D7.3 Common Security Framework for eHealth

Information Note

WP 7– Overcoming implementation challenges

15-10-2018

Version 0.6

Lead: 3rd RHA

Grant Agreement nº 801558

Co-funded by
the Health Programme
of the European Union

Purpose

This note provides information about the objectives, scope and structure of Deliverable 7.3 established in the WP7 specific to data and systems security.

Objectives

The vision of this task is to assist eHealth professionals in building more secure eHealth systems and services at a national and at a cross-border level by producing a Common Cybersecurity Framework for eHealth systems and services (CCFeH).

The objectives of this task are the following:

- Examine the different levels of preparedness that Member States have regarding security issues, which has led to fragmented approaches across the EU. This results in an unequal level of protection of eHealth systems, services and of patients' and health professionals' data involved. Lack of a Common Security Framework makes it impossible to set up an effective mechanism for cooperation at Union level.
- Provide Common Security Framework guidelines for eHealth systems and services at a national and at a cross-border level (Use cases: cybersecurity in eHealth services and architectures, cybersecurity requirements for Patient Summary, ePrescription services, and other interoperability and portability services, security of eHealth systems e.g. medical devices).
- Increase awareness of national health authorities and health professionals on data and systems security issues after identifying the key issues to be tackled through surveys.
- Align with and elaborate on results of other EU projects and initiatives relative to cyber risks such as cPPP[1].
- Align with the Network & Information Security (NIS) Directive, assist in its implementation and aid in tackling challenges on data and systems security.

Scope

Deliverable D7.3 "Data and systems security", part of Work Package 7 of eHAction, will investigate previous Joint Actions' outcomes, other EU related project outcomes such as epSOS and the NIS Directive, as well as already implemented common applications and obstacles in implementing common security guidelines.

It will take 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 (legislation, norms, guidelines, recommendations etc).

It will focus on eHealth information systems and infrastructures as well as on the relevant assets that are considered critical both for the society and for the interested stakeholder groups. As a starting point, this study aims to showcase how the MS implement cybersecurity 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

[1] cPPP: Contract of Public- Private Partnership, see https://ecs-org.eu/cppp

information networks and systems, EHR and 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 and integrity of assets, and continuity of the services.

The aim 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 governmental authorities, policy makers and specialists.

A survey will be conducted among stakeholders regarding security of eHealth systems and services at a national and at a cross-border level. The data analysis will identify the main points that need to be addressed in order to assist eHealth professionals in implementing security guidelines such as:

- measures relating to preparedness, response and recovery
- needs for education, awareness-raising and training programmes relating to the security of eHealth systems and services network
- risk assessment plan to identify risks
- various factors involved in the implementation of the national strategy on the security of network and information systems
- Identification of national legislation on cybersecurity and eHealth, the governing authorities and the service provider organizations
- Assessment of the perceived criticality of the relevant infrastructures and assets
- present the security priorities and challenges.

Using the results of the survey, other existing guidelines and in alignment with NIS directive, D7.3 will produce a CCFeH which will address issues like cybersecurity in eHealth services and architectures, cybersecurity requirements for Patient Summary and other interoperability and portability services as well as security of eHealth systems.

Deliverable structure

D7.3 will report on recent studies after a desk survey using assessment of previous Joint Action's outcomes, projects (like epSOS) and other initiatives even outside the healthcare sector.

D7.3's main objective is to propose a common security framework for eHealth systems and services at a national and at a cross-border level (enhancement of eHealth systems and services security, actions to continuous validations, actions to focus on stakeholders, improvement of user acceptance, adhering to standards and legal and ethical directives).

D7.3 will also present relevant use cases (cybersecurity in eHealth services and architectures, cybersecurity requirements for Patient Summary and ePrescriptions) and extend CCFeH to other correlated fields (like scalability, interoperability, security of data on IoT and medical devices, legal, privacy and ethical issues) and to the eHealth ecosystem in general.

Main challenges and risks

Regarding the possible risks, this Work Package can suffer from a lack of participation in the work done by enough experts from all MS and affiliated entities. Another challenging factor is the dissemination of the outcomes of this Work Package.

Next Steps

- Sharing the outcomes (deliverables) of this Work Package to all interested parties.
- Evaluation of the implementation of the knowledge that MS gained in the Workshops of this WP.
- The Common Security Framework after adoption from eHN shall be published and communicated to all IT staff of large healthcare organizations and relevant external parties.
- The Common Security Framework shall be reviewed at planned intervals or if significant technological or legal changes occur to ensure its continuing suitability, adequacy, and effectiveness.

References

1. https://ecs-org.eu/cppp
2. http://www.epsos.eu/

Terms and Abbreviations

Terms

Abbreviations

Abbreviation	Meaning	Source
cPPP	Contract of Public- Private Partnership	
ENISA	European Union Agency on Network and Information Security	
NIS directive	Network and Information Security Directive	
CCFeH	Common Cybersecurity Framework for eHealth systems and services	