



SECUREHOSPITALS.EU

RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING
TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

D2.4 Relevant cybersecurity projects list and liaisons overview



This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 826497.

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

Title: **Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub**

Coordinator: INTERSPREAD GmbH

Reference: 826497

Type: CSA

Program: HORIZON 2020

Theme: eHealth, Cybersecurity

Start: 01. December, 2018

Duration: 26 months

Website: <https://project.securehospitals.eu/>

E-Mail: office@securehospitals.eu

Consortium: **INTERSPREAD GmbH**, Austria (INSP), Coordinator
Erasmus Universiteit Rotterdam, Netherlands (EUR)
TIMELEX, Belgium (TLX)
Fundacion Privada Hospital Asil de Granollers, Spain (FPHAG)
Cooperativa Sociale COOSS Marche Onlus, Italy (COOSS)
Arbeiter-Samariter-Bund, Austria (SAM)
Johanniter International, Belgium (JOIN)
European Ageing Network, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	D2.4
Title:	Relevant cybersecurity projects list and liaisons overview
Lead beneficiary:	INSP
Work package:	WP2
Dissemination level:	PU
Type	Other
Due date:	30.09.2019
Submission date:	30.09.2019
Authors:	Stela Shiroka, INSP
Contributors:	All partners
Reviewers:	Sigrid Panovsky, SAM

Acknowledgement: This project has received funding from the European Union's Horizon 2020 Research and Innovation Action under Grant Agreement No 826497.

Disclaimer: The content of this publication is the sole responsibility of the authors, and does not in any way represent the view of the European Commission or its services.

TABLE OF CONTENT

1	Introduction.....	7
2	Projects List	8
3	Liaisons overview	9
1.1.	PANACEA 1st End/users/stakeholder workshop	9
1.2.	SPHINX Workshop on cybersecurity situation awareness.....	11
1.3.	ENISA 5th eHealth Security Conference	11
4	Conclusion and next steps.....	12
	Annex 1: Workshop Agendas	13

TABLE OF FIGURES

<i>FIGURE 1: R&D Projects list on the OIAH.....</i>	<i>8</i>
<i>FIGURE 2: SecureHospitalals.eu presentation at the PANACEA Workshop.....</i>	<i>10</i>
<i>FIGURE 3: SPHINX Workshop Banner</i>	<i>11</i>
<i>FIGURE 4: ENISA Conference Banner</i>	<i>11</i>

EXECUTIVE SUMMARY

This deliverable presents the continuation of the work carried out in D3.2 which consisted in the collection of projects and initiatives funded under the Horizon 2020, the Seventh Framework Programme or similar initiatives in the field of cybersecurity for the healthcare domain. Following the collection and classification of the project and initiatives, Task 2.4 involved integrating the list of projects on the SecureHospitals.eu online hub and liaison activities with each of them in order to promote their engagement on the online hub by sharing knowledge and showcasing solutions, but also for the SecureHospitals.eu project to participate in external activities to build and strengthen synergies. The overview on the liaison activities presents what has been undertaken in the first project months, what is currently going on and future plans of collaboration with a number of projects that under the immediate interest of cooperation for the SecureHospitals.eu project.

1 Introduction

Under the Horizon 2020 and Seventh Framework programmes, the European Commission has issued a number of competitive calls for research, innovation and coordination activities in the field of cybersecurity in the healthcare domain, whereas cybersecurity in general is one of the main thematic areas of the Horizon 2020 programmes funding countless projects on the topic. One of the main aims of the funding agencies and of the projects themselves, is to create synergies among the initiatives addressing the same challenges in order to achieve mutual learning, cooperation in the research and innovation outcomes, avoid duplications, and cooperate in disseminating results.

As part of the D3.2, the main project and initiatives of relevance to SecureHospitals.eu were identified. These include cybersecurity projects funded by the Horizon 2020 programme, but also major institutions and initiatives such as ENISA, which is relevant to SecureHospitals.eu both as a knowledge provider but also as a dissemination platform. While the identification and screening of the projects took place as part of the D3.2, the aim of this deliverable is to report on the follow-up activities which can lead to cooperation and synergies with all of the identified.

The list of similar projects and initiatives has thus the following aim:

1. Being added on the SecureHospitals.eu online platform (R&D projects), it is an information resource for solutions seekers and for other researchers, trainers and innovators in the field.
2. Contact lists of each of the following initiatives serve for marketing the SecureHospitals.eu online platform, by offering each of the liaised projects (esp. the RIA/IA types) an additional space to promote their outcomes by actively sharing their information.
3. Building of stronger ties with a smaller number of projects, which consists in mutual sharing of results and co-organisation of training and awareness raising activities.

This deliverable describes the publication of the relevant projects list on the SecureHospitals.eu online hub, as well as liaison activities with the most and less relevant ones.

2 Projects List

The 'Solutions' module on the SecureHospitals.eu online hub seeks to provide information on various solutions for cybersecurity issues to healthcare organisations ('solutions seekers'). This section provides directories of technical solutions, legal consulting and innovation consulting services, and also an overview of the collected R&D projects in the field. The projects and initiatives list, is included under this category, since all of them are knowledge and innovation providers with the aim of 'solving' cybersecurity issues in healthcare.

Figure 1 shows the interactive list of all identified and classified projects and initiatives integrated on the SecureHospitals.eu online hub. This page lists the projects by acronym/name of initiative, and upon clicking on each of them it shows the basic facts and information such abstract, funding programme and duration. Official logos of all projects and initiatives are also being added to the page.

Many of these projects are designing and developing products that are close to being rolled out in the market, so could thus be listed under the 'Technical Solutions' category. Their coordinators and partners on the other hand are at the same providing products and services that address the needs of the solution seekers on the SecureHospitals.eu online hub. Thus, following the full launch of the platform, all of the mentioned projects and initiatives are being contacted with the invitation to register on the online hub, so they can share their knowledge and showcase their solutions to the community. At the latest stage of the development of the hub, the aim will be to have all of these stakeholders engaged within the 'Community of Practice' space, which will provide ground for new collaboration ideas and innovative solutions.

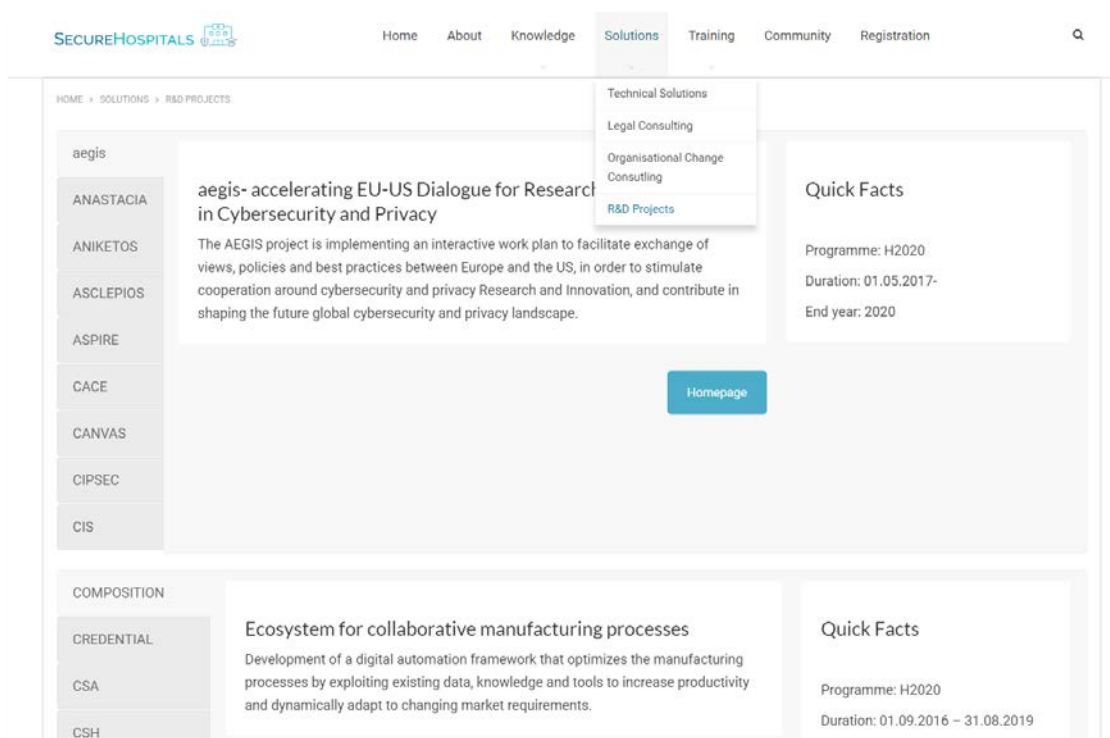


FIGURE 1: R&D Projects list on the OIAH

3 Liaisons overview

Of all the identified projects and initiatives listed within the list, the projects of the outmost interest to SecureHospitals.eu, are those funded by the (same) call H2020-SC1-FA-DTS-2018-1 with focus on security. The mentioned call was divided into the following two topic IDs: SU-TDS-03-2018: *Raising awareness and developing training schemes on cybersecurity in hospitals* – which funded SecureHospitals.eu; and SU-TDS-02-2018: *Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures* – which funded seven projects: [PANACEA](#), [ProTego](#), [CUREX](#), [SERUMS](#), [FeatureCloud](#), [SPHINX](#), [ASCLEPIOS](#).

As the only Coordination and Support action among all the above-mentioned projects, with a strong focus on awareness raising, SecureHospitals.eu understands itself as an initiative for promoting the results of the mentioned projects by engaging them in all the project activities and outcomes. During the knowledge aggregation phase which has run from project Month 1 to 10, most of the mentioned projects were at their early stages of definition of requirements and had not released results. The created training materials coming as a result of knowledge aggregation thus do not reference to any project results. Nonetheless most of them are conceptualised in an open character, making it possible to enrich and adjust content at the later stages, with the aim of feeding upcoming outcomes of similar projects. As the knowledge aggregation phase and the creation of the main training frameworks within SecureHospitals.eu has been concluded, and the online hub has been launched, increased synergies in the following activities will be possible. The planned synergy activities include:

- Engaging other project members to register on the SecureHospitals.eu online hub to showcase their results and remain connected through the ‘community of practice’
- Co-organising webinars featuring perspectives from different projects
- Having a session on the outcomes of other projects, at the SecureHospitals.eu summer school
- Co-organising dissemination events such as the SecureHospitals.eu final conference

Though much of these activities are planned for the next project stage starting at M10, the cooperation activities with other projects have already started and are ongoing. The next section describes the activities that brought the community together and the upcoming one scheduled for October 2019.

1.1. PANACEA 1st End/users/stakeholder workshop

Upon the invitation of the PANACEA coordinators, the first meeting among the community of the projects funded under the same call took place at the Gemelli University Clinic in Rome, Italy on the 28th and 29th of May 2019. Conceptualised as a workshop for the PANACEA end-users (healthcare

organisations) and other stakeholders, it provided the ground for presenting other Horizon 2020 project and identifying potential synergies¹. Besides the presentation of the PANACEA project, and other projects including SecureHospitals.eu, SPHINX and CUREX, the two-day workshop aimed at collecting user-requirements for the toolkits to be created as part of the mentioned project. Since of the foci of the toolkits and user requirements addressed were training needs and governance models, this was particularly important for SecureHospitals.eu where the creation of the training packages and the conceptualisation of the online hub as an information/training resource was ongoing. Outcomes of the workshop regarding the training of medical and administrative personnel in healthcare organisations, as well as strategies for nudging and consulting management level professionals provided an integral part in the development of training packages and strategies (together with the trainer interviews conducted as part of D4.2, and the literature review).

Additional cooperation activities in the form of workshops, trainings, and dissemination events were, and mutual sharing of outcomes were also discussed and planned among all represented projects.



FIGURE 2: SecureHospitalals.eu presentation at the PANACEA Workshop

¹ <https://panacearesearch.eu/events/1st-end-usersstakeholders-workshop>

1.2. SPHINX Workshop on cybersecurity situation awareness



Another activity planned and discussed already during the meeting in Rome was the workshop organised by the SPHINX project in Brussels, Belgium, on the 10th of July 2019². The workshop topics were mostly revolved around technical requirements, thus SecureHospitals.eu was not engaged with an active

participation. However, Brussels-based partners who attended the event and represented the project in the conversations had several important takeaways for example on the healthcare landscapes in Portugal, Romania and Greece, as well as required standards, the work of ENISA etc.

FIGURE 3: SPHINX Workshop Banner

1.3. ENISA 5th eHealth Security Conference



The third event planned during the Cybersecurity Awareness Month is the 5th eHealth Conference³ organised by ENISA in Barcelona, Spain as part of the Barcelona Cybersecurity Congress. Attendance at this conference was already flagged during the meeting in Rome by the conference organisers and eHealth responsible at ENISA.

Aiming to join this event and contribute to the discussions on the cybersecurity issues, the full SecureHospitals.eu consortium decided to attach it to the regular consortium meeting. Although active participation as a speaker/panel in the conference due to the defined topics which were not completely similar to the outcomes generated by SecureHospitals.eu to date, participation of all partner with the purpose of learning more on the recent development in the field and networking with other projects and stakeholder to communicate the project results will be highly important for the project.

FIGURE 4: ENISA Conference Banner

² <https://sphinx-project.eu/workshop-on-cyber-security-situation-awareness-for-health-organizations-cybersec4health/>

³ <https://www.enisa.europa.eu/events/5th-ehealth-security-conference/event>

4 Conclusion and next steps

The initial stage of the synergies' creation has involved identifying similar projects and initiatives, and establishing the first contacts. As the project progresses and it has further shaped its training and awareness raising strategy for the second period, the involvement of external stakeholders will be increasingly important. For this purpose, continuous contacting and cooperation with the projects' list presented in this deliverable will be on the agenda. The three described activities in section 2 present only the initiation of the process of getting to know the community, establishing ties and the plans for future cooperation. In the next months more knowledge sharing and cooperation will take place through the organisation of common training and knowledge sharing events. The SecureHospitals.eu online hub will on the other hand provide more ground for knowledge sharing and cooperation opportunities between all the projects and stakeholders from the field.

Annex 1: Workshop Agendas



www.panacearesearch.eu

1st END-USERS/STAKEHOLDERS WORKSHOP AGENDA

<i>Day 1 – Tuesday, May 28th, 2019</i>		
Time	Activity	Speakers
13:00	Registration	
14:00-14:05	Welcome	FPG
14:05-14:45	About PANACEA project and first results	FPG, RHEA
14:45-15:45	H2020 R&D projects in healthcare and liaison	H2020 Project coordinators
15:45-16:00	Coffee break	
16:00-16:20	Workshop Scope and Instructions	RINA
16:20-18:30	1 st parallel workshop session	ALL
19:30	DINNER at Hotel Marriott Central Park	
<i>Day 2 – Wednesday, May 29th, 2019</i>		
Time	Activity	Speakers
8:30-9:00	Review and wrap up of the previous session results	Group Moderators
9:00-11:00	2 nd parallel workshop session	ALL
11:00-11:30	Coffee break	
11:30-13:00	3 rd plenary session	ALL
13:00-13:15	Review and wrap up of the workshop results	Group Moderators
13:15-13:30	Closing remarks and next steps	FPG
End of the Workshop		



Workshop

Wednesday July 10, 2019	
09:00-09:15	Registration
09:30-09:30	Welcome from the EU/NTUA (SPHINX Coordinator)
09:30-11:00	<p>Session one:</p> <p>"Improved security of Health and Care services, data and infrastructures"</p> <p>Chair/Moderator: Dr. Christos Ntanos, NTUA, Greece</p> <p>Panelists:</p> <ol style="list-style-type: none"> 1. Evangelos Stamatiadis, 5th Regional Authority of Greece Keynote talk on "Greece Cybersecurity healthcare landscape". 2. Ricardo Cabecinha, Hevora Hospital, PT Keynote talk on "Portuguese Cybersecurity healthcare landscape". 3. Sergiu Marin, Polaris Medical, RO Keynote talk on "Romanian Cybersecurity healthcare landscape". <p>Panel Game Discussion with three teams from the Panelists and the audience trying to address the following key questions: What violations have occurred? How are risks evolving? Which Hospital processes /systems are more vulnerable (is more crucial)?</p>
11:00-11:15	Coffee Break
11:15-13:00	<p>Session two:</p> <p>" Less risk of data privacy breaches caused by cyberattacks;"</p> <p>Chair/Moderator: Dr. Evangelos Markakis, HMU, Greece</p> <p>Panelists:</p> <ol style="list-style-type: none"> 1. Mr. George Doukas, NTUA Greece. (20 Minutes Max) Keynote talk on "Cybersecurity Standards for reducing Data breaches" 2. Dr. Evgenia Nikolouzou, ENISA, EU Keynote talk on "ENISA role and work on the eHealth Domain" 3. Mr. Yannis Nikoloudakis, HMU, Greece (20 Minutes Max) Keynote talk on "Vulnerability assessment as a Service" <p>Panel Game Discussion with three teams from the Panellist and the audience (30 Minutes Max) trying to address the following key questions: What is the current protection level? What suspicious log events are found? How Cybersecurity Standards can help?</p>
13:00-14:00	Lunch Break



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2 of 3

Meeting agenda

Brussels, July 10, 2019



14:00-15:30	<p>Session three:</p> <p>"Increased patient trust and safety through Legal and Technological toolset"</p> <p>Chair/Moderator: Mrs. Dimitra Markopoulou, VUB, Belgium</p> <p>Panelists:</p> <ol style="list-style-type: none"> 1. Prof. Vagelis Papakostantinou, VUB, Belgium Keynote talk on "Legal and Technological toolset" 2. Mr. Philippe Costard, Santhea, Belgium Keynote talk on "Patient trust and Security the Santhea Approach" 3. Mrs. Lina Jasmontaite VUB, Belgium, Keynote talk on "GDPR AND CYBERSECURITY." <p>Panel Game Discussion with three teams from the Panellist and the audience (30 Minutes Max) trying to address the following key questions: Are we compliant to legislation? How is legislation evolving? What is the role of Digital Forensics, if any?</p>
15:30-15:45	Coffee Break
15:45-16:45	<p>Session four</p> <p>"United we thrive"</p> <p>Chair/Moderator: Dr. Christos Ntanos, NTUA, Greece</p> <p>Panelists:</p> <ol style="list-style-type: none"> 1. Dr. Evangelos Markakis, Hellenic Mediterranean University, Greece Mr. Marco Manso, EDGENEERING LDA, Portugal Keynote talk on "SPHINX Project focus on User Requirements" 2. Mr. Matteo Merialdo Keynote talk on "PANACEA Project focus on User Requirements" 3. Prof Christos Xenakis, University of Piraeus, Greece Keynote talk on "CURE X Project focus on User Requirements" 4. Mrs. Eleni Darra, KEMEA, Greece Keynote talk on "SAFECARE focus on User Requirements"
16:45-17:00	Closing Mark and Workshop Summary



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3 of 3

ENISA 5TH eHEALTH SECURITY CONFERENCE

AGENDA



CONFERENCE 30 OCTOBER, 2019 AT 08.30 AM

LOCATION OF CONFERENCE FIRA GRAND VIA, AV. JOAN CARLES I, 64, BARCELONA, SPAIN

30 OCTOBER, 2019	EVENT	SPEAKERS / PANELLISTS
	WELCOME SESSION	
08.30 - 09.00	Registration & Welcome Coffee	
09.00 - 09.15	Welcome & Opening	Francisco de Paula Polo Llavata , Spanish Secretary of State for Digital Advancement, Ministry of Economy and Business
09.15 - 09.30	Welcome speech	Hble. Sr. Jordi Puigneró i Ferrer , Conseller de Polítiques Digitals i Administració Pública, Generalitat de Catalunya
09.30 - 09.45	Keynote – EU eHealth Cybersecurity and Privacy Policy Context	Marco Marsella , Head of eHealth, Well-Being and Ageing Unit DG CONNECT, European Commission
	EHEALTH CYBERSECURITY REGULATIONS & INCIDENT REPORTING	
09.45 - 10.00	Incident Reporting under the NIS Directive	TBC , DG CONNECT, European Commission
10.00 - 10.15	CCN as CSIRT of reference for the public health sector	National Cryptologic Centre (CCN)
10.15 - 10.30	Cybersecurity Incident Reporting in the Portuguese Health Service	Pedro Batista , CISO and IT Director, SPMS
10.30 - 11.15	Discussion panel: The incident reporting framework Previous speakers (Moderator ENISA)	
11.15 - 11.30	Coffee break	
	CYBERSECURITY FOR HOSPITALS: ADDRESSING SECURITY IN PROCUREMENT	
11.30 - 11.50	ENISA 2019 study on procurement guidelines for hospitals	Dr. Athanasios Drougkas , NIS Expert, ENISA
11.50 - 12.10	The hospital perspective	TBC
12.10 - 12.30	The vendor perspective	Martha De Cunha Maluf-Burgman , QA/RA Program Manager for RF & Cybersecurity, Medtronic
12.30 - 13.00	Discussion panel on good practices for cybersecurity in procurement Panellists: previous speakers (Moderator Albert Haro , Information Security Manager, Cybersecurity Catalan Agency)	
13.00 - 14.00	Lunch Break	
	HACKING HEALTHCARE	
14.00 - 14.20	Cyber Europe 2020	Dr. Panagiotis Trimintzios , ENISA
14.20 - 14.40	Hacking Demo	Dimitrios Glynos , Census
14.40 - 15.00	From digital to physicians: Protecting the Four Aces of a healthcare organisation	Dr. Juan Carlos Muria Tarazon , Head of Health Sector S2Grupo
15.00 - 15.30	Coffee Break	
	LOOKING AT THE FUTURE	
15.30 - 15.50	Strategies to raise the level of awareness in the health sector	Marco Antonio Lozano , Head of Cybersecurity Services, Companies and Professionals, Spanish National Institute for Cybersecurity

ENISA 5TH eHEALTH SECURITY CONFERENCE

15.50 – 16.10	Awareness cybersecurity strategy of the Health Catalan Institute	Eduard Vilajosana , Head of Security Office, Health Catalan Institute
16.10 - 16.30	Blockchain and eHealth Cybersecurity	TBC
16.10 - 16.30	Closing Keynote	TBC , DG SANTE, European Commission

