SECUREHOSPITALS.EU

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

D5.3 Training Strategy 2

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:	**D5.3**
Title:	**Training Strategy 2**
Lead beneficiary:	**JOIN**
Work package:	WP5
Dissemination level:	PU
Type	Other
Due date:	30.09.2019
Submission date:	08.10.2019

Authors: **Georg Aumayr, Eva Pelgen, Joachim Berney,** JOIN

Stela Shiroka, INSP

Contributors: **All partners**

Reviewers: **Stela Shiroka**, INSP

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

TABLE OF TABLES

TABLE OF FIGURES

EXECUTIVE SUMMARY

This deliverable aims at further planning all training and workshop types of the project SecureHospitals.eu and put the results from D3.4 and D4.3 into practice. With the Massive Open Online Course (MOOC), the SecureHospitals.eu Summer School and the regional workshops, different ways of training and awareness raising can be addressed and allow the uptake of the project results.

- The MOOC is aimed for a large outreach among medical professionals and administrative staff in healthcare settings with different types of access to personal and medical data.
- The Summer School is aimed at management level professionals and trainers for cybersecurity in the healthcare sector.
- The workshops are regional training opportunities offered in the partners' countries, tailored to the local needs (e.g. local languages, awareness levels etc.).

The text elements of this deliverable are written in a way to extract it and use it for the announcement of the trainings on a website and advertisement material. Yet further planning will be ongoing until M12 for providing additional materials and information for registrations.

1 Introduction

The second part of the training strategy is aimed for the timeline and setup of local workshops, the summer school and the Massive Open Online Course (MOOC). The content for the trainings is described by D3.4 and D4.3, where this deliverable mainly described the types of formats to which the created materials will be applied, describing the partners involved in the each of the activities and the timelines of the delivery of the each of the formats. This deliverable provides a strategic setup of training periods and orientations of the single elements. Three main elements form the training related strategic approach of SecureHospitals.eu:

- The MOOC is aimed for a large outreach but low customization to potential 'customers' of a training program (medical professionals)
- The Summer School is aimed at healthcare managers and IT professionals operating as cybersecurity trainers within the healthcare organisations. The cascade of the outreach will take time but allows a higher customization and direct impact in the healthcare strategy.
- The workshops are a regional training for cybersecurity in institutions tailored to the needs of the regional health care staff.

This deliverable aims at collecting all trainings and workshop types of the project SecureHospitals.eu and put the results from D3.4 and D4.3 into practice. With the Massive Open Online Course (MOOC), the SecureHospitals.eu Summer School and the regional workshops, different ways of teaching, training and learning can be addressed and allow the uptake of the project results.

2 Massive Open Online Course (MOOC)

Format: The Massive Open Online Course will be launched starting in March 2020 and will consist of several pertinent modules focused on healthcare cybersecurity. The program is instructor-paced, meaning that each module will be released over the course of four to five weeks. This results in one module per week for participants to complete. The successful completion of the MOOC results in a completion certificate for the participant.

Each module will consist of a variety of materials including video learning components of around 15-20 minutes. In the videos, core cybersecurity concepts and threats will be explained. Concepts will be illustrated with real-life cases, guidelines for minimising risk and further reading materials. One of the sources for reading will be the articles on the Online Information and Awareness Hub, created as part of D3.4. Additionally, guidelines for minimising cybersecurity risks and threats will also be addressed.

Each module will be concluded with exercises and quizzes intended to increase and assess the knowledge comprehension of the participants. These will include both multiple choice questions and open answer questions. Participants need to conclude each module with a passing grade in order to be able to obtain a completion certificate.

To facilitate effective learning, the MOOC participants will be provided with access to an open discussion forum (only for participants) where they can discuss the material and cases further. The forum will also serve as a platform where participants can collaborate and complete open assignments.

Target group: the MOOC will be addressed to healthcare professionals and administrative staff

3 Summer School

Format: The SecureHospitals.eu Summer School will be oriented to management level professionals and cybersecurity trainers and include different formats such as workshops, guest speeches, round tables, field visits etc. The aim of the summer school will be to provide more knowledge to management professionals in healthcare organisation on promoting a cybersecurity culture within their organisations. Firsts, this consists on understanding the threats, scenarios and related outcomes and impacts for their organisations, illustrated with real-life case studies. Secondly, the summer school will aim to provide advanced knowledge on creating and developing the cybersecurity culture with the organisations by addressing key issues such as training of medical and administrative staff, situational awareness, risk management, addressing security in the procurement of new technologies etc. The training is set up by six steps to follow and provides an overview of policies and regulations, handbooks and guidelines, risk assessment and checklists and case studies. All of the lectures and workshops will have a strong hands-on approach and seek to engage the audience throughout all the sessions. A visit to a cyberage is also planned to be part of the 1 – week programmes involving project partners, guests and participant trainers and the managers.

Time & Location: 15-19 June 2020 in Brussels, Rue Joseph II, 144

Registration will be mandatory through the project official email: **office@securehospitals.eu**

Participants need to register first. There is a limited number of participations. If requested, full training can be booked afterwards. Participation at the summer school will be free of charge.

Preliminary Agenda:

Table 1: SecureHospitals.eu Summer School

SecureHospitals.eu Summer School Agenda		
Day	**Content**	
Monday	**Welcome and Introduction** **Why is cybersecurity so important for the healthcare industry?** Keynote speakers **Lecture:** Introduction to the legal frameworks and standards for privacy and cybersecurity in healthcare *Welcome Dinner*	**INTRODUCTION**

Tuesday	**Workshop:** Cybersecurity threats landscape - Existing and emerging threats **Lecture:** Awareness Raising, Training and the finding the right solutions - The SecureHospitals.eu Project and Web Platform **Workshop:** Designing the required training for your staff (6-step methodology)	**PREPAREDNESS**
Wednesday	**Presentations/Panel:** Toolkits for assessing and reducing cyber risks in hospitals and care centres – (Horizon 2020 projects presentation) **Lecture:** Addressing cybersecurity in procurement: ENISA 2019 study on procurement guidelines for hospitals **Workshop:** Setting up cybersecurity infrastructures, teams and carrying out regular exercises	
Thursday	**Visit to a CyberRange, Demos and Onsite Exercises**	
Friday	**Lecture:** Incident response guidelines and procedures **Workshop:** Recovery, lessons learned, and future budget planning **Concluding remarks and future perspectives**	**RESPONSE & RECOVERY**

4 Local Workshops and Webinars

Besides the MOOC and the summer school which will address stakeholder at the European level, the need to reach out to local members of the community, particularly for the addressing the language issue, the need for carrying out local workshops and webinars was identified. During the consortium meeting in Ancona, each of the partners agreed to host two workshops in their countries with the aim of engaging their local communities. Depending on the partner profile, the workshops will have different foci, involving either the topics and materials used for the MOOC or of the Summer School. The following sections provide a brief overview of the planned workshops and webinars among all consortium partners.

4.1. Specialties

Time.lex (TLX) is in the special position to join other workshops from different projects to share content and knowledge. The Austrian Samaritans (SAM) will provide a lecture to use SecureHospitals.eu to train their complete staff in cyber security. Therefore, larger implementation actions are necessary that need more planning. But this allows a direct impact of what SecureHospitals.eu is doing in the daily routines and increases the sustainability of the project. Inspired by this, Johanniter Internaitonal (JOIN) asked Johanniter in Austria for a similar approach and interest was raised. JOIN will also host workshops in Belgium and Germany to increase the reach of SecureHospitals.eu.

4.2. Workshops

INTERSPREAD Gmbh (INSP):

Title: How to promote a cybersecurity culture within your organisation?

Target Group: Healthcare managers and IT professionals

Format and agenda description: The workshops will include a comprised version of the topics of the summer school, seeking to provide local healthcare managers and their staff members working in leading IT positions, with the necessary knowledge on cybersecurity measures for decreasing vulnerabilities. Each of the event will include a one-day workshops organised in Vienna in German.

Time and Location: March, September 2020 in Vienna, Austria

Erasmus University Rotterdam (EUR)

Title: Summary of the MOOC in Dutch

Target Group: Mixed groups

Format and agenda description: EUR will partner with JOIN at the workshops in Brussels. Additionally, JOIN and EUR aim to arrange a workshop for Johanniter International branch that is based in the Netherlands. If possible and where desired, EUR will assist EAN with local workshops in the Netherlands if these are requested by one of their allied organisations.

TIMELEX (TLX):

TLX will contribute to activities co-organised with other projects – with the aim of fostering synergies between different EU project within the same topic – in hosting webinars on topics that involve training, awareness raising and human-oriented solutions to tackle cybersecurity challenges. Preliminary plans include co-hosting two webinars: 1) The first in cooperation with the projects Cyberwatching.eu and PANACEA 2) The second providing a webinar for the International Society for Telemedicine and eHealth.

More details will be available after clearance with other projects.

Fundació Privada Hospital Asil de Granollers (FPHAG):

Workshop 1 – Title: Workshop 1 - Is a connected Hospital secure?

Target Group: open enrolment approach of healthcare and administrative staff

Format and agenda description: The aim of the Workshop 1 from FPHAG is to raise awareness about the cybersecurity dangers and potential solutions of connected hospitals. Workshop 1 is divided into three parts: Lecture, Demo and Working session. First, an explanation will be given to the participants about the most relevant cybersecurity threats of a connected hospital. Once the participants have been introduced to the fundamental cybersecurity threats, a hacking demo will be performed to the participants to show them the easiness of being successfully attacked. Finally, a working session approach will be delivered in order to emphasize the available good practices to prevent the threats, while responding questions from the participants. The total workshop duration will be around 2 hours and be delivered in the form of a workshop including a lecture, demo and a working session.

Time & Location: July at FPHAG's facilities (Granollers)

Workshop 2 – Is a connected Hospital secure?

Format and agenda description: The evaluation of Workshop 1 will help refine and develop further the concepts and deliver a format of Workshop 2.

Target Group: Depending on the evaluation results of Workshop 1, Workshop 2 can potentially be addressed to a more specific healthcare and administrative staff group. Possibly the particular group can be picked directly for enrollment in order to have in the Workshop representative roles identified as more urgent or with more significant impact of taking Workshop 2.

Time & Location: October at FPHAG's facilities (Granollers)

COOSS Cooperativa Sociale Marche (COOSS):

Title: Cybersecurity Awareness

Training event 1

Target Group: the training will be addressed to the coordinators of COOSS structures (RSA, nursing homes, protected homes, daily centres) and to the home care service managers.

Agenda description:

The training will aim to:

- present the most frequent cyber-risks they can meet in the performance of their daily work;
- recognise the vulnerabilities of their system and behaviours;
- explain the most common wrong or dangerous behaviours on the staff part;
- explain measures and behaviours to be adopted;
- present possible technical solutions linked to the specific risks;
- illustrate the main GDPR requirements, mainly in terms of privacy and data management, and the potential consequences of their violations.

Time and location: May 2020, COOSS premises, Ancona, Italy

Training event 2

Target Group: The training will be addressed to the workers involved, with different roles, in the provision of social services. They will be social workers, nurses, assistants, psychologists and educators

Agenda description:

The training will aim to:

- present the most frequent cyber-risks linked to the performance of their daily work;
- recognise the vulnerabilities of their behaviours;
- explain measures and behaviours to be adopted;
- present the risks connected to the use of the different devices they use for their work;
- provide tips and straightforward advice on how to recognise a cyber-risk;

The training will be supported by illustrative material, exercises and case studies.

Time and location: October 2020, COOSS premises, Ancona, Italy

Arbeiter-Samariter-Bund Österreichs (SAM):

Title: Cybersecurity Awareness

Target Group: Health care staff at SAM

Format and agenda description: SAM is planning to train all target groups - management, administrative staff, regional coordinators, quality assurance, nurses, nursing assistants, home care workers, and visiting service. The first training classes, each with around 20 participants, will take place in autumn 2020. Rollouts are planned for the following months, with the goal to train, by and by, all of our staff (currently about 280 persons). With a vast majority of our staff using mobile devices (smartphones equipped with operational planning software, and processing data of

approximately 1000 of our clients), one important focus of our pieces of training will lie on cybersecurity issues regarding those tools. In addition to that, data protection of our clients and staff will be regarded from a more IT-centered perspective. The exact contents still have to be defined by our IT-experts, after analysis of the most common cybersecurity problems arising from working routines in-home care and nursing. The estimated duration of each training will be three hours; adjustments are possible depending on the final volume of information provided. The dates of training are still open, given that several parameters (availability of local trainers, staff and classrooms) have to be taken into account. As training locations, we will choose one or more of Samariterbund's buildings in Vienna.

Time & location: to be announced, 2020, Vienna, Austria

Johanniter International (JOIN):

Workshop 1 – Title: Cybersecurity Awareness

Target Group: Healthcare staff

Format and agenda description: SecureHospitals.eu Workshop 1 from JOIN is focused on raising awareness for cybersecurity in people, who are working in the field of health care. Within the last 20 years, the way we work in care has changed dramatically. Especially in the administration and the handling of health records, new challenges raised. With these challenges, also new threats developed. In this workshop, participants will learn about the potential threats of the cyber-world and how to avoid them. With a small tabletop exercise, the sensibility and understanding for cybersecurity shall be put into practice. Identification of threats, understanding of potential, proper reaction.

Time & Location: 17 April 2020 in Berlin, Germany

Workshop 2 – Title: IT to Healthcare

Target Group: Healthcare managers

Format and agenda description: SecureHospitals.eu Workshop 2 from JOIN is focused on raising awareness for cybersecurity in people, who are working in the field of health care. Within the last 20 years, the way we work in care has changed dramatically. Especially in the administration and the handling of health records, new challenges raised. With these challenges, also new threats developed. In this workshop, participants will learn about the potential threats of cybercrime and attacks. Healthcare manager and team manager will learn how to avoid them in their teams and for themselves. With a small tabletop exercise, the sensibility and understanding for cybersecurity shall be put into practice. Identification of threats, understanding of potential, appropriate reaction.

Time & Location: 12 June 2020 in Brussels

European Ageing Network (EAN)

Workshop 1 – Title: "Raising awareness for cybersecurity in hospitals"

Target Group: primarily DPO and healthcare / social services staff; Directors of social care facilities and hospitals on European level

Format and agenda description: Participants will learn about the potential threats of the cyber-world and how to avoid them. Ethical hacking will be introduced. Threats in the administration and the handling of health records. The format of the workshop will include lectures and a workshop for 15 - 20 participants.

Time & Location: July/August 2020, Czech Republic

Workshop 2 – Title: "Raising awareness for cybersecurity in social care facilities"

Target Group: primarily DPO and healthcare / social services staff; Directors of social care facilities and hospitals on European level

Format and agenda description: Participants (primarily directors and administration staff of social care facilities) will learn about the potential threats of the cyber-world and how to avoid them. Ethical hacking will be introduced. Threats in the administration and the handling of health and social records. The format of the workshop will include lectures and a workshop for 15 - 20 participants.

Time & Location: October 2020, Czech Republic

Workshop 3 – Title "Raising awareness for cybersecurity in social care facilities"

Target Group: DPO and healthcare / social services staff; Directors of social care facilities and hospitals on European level

Format and Agenda description: Participants (primarily directors and administration staff of social care facilities) will learn about the potential threats of the cyber-world and how to avoid them. Ethical hacking will be introduced. Threats in the administration and the handling of health and social records. The format of the workshop will include lectures and a workshop for 15 - 20 participants.

Time & Location: October 2020, Spain

Workshop 4 – Title "Raising awareness for cybersecurity in social care facilities"

Format and Agenda description: Participants (primarily directors and administration staff of social care facilities) will learn about the potential threats of the cyber-world and how to avoid them. Ethical hacking will be introduced. Threats in the administration and the handling of health and social records. The format of the workshop will include lectures and a workshop for 15 - 20 participants.

Target Group: DPO and healthcare / social services staff; Directors of social care facilities and hospitals on European level

Time & Location: November 2020, Austria

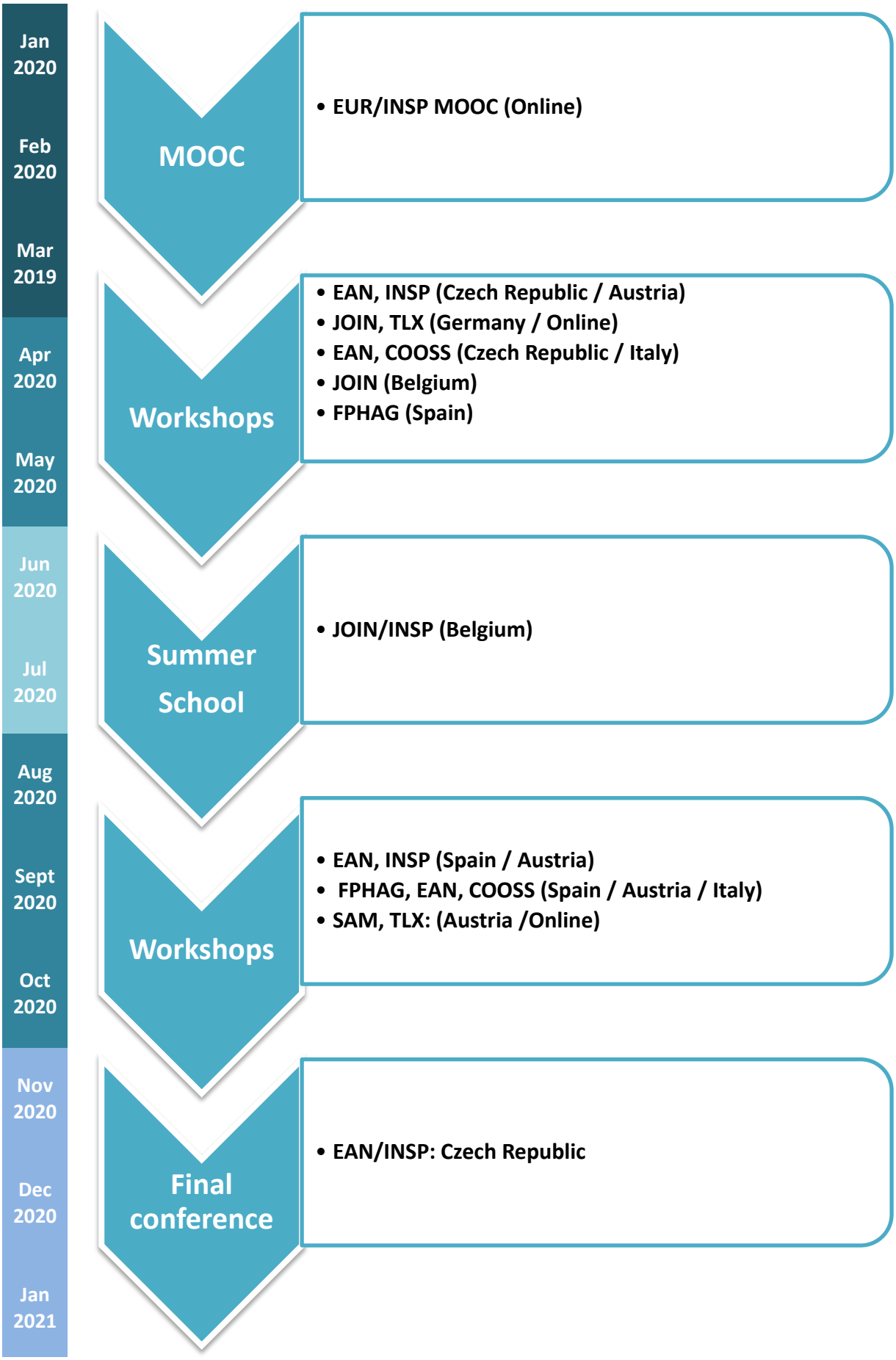

Figure 1: Training activities timeline

5 Conclusion

The program and timeline are outlined and can be used for further communication of the project. The schedule will be available on the website and all partners may use this document as a reference and invitation to third parties. With the temporary schedule of the Summer School, all content strings relate to the train the trainer concept.

The MOOC is positioned and framed for the next steps and ready to be explored by users. With the regional workshops, the impact and potential of uptake of results are increased. Especially the commitment of Arbeiter Samariter Bund in Austria is a guarantee for the direct impact of SecureHospitals.eu in the healthcare industry. This deliverable is a piece of cooperative work and mirroring the cooperation of the partners. The cooperation will be ongoing until the end of the M12 in order to conclude the next planning steps in terms of more specific agendas, promotion of the events and the recruitment of participants and speakers to all of the training formats. The outcomes of each of the planned training activities will be reported in dedicated deliverable reports for each of the formats (D5.4 for the MOOC; D5.5 for the Summer School; D5.6 for the workshops and webinars).

© 2019 SecureHospitals.eu | H2020-SC1-FA-DTS-2018-1| 826497

6 References

SecureHospitals.eu Project deliverable 3.3 (2019) ‘State-of-the art and potentials for eLearning and Approaches in Cybersecurity in hospitals training report’