eHAction
Joint Action supporting the eHealth Network

D7.3 Common security framework for eHealth systems and services at a national and at a cross-border level

(Proposed New Title: Practical cybersecurity guide for healthcare providers)

Information Note

WP7 Overcoming implementation challenges

Revision 2.2, 02-05-2019

15th eHN meeting, June 2019

For Discussion

Grant Agreement nº 801558

Co-funded by the European Union's Health Programme (2014-2020)

Disclaimer

The content of this deliverable represents the views of the author only and is his/her sole responsibility; it cannot be considered to reflect the views of the European Commission and/or the Consumers, Health, Agriculture and Food Executive Agency or any other body of the European Union. The European Commission and the Agency do not accept any responsibility for use of its contents.

Purpose

The proposals for the work item on cybersecurity, submitted to the eHealth Network in November 2018, were discussed and considered too ambitious given the state of deployment of the national cross-border eHealth projects supported by the CEF programme and the lack of maturity for deciding upon common policy and measures. eHAction WP7 was therefore requested to reconsider the scope of this work item and reframe the activities towards a more supportive approach involving learning and sharing of national experiences and eventually supporting national organisations in meeting their security objectives, not least those emerging from the implementation of Directive (EU) 2016/1148, referred to as the Network and Information Security (NIS) Directive[1].

This Information Note provides information about the revised scope, objectives, work approach and deliverables to the eHealth Network over the next year.

The eHealth Network is invited to reflect on these proposals and provide additional direction as appropriate for this work.

Scope

The work on eHealth Systems and Information Security should focus on:

(i) Facilitating co-operation and exchange of information and good practices on digital health cybersecurity of eHealth systems and services at national and cross-border levels. This may be facilitated by the national legal frameworks that transpose the NIS Directive;

(ii) Supporting healthcare organisations through a responsive approach, tailored to the needs for practical guidance for healthcare providers on prioritised cybersecurity issues.

These objectives will be pursued in close collaboration with European Union Agency for Network and Information Security (ENISA).

Objectives

I: Co-operation and Information Exchange

The first objective is to support co-operation of eHealth systems and services at a national and at a cross border level, leveraging on the national legal frameworks that transpose Directive 1148/2016 and through exchange of information and good practices on digital health cybersecurity.

Building trust in the health information systems and technologies ecosystem is key to scaling up eHealth services and creating added value for the citizens, through integration of information systems, services and resources, as well as through exploitation of health data. Information

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://data.europa.eu/eli/dir/2016/1148/oj

security and cybersecurity is a value enabler for health entities and for the health sector as a whole. Current studies and research[2,3,4,5] clearly show that overall there is a relatively low level of maturity in cybersecurity management across the health sector worldwide; at the same time however, these studies highlight the recognition of the importance of cybersecurity in the broader digital health context and the need to employ harmonised security frameworks to address common challenges and threats together.

II: Practical Guidance for healthcare providers on a priority set of issues.

The second objective is to create and deliver practical guidance for operators of critical services in the healthcare sector on a priority set of issues, set forth by the eHealth Network.

A risk-based approach to cybersecurity encompasses the people, processes and technology dimensions of organisations, their vital assets and their specific cyber context. Supporting healthcare organisations and competence centres to tackle this broad spectrum of challenges at the appropriate level of granularity through European co-operation may be pursued through exploiting and building upon the existing knowledge, not least what has been generated through national and international efforts.

Work Approach

Desktop research and analysis is currently being carried out in order to establish a ***framework for discussion with representatives for hospitals and eHealth Competence Centres in EU member states*** participating in the July 2019 workshop in Thessaloniki. These sources include a number of recent ENISA studies focusing on the health sector, the information security guidance and criteria that EU member states (MS) are fulfilling as part of the audit process for launching cross-border eHealth services, national and international documents focusing on security frameworks for cybersecurity for eHealth, and useful resources from recent and ongoing relevant EU projects.

The discussion will be launched during the July 2019 eHAction workshop in Thessaloniki, employing a methodology leading transparently to an ***initial list of priorities*** to be collaboratively addressed, representing a balanced mix of policy and operational perspectives. This will be followed up by a survey among EU MS aiming to capture priorities for joint efforts in the area for improving eHealth cybersecurity.

The work should lead to a ***documented proposal for priority areas and work items for further MS co-operation***, to be submitted for endorsement by the eHealth Network in November 2019.

[2] Reference document on security measures for Operators of Essential Services, NIS Co-operation Group, Feb 2018
[3] Security and Resilience in eHealth, Security Challenges and Risks, ENISA 2015
[4] Smart Hospitals, Security and Resilience for Smart Health Service and Infrastructures, ENISA 2016
[5] Global Digital Health Partnership, White Paper: Securing Global eHealth Efforts (in progress)

European co-operation may be best addressed through a stepwise approach, building on prioritised and mature use cases and leveraging the existing mechanisms of European co-operation in Directive 2011/24[6] and the NIS Directive.

Harvesting the knowledge that has and is being documented by MS and shared in the framework of the CEF deployment ***of cross boarder exchange of patient summaries and e-prescriptions,*** for the purposes of the formal audit process and particularly the Information Security thematic area will provide a sound basis for identifying common approaches and best practices taking into account the national realms. This will be supplemented by knowledge to be found in studies published by ENISA and other international organisations on cybersecurity in eHealth services and architectures in order to arrive at ***a practical guide for healthcare providers, on a prioritised list of topics.***

This guide will be submitted to the eHealth Network for adoption in Spring 2020.

Main challenges and risks

There is a significant degree of variation across MS of the practices applied. A lack of a harmonised approach and a minimum set of commonly agreed safeguards to be applied by healthcare providers across MS would significantly endanger sharing of health data across borders.

Next Steps

- First eHAction eHealth Interoperability Workshop , July 10-11, 2019, in Thessaloniki, Greece.
- Sharing the outcomes (deliverables) of this Task to all interested parties.
- Enlargement of the knowledge gained in this Task, through launching a broader survey.
- The Practical Cybersecurity guide for healthcare providers, after adoption by the eHealth Network, shall be published and communicated to all IT staff of large healthcare organisations and relevant external parties.
- The Practical Cybersecurity guide shall be reviewed at planned intervals or if significant technological or legal changes occur to ensure its continuing suitability, adequacy, and effectiveness.

[6] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, http://data.europa.eu/eli/dir/2011/24/oj