methodology for CII in national level.

A.23 Romania

Healthcare Governance Model

The head of the current healthcare system is the government, a centralised model, which conducts most of its steering through the Ministry of Public Health. However, district public health authorities (DPHAs), district health insurance funds (DHIFs), district councils, district public finance departments and district colleges of physicians ensure the delivery of healthcare services. While the bodies at the national level are responsible for creating healthcare policy and objectives, it is the organisation at the district level that have important impact on the modelling of services.

The National Health Insurance Agency is the operator of the electronic health file and the eHealth cards. They are under the supervision of the MoH. National Health Insurance Agency (CNAS) is a public autonomous institution of national interest with legal personality whose main object of activity is to ensure uniform and coordinated functioning health insurance system in Romania.

National eHealth Strategy and Legislation

The absence of agreed National eHealth Strategies for Romania has resulted to many end to end IT equipment without the evaluation of the real needs and the existing applications.

Because of the fact that Romania has a tightly centralised government system, no regional eHealth strategies have been considered.

The Health Reform Law 95/2006 requires the Ministry of Public Health to establish an integrated information system for public health management.

eHealth Services and Infrastructure

- eHealth card system
- electronic health file

Security Requirements related to eHealth Services

No relevant information has been identified.

A.24 Slovakia

Healthcare Governance Model

The Ministry of Health is the key policy-maker and regulator in the system, collaborating closely with the Ministry of Finance. As the main state executive body responsible for healthcare and health protection, the Ministry of Health proposes the principal directions and priorities of state health policy and prepares and submits the appropriate draft legislation to the Government.

National eHealth Strategy and Legislation

- Strategic Goals of eHealth – key tool of public governance informatisation in the area of healthcare (2008)
- eHealth Programme in Slovakia (2008-2020)
- Act no. 153/2013 Coll. on the National Health Information System and on Amendments and Additions to Certain Laws

eHealth Services and Infrastructure

Slovakia is still in the planning phase of its eHealth services and infrastructure.

Security Requirements related to eHealth Services

No relevant information has been identified.

A.25 Slovenia

Healthcare Governance Model

The Ministry of Health develops the national health policy and provides regulatory and supervisory support to the healthcare system and health monitoring. The Council of Informatics in healthcare and the Committee for healthcare information standards are the expert bodies for ICT in healthcare.

National eHealth Strategy and Legislation

- Strategy for informatization of the Slovenian health care system 2005-2010 (Ministry of Health, 2005) eHealth Programme in Slovakia (2008-2020)
- Slovenian strategy for eHealth called "e- Zdravje2010" (e-Health2010) for the period from 2006 to 2010 focuses on information systems and services that contribute to the development of the healthcare sector and bring improvements in access to care and quality of services taking also into account business and professional challenges. "e- Zdravje2010" is part of a comprehensive document for 2006 - 2013 named "Strategy of the Republic of Slovenia " (aka si2010).
- Resolution on the National Health Care Plan for the period 2008-2013 (Ministry of Health, 2008)

eHealth Services and Infrastructure

There is a plan to digitalising the healthcare sector, including EHR and ePrescription, however this system is not functional yet.

Security Requirements related to eHealth Services

No relevant information has been identified.

A.26 Spain

Healthcare Governance Model

Spain has decentralised its administration and, nowadays, is divided into 17 autonomous communities, plus two autonomous cities (Ceuta and Melilla), which have competences in many areas. In this process, responsibility for most administrative services has been transferred to the regional level[25]. The Spanish health system has two levels of organisation: the central and the regional health services. The main body of the central administration is the Ministry of Health. The Ministry is in charge of the proposals and implementation of the government's general guidelines about health policies. The regional organisation of health services is the responsibility of the autonomous regions. The health planning must be based on the central administration policies, and each region

[25] http://www.ehealth-strategies.eu/database/documents/Spain_CountryBrief_eHStrategies.pdf, page 8

is required to have its own health centre. Local health services are the fundamental structures of the Spanish health system.

National eHealth Strategy and Legislation

In Spain, there is no national eHealth strategy. However, regional eHealth strategies have been developed such as the Strategic Plan for the ICT in Health in Catalonia (2008-2011), the Quality Plan for the National Health System and Plan Avanza .

eHealth Services and Infrastructure

There are several eHealth systems at the regional level, which address the issues such as e-prescription and Electronic Health Record. One of the most advanced examples is DIRAYA system, the public health system in the autonomous region of Andalusia (eight million inhabitants). Structured around an electronic shared patient file which is accessible to nearly all healthcare professionals in the region, it has all sorts of practical uses for patients while at the same time enabling a better management of health spending in an area which is hard-hit by unemployment. Launched in 2000, the system is currently used by nearly 1,500 health centres, 29 hospitals and 102,000 healthcare professionals (94%).

Security Requirements related to eHealth Services

In Spain healthcare systems are considered critical information infrastructures. The Spanish Law 8/2011 (April 28) that includes measures for protecting critical infrastructure in Spain, covers the baseline requirements by the public and private sectors.

A.27 Sweden

Healthcare Governance Model

Sweden is administratively divided into 21 county councils and 290 municipalities; and the healthcare system is decentralized and organized on three levels: national, regional and local. The municipalities (local level) are accountable for the social services and elderly care whereas the county councils (regional level) are primarily responsible for planning and organizing healthcare including eHealth services. Accordingly, the National Board of Health and Welfare (NBHW) and Swedish Association of Local Authorities and Regions have agreed on a National Strategy for eHealth.

There are two overall (national) responsible agencies: (a) Datainspektionen (Swedish Data Protection Agency) and (b) Myndigheten för samhällsberedskap (Swedish Civil Contingencies Agency)

National eHealth Strategy and Legislation

National eHealth – the strategy for accessible and secure information in health and social care (2010)[26].

eHealth Services and Infrastructure

There are seven basic national infrastructure services that allow healthcare providers to securely access essential patient data:

- SITHS is a national security solution for electronic and physical identification for secure and authorized communication of information. By using the SITHS ID-cards, providers can identify themselves and verify their authorization, independent of organizational and geographical boundaries. In this manner the

[26] *http://www.nationellehalsa.se/*

identity and the legal responsibility of the health service provider during patient data transfer at any time point is guaranteed.
- Sjunet is a robust, dedicated IP-based broadband network that enables electronic communication between Swedish hospitals, primary care centers and many other health care providers. This quality-assured network allows secure communication and transfer of data for more than 100 services such as ePrescriptions, medical images, patient data transfer, etc.
- Security services
- HAS Directory service
- Teleconsultation
- Common Service Platform
- List of medication (part of the Patient Summary (PS))

Security Requirements related to eHealth Services

The level of security of the Swedish eHealth Agency is considered to be medium due to budget limitations. The means used to ensure security comprise: (a) compliance with national regulation, (b) implementation of security measures, (c) SLAs and (d) internal audits.

A.28 United Kingdom

Healthcare Governance Model

There is no unified British healthcare system. Instead, England, Scotland, Wales and Northern Ireland are managed by four distinct National Health Systems ("Health and Care service" in the case of Northern Ireland), although it is the English NHS that represents Great Britain as a whole in exterior matters. Therefore, Great Britain encompasses four distinct healthcare systems, each with its own unique characteristics.

The Department of Health of England has set the HSCIC to be the supervisory authority for eHealth operators. The setting in England can be called de-centralised as the same applies for Wales, Scotland and the other regions. They are responsible for: collecting, analyzing and presenting national health and social care data, maintaining a register of all the medical information, managing national IT systems that handle medical data, setting standards and guidelines in the field of data collection, publishing a set of rules on how the personal confidential information of patients should be looked after through indicators that can be used to measure the quality of health and care services, and finally they help health and care organizations improve the quality of the data they collect and receive.

National eHealth Strategy and Legislation

Great Britain basically pursues several distinct healthcare strategies, as each NHS develops its own solutions in accordance with its respective legal framework. All NHS do, however, see the development of eHealth services as crucial for the future, and are independently developing state-of-the-art eHealth solutions.

There is a specific eHealth strategy established in England. The department of Health published in 2012 a document called “The Power of Information” and this was followed in November 2014 by the National Information Board’s "Framework for Action".

The Health and Social Care Information Centre produces and tests the healthcare information exchange policy primarily through standards and toolkits.

eHealth Services and Infrastructure

- NHS Care Record Service
- Summary Care Records
- Electronic Prescription
- Electronic Appointment Booking
- Hospital Information System
- Laboratory Information System
- Radiology Information System
- Electronic Health records
- Patients Health Record
- Patients Summary
- Patients Summary

EHR, patient records, reimbursement system are interlinked. All primary care networks are all connected. Also other services in scope: data sent for reimbursement, national applications (demographics – national index central model, ePrescription), link to national application from the hospital's, GPs applications, and messaging exchanges between hospitals and GPs. No storage of data only monitoring!

Security Requirements related to eHealth Services

In UK the Health sector is considered a critical sector. With respect to critical national infrastructure including CIIP the approach is from an 'all risk perspective'. This enables to consider the scale of cyber risk and the necessary response against other threats and hazards facing the UK's CNI. In the interests of national security the UK does not makes its critical sectors public. However they do include those public and private sectors which ensure the provision of critical services to the UK and whose loss or disruption may carry a significant economic, social or health consequence.

England has developed non regulated methodology for CIIs in national level, which was based in EU guidelines. However no specific security requirements are mentioned there. These are set by the CPNI.

ENISA

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

Athens Office

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

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