



15TH eHEALTH NETWORK 11-12 JUNE 2019, BUCHAREST, ROMANIA

COVER NOTE BY eHEALTH NETWORK SECRETARIAT

Topic 4.3.1. D7.3 Report Common Security framework for eHealth - eHAction

Issue at stake

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

The proposals for the work item on cybersecurity, were submitted to the members of the eHealth Network meeting in November 2018. The proposals were discussed and considered too ambitious, given the state of deployment of the national cross-border digital health projects. This information note provides information about the revised scope, objectives, work approach and deliverables over the next year.

Summary

eHAction has reconsidered the scope of this work item and has reframed 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.

The new proposed scope is focused on two key priorities: (i) supporting co-operation of digital health systems and services at national and cross-border level, leveraging on the national legal frameworks that transpose Directive 1148/2016 and exchanging information and good practices on digital health cybersecurity; (ii) creating and delivering practical guidance for operators of critical services in the healthcare sector on a priority set of issues, set forth by the eHealth Network.

A number of studies, including by the ENISA, have focused on cybersecurity in the health sector. At the same time, information security guidance and criteria are successfully fulfilled by the EU Member States joining the community of cross-border digital health services. National and international documents focusing on security frameworks for cybersecurity for digital health, and useful resources from recent and ongoing relevant EU projects are also part of supportive documentation.

The discussion will be launched during the eHAction workshop in July 2019 in Thessaloniki, Greece, employing a methodology leading transparently to an initial list of priorities to be collaboratively addressed, representing a balanced mix of policy and operational perspectives.

Coordinator of eHAction has proposed that this will be followed up by a survey among the Member States aiming to capture priorities for joint efforts for improving cybersecurity in digital health. In addition, it was suggested to plan additional WS on cybersecurity on 1-3 October 2019, in Portugal, where it will be presented by ENISA (EU - CERT). Appeal for the presence of all Member States and countries in the workshop to explore a joint planning and to create more rapid response reaction to incidents.

The Global Digital Health Partnership (GDHP) is a collaboration of governments and territories, government agencies and the WHO, formed to support the effective implementation of digital health services, where many Member States are part of it, and it has worked out a 3 year roadmap that is worth analysing from a eHealth Network perspective.

The work should lead to a documented proposal for priority areas and work items for further Member States co-operation, to be submitted for endorsement by the eHealth Network in November 2019/May 2020.

Format of procedure in the eHealth Network meeting

The Member State co-chair introduces the topic and opens the floor to the eHealth Network for comments and questions.