SECUREHOSPITALS.EU

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

Kick-off Meeting Report

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 Aging Network, Luxembourg (EAN)

DELIVERABLE DESCRIPTION

Number:	**D1.2**
Title:	**Kick-off meeting report**
Lead beneficiary:	**INSP**
Work package:	WP1
Dissemination level:	Confidential (CO)
Type	Report (R)
Due date:	31.01.2019
Submission date:	31.01.2019

Authors: **Stela Shiroka,** INSP

Contributors: **All Partners**

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

TABLE OF CONTENT

EXECUTIVE SUMMARY

The SecureHospitals.eu project seeks to raise awareness on cybersecurity risks and protection opportunities for healthcare organisations and professionals. Through the creation of tailor-made training packages, application of different training approaches and creation of an online community of practice, the project will boost the level of training in cybersecurity for healthcare professionals in Europe. Thus, contribute to decreased human errors and more solid strategies against external attacks.

To bring forward the collaboration of the consortium partners in fulfilling the project aims, the project kick-off meeting was organised in Vienna between 24.01.2019 -25.01.2019, with the participation of representatives from all 8 consortium organisations. All partners provided valuable inputs regarding the overall project, the different objectives, tasks and challenges.

During the first day of the meeting, all staff members had the chance to gain a more in depth understanding on the profiles, expertise, contacts and networks of the rest of the team and the respective organisations. The project coordinator, INSP, gave an overview of the project and its structures including the overall concept, main objectives and expected impacts, overall methodology etc. Following the initial introduction of the overall project, all work packages including their tasks and deliverables were presented by their respective leads. Open questions concerning these tasks and deliverables were discussed and collected for further discussion on the next day of the meeting.

On the second day of the meeting, two intensive working sessions sought to collect inputs from all partners regarding upcoming deliverables especially in WP2 – WP5. Questions collected from the first day as well as new questions were discussed by the consortium in order to gain a clear understanding of the content, reach an agreement on certain topics and distribute responsibility of the tasks and deliverables.

An overall explanation on project management and coordination and creation of the communication and collaboration mechanisms were addressed in both days. The coordinator held a presentation describing all the guidelines put forwards the European Commission and explained how the consortium internal rules of communication and collaboration. Moreover, the distribution of quality assurance responsibility and decisions regarding upcoming meetings were completed.

1. Introduction

The SecureHospitals.eu kick-off meeting took place from Thursday, January 24th to Friday, January 25th 2019, at Fleming's Conference Hotel Wien in Vienna, Austria. Representatives of all 8 participating institutions were present at the meeting.

On Thursday the emphasis was on the overall introduction of the members of the consortium, their motivations and expectations on the project, and on providing an overview over the project. In this context, leaders of each work package presented the work package's objectives with their respective tasks and deliverables. Open questions concerning these tasks and deliverables were collected for further discussion. Each work package leader presented the tasks, and guided the consortium through the discussion of particular tasks and open questions. The target of these sessions was to gain a clear understanding of the content of the tasks and deliverables, to produce schedules and reach agreements about the open questions discussed on previous day. The roles and responsibilities of each partner in the upcoming tasks were discussed and clarified, and the initial steps for producing the first project deliverables were formulated. In the last session of the 1st day, the project coordinator INSP, described the procedures and obligations of all partners towards WP1, as well as the communication and coordination structures and tools, the reporting and project management structures, etc.

On Friday, the consortium started working more in depth on the upcoming tasks, presenting the conceptualisations and work carried out so far and defining the further steps towards the finalisation of the first deliverable reports.

2. Participants

All 8 consortium partners attended the kick-off meeting with a total number of 16 participants listed in the table below.

No.	PARTICIPANT	ORGANISATION	COUNTRY
1	Peter Leitner	INSP	Austria
2	Stela Shiroka	INSP	Austria
3	Jason Pridmore	EUR	Netherlands
4	Tessa Oomen	EUR	Netherlands
5	Yung Shin Van Der Sype	TLX	Belgium
6	Javier Morate	FPHAG	Spain
7	Marc Jofre	FPHAG	Spain
8	Francesca Cesaroni	COOSS	Italy
9	Marco Antomarini	COOSS	Italy
10	Sigrid Panovsky	SAM	Austria
11	Hermine Freitag	SAM	Austria
12	Wolfgang Fessl	SAM	Austria
13	Georg Aumayr	JOIN	Belgium / Austria
14	Eva Pelgen	JOIN	Belgium
15	Karel Vostrý	EAN	Luxembourg / Czech Republic
16	Jiří Horecký	EAN	Luxembourg / Czech Republic

3. Agenda

Day 1	Thursday, January 24, 2019	09:30 – 18:00
09:30 – 10:00	***Get together***	
10:00 – 10:15	**Welcome and agenda presentation (**INTERSPREAD)	
10:15 – 11:15	**Introduction of the consortium partners and staff members** (5' each partner organisation)	
11:15 – 11:30	***Coffee break***	
11:30 – 12:30	**Project overview and structures** (INTERSPREAD) - Facts and figures - Background and concept - Project goals, timeline, targets to fulfil (KPIs) - Project Structure & Interconnections of tasks - Management structure	
12:30 – 14:00	***Lunch***	
14:00 – 16:00	**Short Presentations by WP Leads (Part 1)** 30' each - **WP2 INVOLVE:** Hospitals and Practitioners via an Online Awareness and Information Hub – by **COOSS** - **WP3 AGGREGATE:** Existing Knowledge and Approaches on Cybersecurity in Hospitals – by **EUR** - **WP4 CREATE:** Structured Training Schemes and Curricula for Hospital Staff & Trainers – by **FPHAG** - **WP5 BOOST:** Training Initiatives in Hospitals and Integration of Providers and courses – by **JOIN**	
16:00 – 16:30	***Coffee break***	
16:30 – 17:00	- **WP6 COMMUNICATE:** Awareness Raising on Project Activities and Promotion of the Hub – by **EAN**	
17:00-18:00	**WP1 MANAGE:** Project management and Coordination **QUALITY ASSURANCE**	
20:00	***Evening program:*** *Dinner*	

Day 2	Friday, September 25, 2019	09:00 – 17:30
09:00 – 10:00	**Program and Aims for Day 2 (INTERSPREAD presents the Outcomes)** Project Outcomes most relevant for each project partner *(each partner contributes and this will be circulated before the meeting)*	
10:00 – 11:00	**Working Session 1** (World Cafe) **Task 2.1:** Collect relevant stakeholders, setup the expert and advisory board, create an involvement roadmap and an engagement **Task 5.1** Develop a training and engagement strategy to include specifically targeted audiences and means of training delivery **(JOIN)** - Strategy and orientation presentation **(COOSS)** - Synergies between Community Building and the OIH **(INSP)** - Stakeholder Mobilisation **(EAN)** - Questions / Inputs / Discussion Participants: All Partners	
12:30 – 13:30	***Lunch***	
13:30 – 15:30	**Working Session 2** - **Task 3.1:** Map existing knowledge, courses and training programmes by collecting and reviewing publications, toolkits and other materials **(EUR)** - **Task 4.1** Collect and assess existing courses and training programs on cybersecurity across various domains **(FPHAG)** - **Wrap-Up** Participants: All Partners	
15:30 – 16:00	***Coffee break***	
16:00 – 17:30	**Outcomes and Synthesis from the Working Sessions** - General direction, strategy and schedule - Tasks and Deliverable Outlines - Open issues and discussion	
17:30	***End of Day 2***	

4. Meeting Minutes and slides

4.1 Day 1 (24.01.2019)

Welcome and agenda presentation

The kick-off meeting began with a short introduction of the project and presentation of the agenda by INSP. All consortium partners (12 partners from 8 different countries) were represented at the kick-off meeting. A collection of material which included the project-plan, a list of deliverables and a summary of the main aspects of the project was handed out to all participants.

Introduction of consortium partners

After a short presentation of the activities and the staff of INSP and the SecureHospitals.eu project, the partners presented their organisations and introduced their staff members.

EUR – Erasmus Universiteit Rotterdam: EUR is an internationally oriented research university with a strong social orientation in its research and teaching. It is ranked in the top 100 universities globally and has over 28.000 students, and 3500 faculty and staff. The project will be carried out by the Erasmus Research Centre for Media, Communication, and Culture (ERMeCC) which focuses on 1) Interdisciplinary research on media, communication and culture 2) Empirical, interdisciplinary and comparative research 3) MAPS research cluster focused on personal, social, and ethical consequences, and (cyber) security threats of mobile and interconnected media technologies and devices. The project members include Jason Pridmore, Assistant Professor at the Department of Media and Communication who is a Principle Investigator for the Mapping Mobile Privacy Project (Dutch research funding), Project Exploitation Manager and Data Security Manager: BIM SPEED Project (H2020). His research focus is on: (Cyber)Security, Information Communication Technology, Surveillance, Privacy, Data Ethics, Marketing. The second staff member to join the team officially in February is Tessa Oomen, Researcher at Department of Media and Communication. Previously she acted as research and education assistant at the Institute of Security and Global Affairs of Leiden University and has Master's degree in Crisis and Security Management (MSc) focusing on Cybersecurity. The overall focus of EUR for SecureHospitals.eu is on cybersecurity in practice, use of media and communication tools to change everyday practices, education innovation and connecting with relevant stakeholders in the Netherlands.

TLX - TIMELEX: Timelex is a leading niche law firm specialised in the legal aspects of information technology, privacy and data protection, intellectual property, and media & electronic communications. Its main expertise includes: 1) International, European and national legal framework in the area of privacy and data protection, 2) Legal issues related to intellectual property issues related to ICT and innovation, 3) Specialized legal expertise in the domain of information security. Similar projects and FP7/Horizon 2020 experience (limited to the most recent ones): HERMENEUT: External Ethics Advisor; CUREX addresses comprehensively the protection of the confidentiality and integrity of health data by producing a novel, flexible and scalable situational awareness-oriented platform. CUREX aims to be fully GDPR compliant by design. At its core, a decentralised architecture enhanced with a private blockchain infrastructure ensures the integrity of the risk assessment process and of all data transactions that occur between the diverse range of

stakeholders involved; KONFIDO aims to leverage proven tools and procedures, as well as novel approaches and cutting edge technology, in view of creating a scalable and holistic paradigm for secure inner- and cross-border exchange, storage and overall handling of healthcare data in a legal and ethical way both at national and European levels; AEGLE aimed to develop a European platform (Biolytica) for Big Data analytics in the health sector. Timelex mobilised its network of national legal correspondents to deliver an overview of the legal rules applicable to (re-)using patient data for research purposes in 30 European countries. The participant staff members from TLX include Prof. Dr. Jos Dumortier, Attorney at law at Timelex (founding partner) | Honorary professor in IT law (KU Leuven), founder of the Interdisciplinary Centre for Law and Information Technology (ICRI – KU Leuven), regular expert for the Belgian government and the European Commission, Advisor for foreign governments and for private organisations, member of several boards and committees and long list of publications and with an expertise in numerous projects. The second staff member present during the meeting is Dr. Yung Shin Van Der Sype who is also an attorney at law at Timelex, guest lecturer KU Leuven and Data Protection Officer. She was the main contact person for research ethics and legal issues in several FP7/H2020 projects, and external ethics advisor several projects. She is an advisor for the Belgian government, for the European Commission and for private organisations, and member of several boards and committees and long list of publications. TLX's motivation on the project includes: scientific development of the Timelex expertise and gaining more insight in the particularities of the healthcare sector. As such it will Assist the consortium to integrate legal competence in the SecureHospitals.eu solutions and in dealing with legal questions that may arise during the whole duration of the action.

FPHAG: Fundacion Privada Hospital General De Granollers: is located in Spain and includes 1600 health professionals, has 8 operating spaces and reaches a population of 400.000. Its involvement projects for the development of innovative technological solutions includes projects such as: I-DONT-FALL Integrated prevention and detection solutions tailored to the population and risk factors associated with falls; and RADI: Robots in assisted living environments: Unobtrusive, efficient, reliable and modular solutions for independent ageing H2020-PHC-19-2014 (Personalising Health and Care). Its goals are to improve the quality of the services provided in the scope of the hospital and gain additional insights on edge technologies for supporting Health Services. The relevance of the project for the organisation includes: Raising awareness on cybersecurity; challenging industry, research institutions/Universities and medical centers to: ensure timely communication of information, improve patient data safety in hospital and after discharge, promote active patient involvement in his health record history. The team of FPHAG working on the project include Dr. Diana Navarro who acts as the project lead and head of the project board. Next to Diana, Marc Jofre will be leading the project management, IPR, dissemination, communication and coordination. The principal investigators for the topics of the relevance are Ramon Romeu and Toni Alonso who will also be supported by Javier Morate from the technical team. Their next goals include: building solid training schemes and materials for hospital professionals, define training concepts and collecting current state-of-the-art, defining quality standards etc.

COOSS – Cooperativa Sociale COOSS Marche Onlus Societa Cooperativa per Azioni: COOSS is a social services provider organization which provides assistive and educational services to disadvantaged targets, manages residential settings, daily centres, communities, provides home care services, operates mainly within the regional area. It has 2900 member-employees serving to 8680 users, among which elderly, disabled people, mentally impaired, drug addicts, migrants etc. within 29 private residential settings. As such it hold three following certifications SA8000 (Social

Responsibility), ISO9001(Quality Assurance) and OHSAS18001 (Safety on the working places). The COOSS Department of Research and Training was born in 1993, it counts nowadays14 staff units; it iss an accredited VET body, is registered at MIUR as Research Centre, and it has run RIA projects under AAL, FP, ICT-PSP, H2020, addressed to frail targets. Its main roles included: user needs analysis, usability assessment, scenarios definition, pilots' management. It is also experienced in testing AT solutions to improve the users' quality of life. COOSS is facing the complexity and risks linked to data management because of: H2020 running projects, where data-gathering and treatment are involved and digitalization of its services. Their current activities include: 15 national and European projects running; a training course for Web experts running (with a section devoted to cybersecurity; and new courses for OSS (Socio-Sanitary Operators), a profile enabling to work in health and care structures. The research interest are on experimenting solutions beneficial to our targets and/or our organization and guaranteeing our customers' data protection. The training modules resulting from SH, will be very relevant for its workers and existing training courses. From SecureHospitals.eu the team also expects to gather the opinion of health professionals on data security issues (in terms of needs, barriers, perceived facilitators); involve different targets in the experimentation of the training modules; and transfer the SH modules in different training contexts after the end of the project. The main project team will be composed by Francesca Cesaroni who will be in charge opf project coordination and process development and Marco Antomarini who will contribute with his technological competences and research expertise.

SAM- Arbeiter-Samariter-Bund Wien Gesundheits-und Soziale Dienste Gemeinutzige GmbH: Samaritan Austria has been founded in 1927 and enlarged in response to social needs and in conscience of ethical issues. It includes 150.000 members and supporters and a staff of 5.000 volunteers and employees in various fields of activity. Its mission is to provide help and support in an individually adapted and socially responsible way. Sam offers: Ambulance services: Paramedics, Critical care Paramedics; Disaster relief & Development cooperation; Rescue dogs, Drinking water purification; Senior citizen assistance: Home Care services, Meals on wheels; Emergency/Panic alarm services; Homeless shelter: Social assisted living; Refugee relief; Social markets: Good value food; Trainings & Youth groups: First Aid, Water rescue, Home health care; Mobile services (Nursing, Home care, Visiting services); Sheltered housing communities for older adults; Active Assisted Living. SAM participated in various projects such as Fearless and EnterTrain and is interested in technological innovation for older adults. The SAM team is composed of Wolfgang Fessl who is the Head of the IT department, Hermine Freitag who is the Head of the Home Care Department and the Sigrid Panovsky who acts as the Project Assistant.

JOIN – Johanniter International: JOIN is an international network of 17 St John charity organisations and the 4 Orders of St John facilitating cooperation at European and international levels. Its areas of activity include: First Aid (provision and training), Ambulance service, Patient transport (incl. internationally), Hospitals, Youth work, Elderly Care, Care for people with disabilities, People in Need, International Humanitarian Aid, Disaster Management. In continental Europe the organisations are known as Johanniter, while in the UK, Jerusalem and other areas with the name of St. John. JOIN's focus is on the establishment of expert groups/ Working Groups (WG), exchange and cooperation between members & international practitioners in the health sector, and clinical WG: drafting the very first European-wide First Aid Standards. The JOIN team is led by Georg Aumayr, M.A. Communication Science, Head of R&D at Johanniter Austria; Research: Information Technology and Society, Health Data Processing, Biomedicine, Health Care and Prevention with experience in some EU projects, i.e. SOCIALCARE (AAL), EUinAid (Erasmus+); Joachim Berney, M.A. Political Science,

General Manager of JOIN and Eva Pelgen, B.A. Intercultural Management and Communication, JOIN EU Officer; who has research experience in Intercultural Competence, Diversity Management and worked in the DIVERSE project (European Integration Fund) and EUinAid (Erasmus+). JOIN's motivation for making SecureHospitals.eu a successful project includes: Reduce cyberthreats in European health care organisations and for the health activities of JOIN members (hospitals, health applications); and increasing, learning from and contributing to the network and community of practice dealing with interconnective devices and cybersecurity in the health sector. The most relevant project outcomes for the JOIN team are: the Online Awareness and information Hub and accelerated exchange and collaboration; Trained professionals that are aware of the risks in cybersecurity and pass on their knowledge; Easily accessible tailored training material and approaches; For the success of SecureHospitals.eu JOIN can provide: Access to our network of health and care professionals, trainers and medical experts and their affiliated followers ensuring connection and dissemination of the project; Targeted outreach to end-users/ practitioners trough international and local communication platforms and tools; Contact in Brussels with relevant European organisations; and Johanniter's > 1'000 years of experience in health and care.

EAN – European Ageing Network: The EAN groups more than 10.000 care providers across the European continent. Members represent all types of organizations and individuals active for older persons and all types of ownership including for profit, not-for-profit and governmental organizations. It is their vision and mission to improve the quality of life for older persons and support them in making each day a better day for by providing high quality housing, services and care. It is present in 28 European countries. With EAHSA well represented in North-West Europe and EDE in the South-East, the combination makes of the European Ageing Network a truly pan-European organization. The headquarters of the organisaiton are located in Luxembourg, another head office is in Belgium and the administration office is in the Czech Republic. The team has participated in more than 9 projects and is owner of vocational training certificates and co-owner of e-Qalin, a practical and user-friendly quality management model tool which examines the services provided in the institutions and their effectiveness in regard to the satisfaction of all those involved. The primary team member of EAN is Karel Vostrý – EAN Executive director, former director of nursing home, director of CRA UZS ČR with a background in economics. The second member of the team is Jiří Horecký – EAN president, President of APSS ČR, UZS ČR and Vicepresident FESE. He has a Background in Economics and MBA in Public Law.

11:30 Project overview and structures

INSP gave an overview of the SecureHospitals.eu project's facts and figures by going through the overall concept of the project and the consortium map.

The main objectives of the project were elaborated with special emphasis on the timeline for the tasks to be fulfilled within each given work package (WP). Interdependencies between the work packages were highlighted pointing out the importance of the WPs working closely together. Individual WP-orientated calls will be provided by INSP.

The first point of discussion was the Expert and Advisory Board, consisting of four experts from different countries. Other potential members were discussed and a plan for contacting them was made. All the partners were urged to check this. The importance of including different stakeholders was emphasised: Different stakeholders should know about the final project, so dissemination is a very important part of the whole project from an early stage on.

Next, the deliverables and milestone lists were introduced. The deliverables list contains a chronological list of all deliverables and responsibilities as well as related work packages. It was stressed that any partner should inform INSP as early as possible if something does not work as planned and a deadline cannot be fulfilled – open and regular communication with the partners is very important. Most of the deliverables are reports which can be submitted as PDF documents. Other deliverables are prototypes, newsletters etc. which can be submitted as zip-files, links etc. Some deliverables are confidential, i.e. nobody except the consortium is to see it (e.g. the kick-off meeting report), others are public (e.g. the project website). These possibilities should be considered beforehand. A draft version of every deliverable should be delivered before the official deadline to give all partners a chance of review and internal feedback. The milestone list is mostly important to the European commission and should give an overview to the partners.

The concepts, modules and strategy of the Open Information and Awareness Hub (OIAH) were described in detail. The development of this platform is covered by a single in the work packages, however the content created shall come from all other work packages and tasks feeding their results in it. It will also be the responsibility of all partners to produce rich content for the OIAH and mobilise their networks in using it.

Besides that, the training packages that should be offered to stakeholder were addressed. The importance of implementing also the 'train-the-trainer' concept was pointed out and the methodology of all training was discussed. Especially the methodology and type of the MOOC, as the most ambitious and challenging part of WP5 was discussed in detail and some initial plans were made.

Furthermore, the project's expected impacts were presented. KPIs are up to be defined and should be discussed in the particular work packages – what could be useful, what is realistic in the project, which can't be reached? This will also help to communicate the project to the Commission.

Communication and dissemination activities, and their distinction, were stressed as critical activities to carried out by all partners for contributing to the project success. Moreover, the means of measuring the dissemination activities of each of the partners were presented. A communication plan including digital communication templates, awareness sheets, posters, factsheets, guides and booklets etc. shall be created.

The partners should also reflect what is needed and practical and communicate research in a way that is understood by non-specialists. To create meaningful project identity materials, the inputs of all project partners were gathered and a new project logo will be created and relevant images will be chosen for the project website, social media channels and all dissemination materials.

First, INSP introduced the project-website and explained its (planned) content:

- Like every project website for Horizon 2020 the website only provides basic information.
- There is a public version and a closed section; all public deliverables will be published on the (public) website, as well as factsheets and dissemination material (both digital and downloadable).
- The project website contains the consortium numbers and descriptions about and links to every member of the consortium.
- Most of the information available at the moment is congruent with what was written in the proposal.
- The project website will be made public by the end of January 2019.
- There will be a dissemination package like a factsheet with all important information made available as early as possible. All material will be available digital but also downloadable for

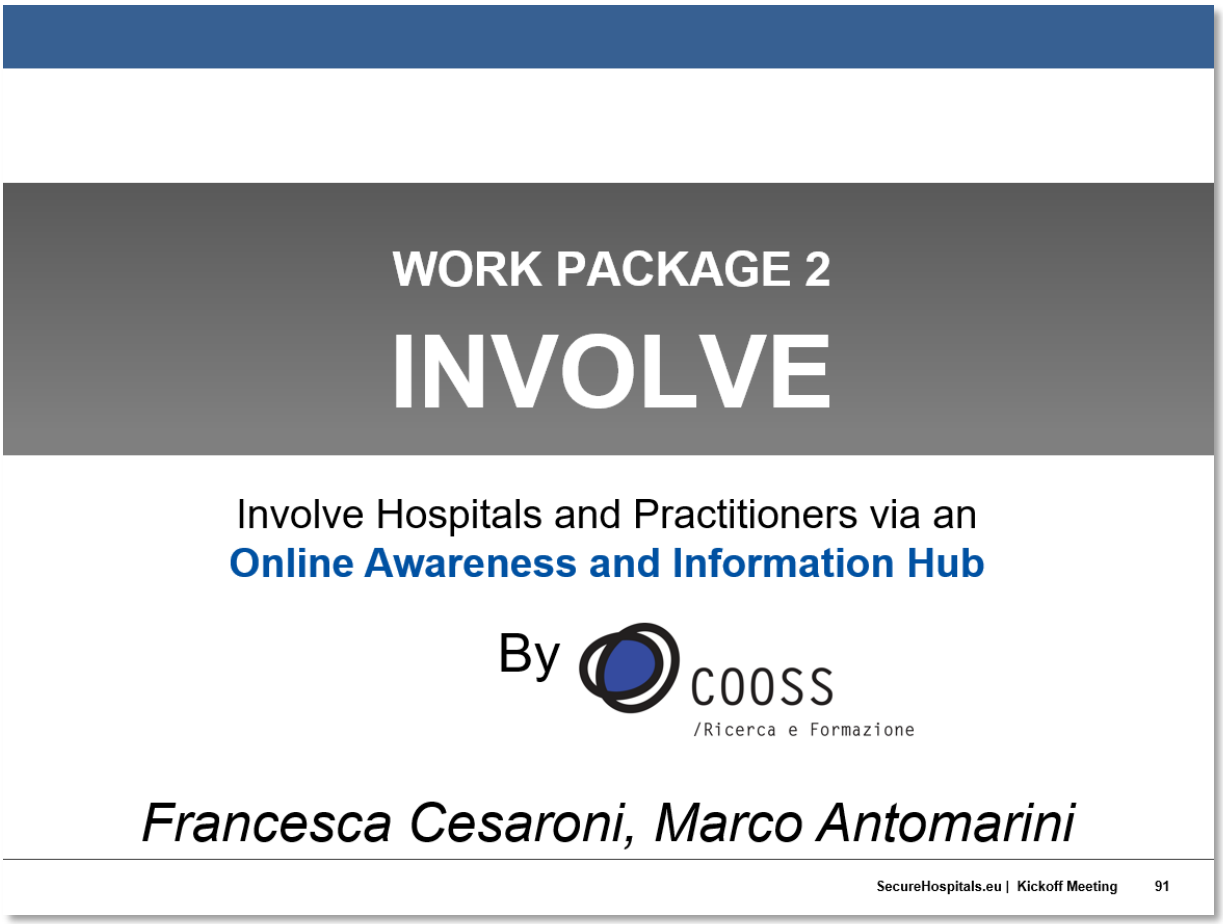
professional printing services; each partner also has some budget for printing and can use the provided material.
- There are also links to social media channels (which are secured but not yet established), there will also be a button to sign up for a newsletter (most likely on the homepage).
- There will be an open and a closed section.
- All feedback and inputs concerning the project website should be given to INSP.
-

After this short introduction the consortium was asked to give feedback and gather ideas on (1) the project identity, (2) digital awareness sheets and (3) on the web platform (modules and features).

Ideas for project pictures:

- Hospital building, shield, academy/training sign, medical people with technology, hospitals and tech, security lock, medical person fighting a Trojan etc.,

WP2: INVOLVE: Hospitals and Practitioners via an Online Awareness and Information Hub **– by COOSS**



Duration: 10 MONTHS

Partners involved:

- **COOSS – 4PM**
- INSP – 5PM
- EUR – 2PM
- EDE – 2PM
- FPHAG – 2PM
- JOIN – 1PM
- SAM – 1PM
- TLX – 1PM

Tasks:

T2.1 Collect stakeholders
T2.2 Mobilise stakeholders
T2.3 Online Hub
T2.4 Promote synergies

WP 2
WP LEADER: COOSS

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 92

WP 2: OVERVIEW

WP Objectives:

1 – Involvement and integration of key stakeholders

- To *identify* the main stakeholders in cybersecurity in hospitals
- To *select* outreach and engagement activities
- To *bring together* research experts, content providers, technology specialists, legal experts, practitioner groups, other (?).

2 – To launch the Online Awareness and Information Hub – OAIH

WP Milestones:

M4 = Creation of the open ***online information hub*** completed

M3 = *Knowledge* aggregation completed **[????]**

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 93

WP 2: OVERVIEW

WP Objectives:

1 – Involvement and integration of key stakeholders

- To *identify* the main stakeholders in cybersecurity in hospitals
- To *select* outreach and engagement activities
- To *bring together* research experts, content providers, technology specialists, legal experts, practitioner groups, other (?).

2 – To launch the Online Awareness and Information Hub – OAIH

WP Milestones:

M4 = Creation of the open ***online information hub*** completed

M3 = *Knowledge* aggregation completed **[????]**

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 93

TASK 2.1: COLLECT RELEVANT STAKEHOLDERS, SETUP THE EXPERT AND ADVISORY BOARD, CREATE AN INVOLVEMENT ROADMAP AND ENGAGEMENT

- ***To identify and categorise groups of actors and stakeholders*** involved in the European cybersecurity in ***healthcare*** landscape.
- ***To create a roadmap for the mobilisation of stakeholders***, outlining potential areas of engagement, **involvement** strategies and **cross-fertilisation approaches**.
- ***To design and implement the*** **Online Awareness and Information Hub – OAIH, based on the information provided by the involved stakeholders.**

(Lead: COOSS, Participants: INSP, EUR, TLX, FPHAG, SAM, JOIN, EDE)

Period: M1-M3

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 94

TASK 2.2: MOBILISE STAKEHOLDERS AND TARGET GROUPS TO IDENTIFY CURRENT PUBLIC PERCEPTIONS, EXPERIENCES AND ATTITUDES ON CYBERSECURITY

Public consultations to obtain first hand information on the current status and attitudes on cybersecurity in hospital and care centres.

Objectives

To gather stakeholders needs, feedback and suggestions enabling the partnership to:

- Provide lessons learned (WP3),
- Define training curricula (WP4)
- Organize tailored workshops, knowledge cafés and webinars to deliver the knowledge to trainers and practitioners all over Europe (WP5).

(Lead: EDE, Participants: COOSS, JOIN, SAM FPHAG

Period: M2-M5

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 95

TASK 2.3: SET UP AN ONLINE AWARENESS AND INFORMATION HUB (OAIH) WITH MULTIFUNCIONAL MODULES AND CHANNELS ACCESSIBLE VIA OUR WEBSITE

Launch of the OAIH

What is it?

A meaningful collaboration and discussion space on the topic of cybersecurity in hospitals.

Expected functionalities:

•Adaptability and scalability (?) of modules;

•Facilities allowing constructive discussions and training delivery.

(Lead: INSP)

period (M5-M8)

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 96

TASK 2.4: PROMOTE STRONG STRATEGIES WITH THE WINNING SU-TDS-02-2018 PROJECTS TO ENHANCE PAN-EUROPEAN KNOWLEDGE EXCHANGE VIA THE OAIH

To establish strong communication and knowledge transfer links with these projects

HOW?

- Sharing analyses on cybersecurity in hospitals;
- Round table discussions (both via on-line and in-person modes).
- Joint workshops and events.

(Lead: INSP, Participants: COOS, EDE, EUR)

period (M5-M10)

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 97

TASK 2.1: METHODOLOGY: STRATEGY

STEP 1 : WHO
HEALTH/SOCIAL SECTOR
DIRECT BENEFICIARIES
INDIRECT BENEFICIARIES
INFORMERS/TRAINERS (ICT EXPERTS)

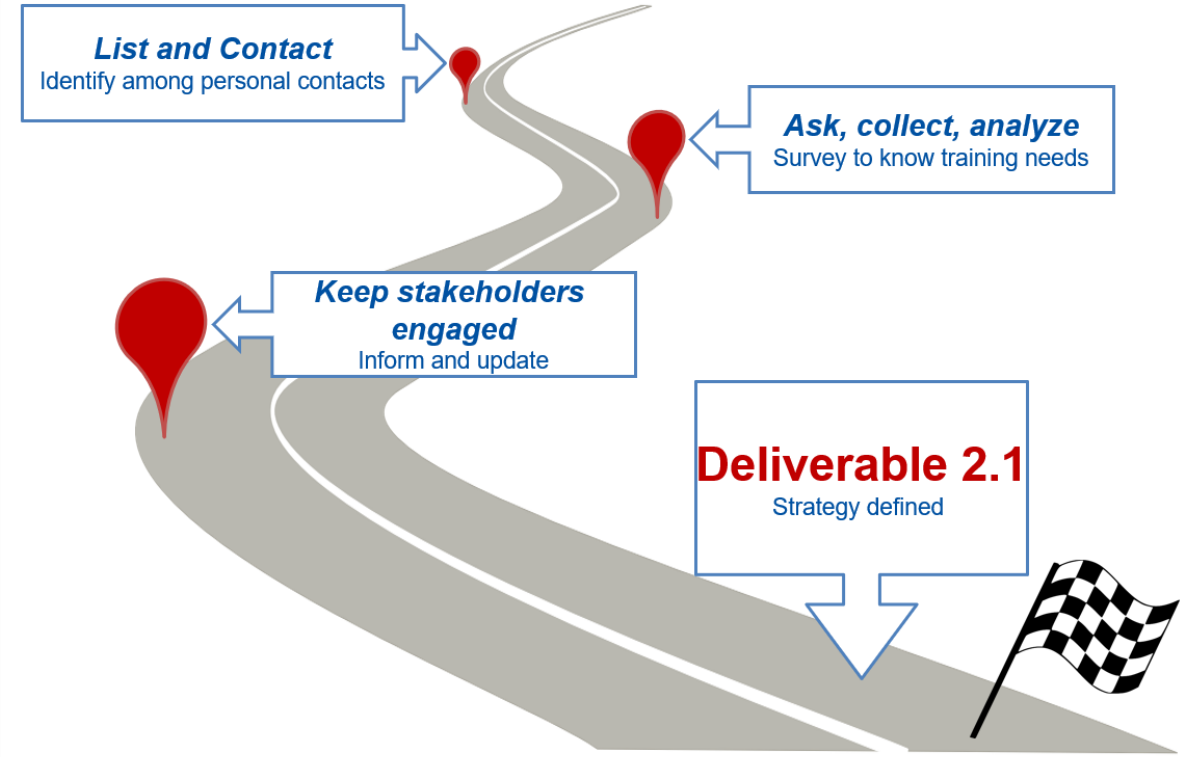
STEP 2 : WHAT
TRAINING NEEDS
STAKEHOLDERS INFRASTRUCTURES
CURRENT WORKING PRACTICES

STEP 3: HOW
SURVEY (QUESTIONNAIRE) TO GET INFORMATION **FOR US**
MAILING LIST, NEWSLETTER, SOCIAL , TO PROVIDE INFORMATION **FOR THEM**

COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 98

TASK 2.1: METHODOLOGY (ROADMAP)



COOSS /Ricerca e Formazione

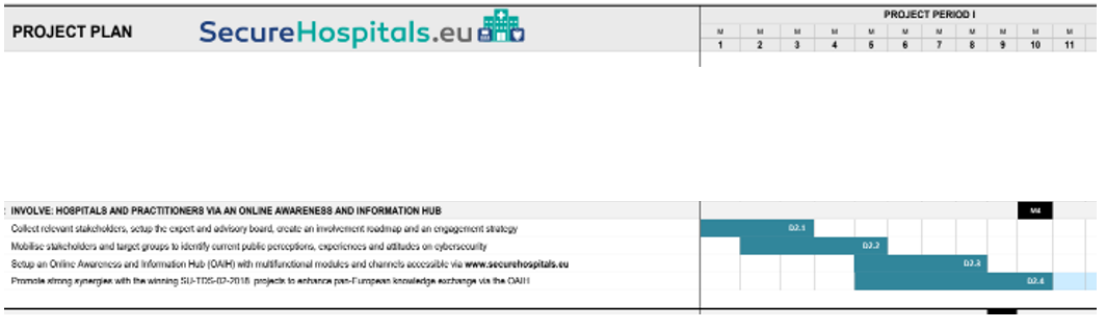
SecureHospitals.eu | Kickoff Meeting 99

WORK FLOW AND DISTRIBUTION

What are the commitment for the next months?

To be discussed and agreed on **Day 2**

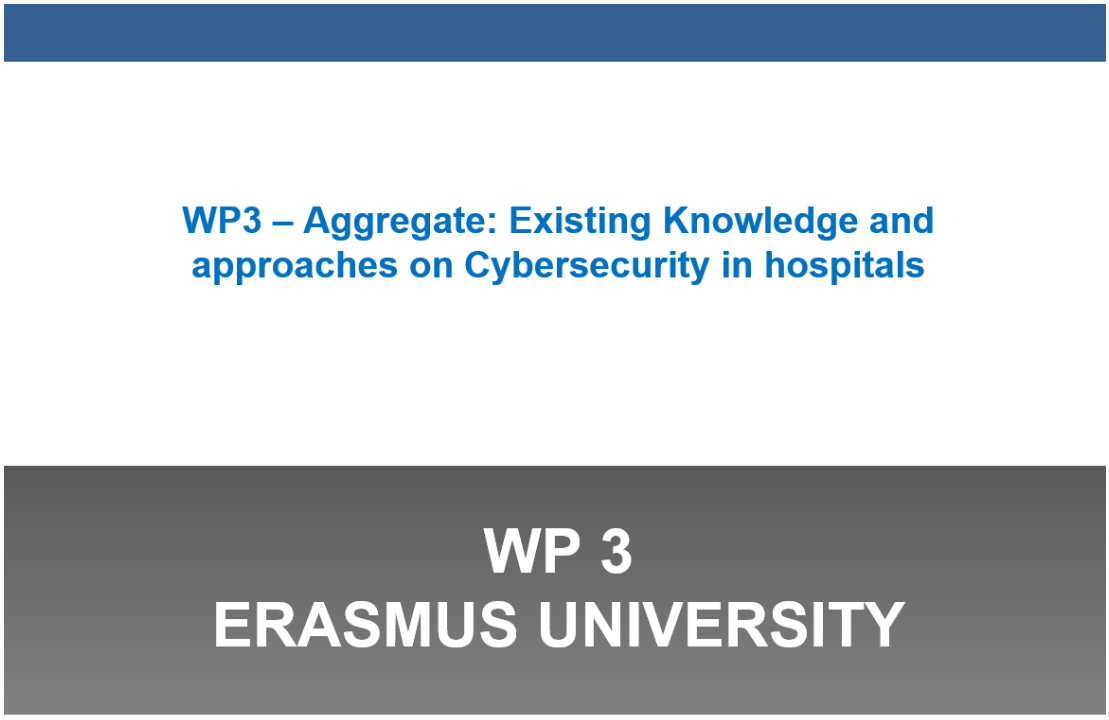
Commitment	Partners responsible	Deadline
TASK 2.1 – Del. 2.1	COO	February '19
TASK 2.2 – Del. 2.2	EDE	April '19
TASK 2.3 – Del. 2.3	INSP	July '19
TASK 2.4 – Del. 2.4	INSP	September '19



COOSS /Ricerca e Formazione

SecureHospitals.eu | Kickoff Meeting 100

WP3: AGGREGATE: Existing Knowledge and Approaches on Cybersecurity in Hospitals – **by EUR**



WP 3: OVERVIEW

- *Knowledge mapping of cybersecurity in EU hospitals* and health care organisations
  - Draw from EU projects and relevant activities to determine:
    - Key knowledge sources
    - Activities and embedded practices
    - Tools for education and training
- Prepare knowledge libraries for integration into online hub
  - Focus on categorisation for future use
- Observe implementation of ICT tools on training for cybersecurity
- Feed outputs into WP 4 and 5

SecureHospitals.eu | Kickoff Meeting 105

TASK 3.1: MAPPING KNOWLEDGE

Task title: Map existing knowledge by collecting and reviewing publications, toolkits and other materials
Lead – FPHAG; Participants – INSP, EUR, COSS, SAM, JOIN, EDE

- Collect, review and map knowledge sources
- Determine holistic view of cybersecurity within hospital/healthcare ecosystem
- Two foci
  - Map knowledge for *internal use* in the creation of training materials
  - Create a *library of mapped sources* to integrate into online hub

Deliverable 3.1: Cybersecurity in hospitals Knowledge Map (Month 6)

- Develop stakeholder map with sources, materials and relevance for further development
- Infographic of the ecosystem of cybersecurity in hospitals in Europe

SecureHospitals.eu | Kickoff Meeting 106

TASK 3.2: RELEVANT PROJECT IDENTIFICATION

Task title: Identify and collect European and international projects, initiatives and stakeholders to build knowledge on their learned lessons

Lead – JOIN; Participants – INSP, COOS, EDE, EUR

- Collect existing European projects, EU funded initiatives, major institutional developments
- Observe experiences and build on their lessons learned
- Exchange information with other actors and build synergies with their work

Deliverable 3.2: European project and stakeholders on cybersecurity in hospitals report (Month 7)

- Report on related projects and initiatives
- Identify synergies for SecureHospitals

SecureHospitals.eu | Kickoff Meeting 107

TASK 3.3: ICT TOOL ASSESSMENT

Task title: Assess the potential of ICT tools for training on cybersecurity in hospitals and provide the state- of-art of their application

Lead – INSP; Participants – EUR, TLX, FPHAG, SAM, JOIN, EDE

- Introduce eLearning and e-approaches to training
- Enable trainers build more successful course curricula
- Map ICT tools with a relevance to training
- Develop recommendations on the inclusion of specific technologies and eLearning methods

Deliverable 3.3: State-of-the art and potentials for eLearning and Approaches in Cybersecurity in hospitals training report (Month 8)

- Report on current practices and potentials for increased usage of existing/alternative approaches (MOOCs, Webinars, Game-based learning, m-Learning, communities of practices and other online communities etc.) or new developments

SecureHospitals.eu | Kickoff Meeting 108

TASK 3.4: BASELINE REPORT

Task title: Provide a baseline report structuring all knowledge and sources so that it is easily navigable and comprehensive by trainers and practitioners

Lead – EUR; Participants – INSP, FPHAG, JOIN

- Gather collected information and create baseline report
- Handbook of information to be included in the online hub
- Final review of relevant sources

Deliverable 3.4: Cybersecurity in hospitals Knowledge Baseline Report (Month 9)

- Baseline report as handbook with library of sub-sources ready to be implemented into the online hub

SecureHospitals.eu | Kickoff Meeting 109

DELIVERABLES AND MILESTONES OVERVIEW

Deliverable Short Name	Responsible Partner	Due
Cybersecurity Knowledge Map	FPHAG	M6
European projects and stakeholders report	JOIN	M7
eLearning Potentials report	INSP	M8
Cybersecurity Knowledge Baseline Report	EUR	M9

SecureHospitals.eu | Kickoff Meeting 110

METHODOLOGY AND PROCESS

Work with Task leaders to determine division of work

Task 3.1 Division
- Academic publications (EUR)
- Organisational White papers
- Industry solution papers
- Current toolkits

Task 3.2 Division
- European projects
- International projects
- Regional initiatives
- Stakeholder investments
- Corporate solutions

Task 3.3 Division
- Current training tools
  - Regional divide
- Potential Training tools and effectiveness

Task 3.4 Division
- EUR integrates D3.1, D3.2, and D3.3 into report
- WP task leaders to review integration process

SecureHospitals.eu | Kickoff Meeting 111

WP4 CREATE: Structured Training Schemes and Curricula for Hospital Staff & Trainers – by FPHAG

WP2-3 + WP4 + WP5-6] WP1

SecureHospitals.eu

WP 4
WP FPHAG

SecureHospitals.eu | Kick-off Meeting 113

Creation of new training material (M5)

- All training on cybersecurity in hospitals should:
  - comply with certain quality standards.
  - follow guiding materials to develop tailor-made courses.

SecureHospitals.eu | Kick-off Meeting 114

T4.1.- Collect and assess existing training courses and programmes on cybersecurity in hospitals across various domains

(Lead FPHAG, Participants: SAM, EUR, JOIN)

- Get the big **picture across regions** and **organizations** by:
  - updating collection of courses on the online hub (at least 50).
  - Benchmarking types of existing trainings (at least 3).

SecureHospitals.eu | Kick-off Meeting 115

T4.2.- Engage trainers and experts to map and understand needs and challenges in training for cybersecurity in hospitals

(Lead JOIN, Participants: SAM, EUR, EDE)

➢ Search for additional **inputs** from **trainers** and **experts** by:

- stakeholder interviews (at least 20).
- small workshops or focus groups (for trainers i.e. hospitals staff) (at least 2).
- Other methodologies will be considered if necessary (design thinking , ..)

SecureHospitals.eu | Kick-off Meeting 116

T4.3.- Create novel training curricula on cybersecurity in hospitals topics and define minimum quality standards for training material

(Lead INSP, Participants: EUR, FPHAG, SAM, JOIN)

➢ **Creation** of the course **curricula** by:

- designing infographics (at least 3).
- disseminated across all available channels (at least 3).

SecureHospitals.eu | Kick-off Meeting 117

T4.4.- Conceptualize online tools to support trainers in developing tailor-made courses on cybersecurity in hospitals

(Lead: EUR, Participants: TLX, FPHAG, SAM, JOIN)

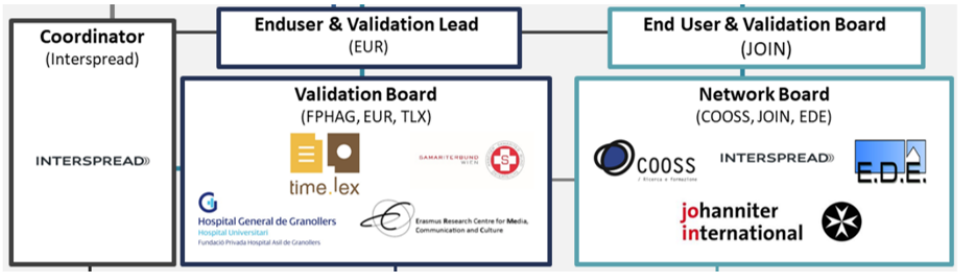
- **Roadmap** that leads **trainers** to the **development** of **new curricula** by:
  - building a step-by-step guide (at least 1).
  - uploading the guide as an online tool in the OAIH.

SecureHospitals.eu | Kick-off Meeting 118

Deliverables/ Milestones	Description	Month of Delivery	Lead
D4.1	Cybersecurity in hospitals courses and programmes collection	**M07**	FPHAG
D4.2	Trainer interviews and workshops report	**M08**	JOIN
D4.3	New cybersecurity in hospitals curricula and materials and quality assurance report	**M10**	INSP
D4.4	Step-by-step guide for the development of new course curricula	**M13**	EUR
M5	**Creation of training schemes and materials completed**	**M15**	**FPHAG**

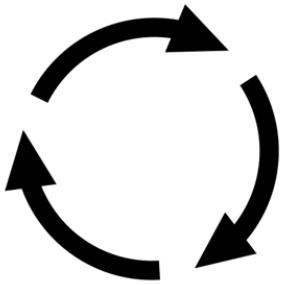
SecureHospitals.eu | Kick-off Meeting 119

Objectives are already defined



Monitoring [Implementation ⟷ Expertise

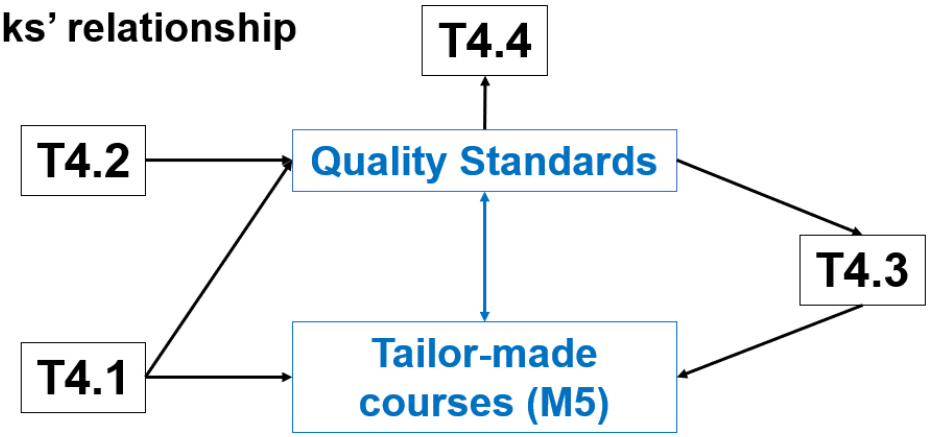
- Tasks ⟶ Reporting
- Milestones ⟶ Measure results



Quantify Impact

SecureHospitals.eu | Kick-off Meeting 120

- **Tasks' relationship**



- **Chronogram**

Month number	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13
T4.1							D4.1						
T4.2								D4.2					
T4.3										D4.3			
T4.4													D4.4

SecureHospitals.eu | Kick-off Meeting 121

Months 1 - 6

Proposed commitment	Partners responsible	Deadline
Subtask 4.1 – Collect existing courses on cybersecurity working session	FPHAG	Kickoff meeting
Subtask 4.1 – Having overview of types of existing trainings	FPHAG	M3
Subtask 4.3 – Functional Online Hub available	INSP	M4
Subtask 4.2 – Stakeholders and small workshops/focus groups with trainers and experts	JOIN	M6
Subtask 4.1 – Updating collection of courses on the online hub	FPHAG	M6

SecureHospitals.eu | Kick-off Meeting 122

Months 7 - 13

Proposed commitment	Partners responsible	Deadline
Subtask 4.2 – Teleconference meeting updating WP4 partners	FPHAG	M8
Subtask 4.3 – Curricula infographics created	INSP	M8
Subtask 4.4 – Build a step-by-step guide roadmap	EUR	M8
Subtask 4.3 – Teleconference meeting updating WP4 partners	FPHAG	M10
Subtask 4.4 – Teleconference meeting updating WP4 partners	FPHAG	M12
Subtask 4.4 – Uploading roadmap in the OAIH	EUR	M13

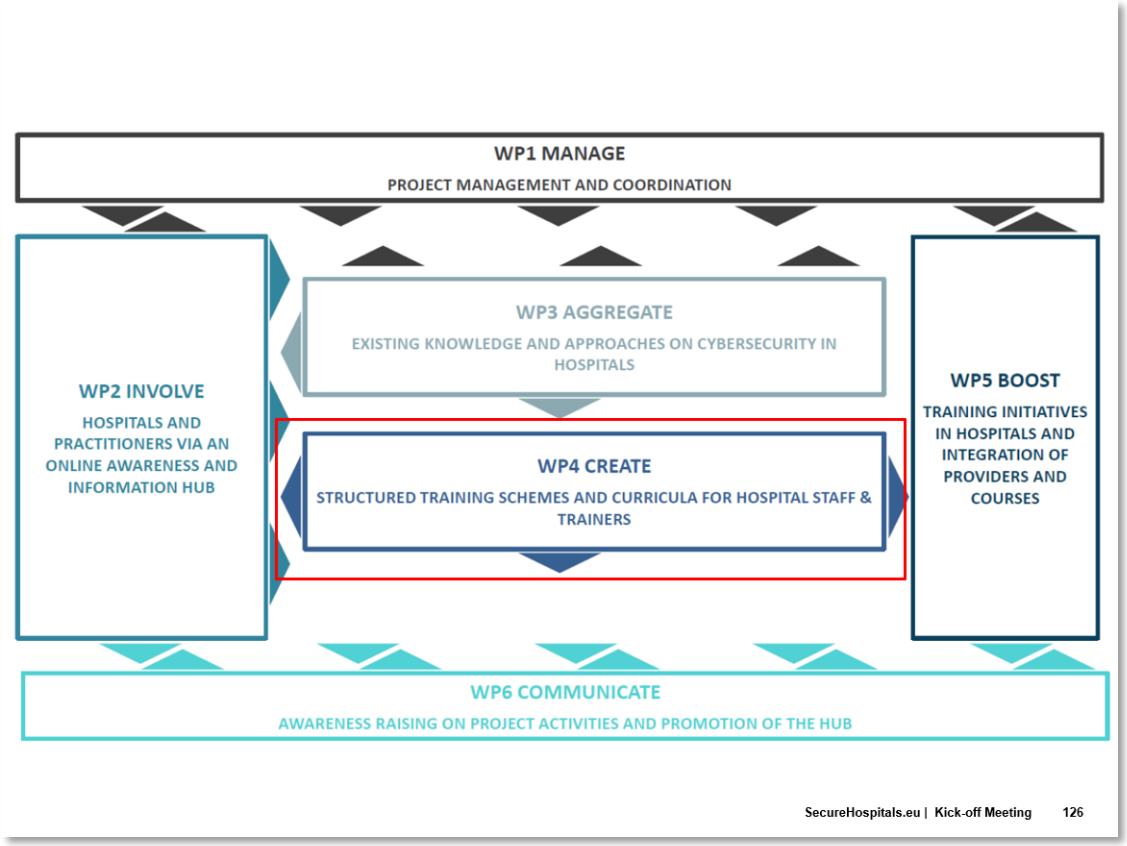
SecureHospitals.eu | Kick-off Meeting 123

Description of Risk	Work package concerned	Proposed risk-mitigation measures
Events fail to involve a large number of stakeholders or not the right ones	WP4	The vast network of experts from the think-tanks of the consortium, their affiliated fellow, board members and the SecureHospitals.eu Expert and Advisory Board will ensure that the project is well connected and disseminated n the community
Tasks are delayed	WP4	A contingency plan will be executed with weekly reporting to the coordinator

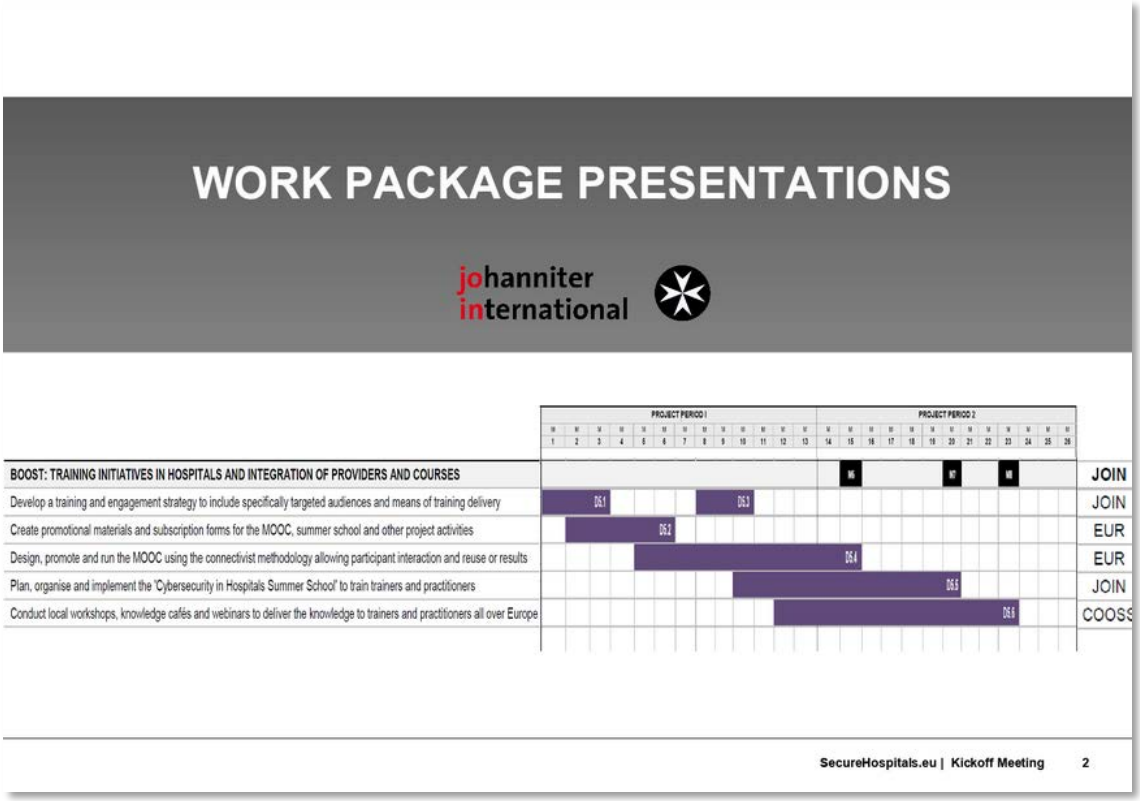
SecureHospitals.eu | Kick-off Meeting 124

FPHAG workpackage/task/deliverable leader													
Year	2018	2019											
Year number	Year 1												Year 2
Month	dic-18	ene-19	feb-19	mar-19	abr-19	may-19	jun-19	jul-19	ago-19	sep-19	oct-19	nov-19	dic-19
Month number	M01	M02	M03	M04	M05	M06	M07	M08	M09	M10	M11	M12	M13
WP4: Create: Structured training schemes and curricula for Hospitals staff & Trainers													
T4.1 Collect and assess existing training courses and programmes on cybersecurity in hospitals across various domains							D4.1						
T4.2 Engage trainers and experts to map and understand needs and challenges in training for cybersecurity in hospitals								D4.2					
T4.3 Create novel training curricula on cybesecurity in hospitals topics and define minimum quality standards for training material										D4.3			
T4.4 Conceptualise online tools to support trainers in developing tailor-made courses on cybersecurity in hospitals													D4.4

SecureHospitals.eu | Kick-off Meeting 125



WP5 BOOST: Training Initiatives in Hospitals and Integration of Providers and courses – by **JOIN**



WP 05
JOIN

T5.1 Develop a training & engagement strategy incl. targeted audiences and means of training delivery
Lead: JOIN: Participants: SAM, FPHAG, EDE Duration: M1 - 3

T5.2 Create promotional materials and subscription forms for MOOC, summer school, etc.
Lead: EUR, Participants: INSP, COOS, EDE Duration: M2 - 7

T5.3 Design, promote and run MOOC using connective methodology
Lead: EUR, Participants: INSP, COOS, EDE Duration: M5 – 15

T5.4 Plan, organise and implement the 'Cybersecurity in Hospitals Summer School'
Lead: JOIN, Participants: COOSS, SAM, FPHAG Duration: M10 – 20

T5.5 Conduct local workshops, knowledge cafes and webinars throughout Europe
Lead: COOSS, Participants: JOIN, EDE Duration: M12 - 23

SecureHospitals.eu | Kickoff Meeting 3

WP 05: OVERVIEW

WP Objectives:

- Exploitation of knowledge of EU projects, institutions and other actors of cyber security in hospitals
- Exploitation of first training materials
- Use multiple training formats
- Organization of MOOC, Summer Schools and webinars

- Each partner has to carry out at least 4 trainings (Workshops or knowledge cafes)

SecureHospitals.eu | Kickoff Meeting 4

TASK 5.1: DEVELOP A TRAINING AND ENGAGEMENT STRATEGY TO INCLUDE SPECIFICALLY TARGETED AUDIENES AND MEANS OF TRAINING DELIVERY

Lead: JOIN: Participants: SAM, FPHAG, EDE Duration: M1 - 3

Task Objectives:

- **Master plan for training and stakeholder management**
- **Definition of target group**
- **Define dates for trainings**

Two iterations shall be done: 1. defining staeholder and strategy for contacting them. 2. setting timeline and agendas for all the other trainings

TASK 5.1: DELIVERABLES AND MILESTONES

D5.1.

- M3
- Report
- The first iteration of the training strategy will list the targeted stakeholder at the local and European level and the means of their engagement in the project trainings.

TASK 5.1: DIFFICULTIES AND SOLUTIONS

- Potential Obstacles
  - Finding the right approach for the topic and the right stakeholder
  - "Field entrance"
- Strategies to overcome them
  - Use of personal network
  - If not sufficient stakeholder reply to our request, we follow official trails. This will result in a delay.

TASK 5.2: CREATE PROMOTIONAL MATERIALS AND SUBSCRIPTION FORMS FOR THE MOOC, SUMMER SCHOOL AND OTHER PROJECT ACTIVITIES

Lead: EUR, Participants: INSP, COOS, EDE Duration: M2 - 7

Task Objectives:

- **Create promotional material**
- **Promotional video**
- **Subscription forms**

This feeds into WP 6

TASK 5.2: DELIVERABLES AND MILESTONES

D5.2.

- M6
- demonstrator
- The promotional materials and subscription form will be integrated in the online hub and similar channels for advertising purposes.

TASK 5.2: DIFFICULTIES AND SOLUTIONS

- Potential Obstacles
  - Quality of Material is not sufficient
  - Different "language" and understanding between experts, stakeholders and users.
  - No marketing expert is in the project and
  - the time is not sufficient for professional material
  - Because no content is available NOW
- Strategies to overcome them
  - Use what is available until the deadline.
  - Reduce number of different channels
  - Focus on the primary channel of targetgroup (buyers)
  - Produce the rest materials later with a delay.

TASK 5.3: DESIGN, PROMOTE AND RUN THE MOOC USING THE CONNECTIVIST METHODOLOGY ALLOWING PARTICIPANT INTERACTION AND REUSE OR RESULTS

Lead: EUR, Participants: INSP, COOS, EDE Duration: M5 – 15

Task Objectives:

- **Implementation of MOOC**
- **Development of Curriculum**
- **Taking existing material and rebrand it**

TASK 5.3: DELIVERABLES AND MILESTONES

D5.3. Training Strategy 2

- M11
- Report
- The second iteration of the training strategy will provide the timelines and agendas of local trainings and the webinars

TASK 5.3: DIFFICULTIES AND SOLUTIONS

- Potential Obstacles
  - Low interest in the workshops
  - Availability of certified trainers in the consortium is unclear
  - Experts in cyber security are not always the best trainers for lay persons
- Strategies to overcome them
  - Offer courses for a small amount of money
  - Hire certified trainer
  - Cascading process?

TASK 5.4: PLAN, ORGANISE AND IMPLEMENT THE 'CYBERSECURITY IN HOSPITALS SUMMER SCHOOL' TO TRAIN TRAINERS AND PRACTITIONERS

Lead: JOIN, Participants: COOSS, SAM, FPHAG Duration: M10 – 20

Task Objectives:

- **Planning, implementation and organisation of summer schools**
- **Designing curriculum and materials**

TASK 5.4: DELIVERABLES AND MILESTONES

D5.4.

- M15
- Report
- The MOOC report will summarise the whole participation in the MOOC, the evaluation of the assignments, the number of participants and issued certificates, the level of online collaboration, the feedback from the participants etc.

D5.5.

- M20
- Report
- The summer school report will also detail the participations, the agenda, courses, learning outcomes, social activities, and the most crucially the participant feedback.

TASK 5.4: DIFFICULTIES AND SOLUTIONS

- Potential Obstacles
  - Low interest in the workshops
  - Availability of certified trainers in the consortium is unclear
  - Experts in cyber security are not always the best trainers for lay persons
- Strategies to overcome them
  - Offer courses for a small amount of money
  - Hire certified trainer
  - Cascading process?

TASK 5.5: CONDUCT LOCAL WORKSHOPS, KNOWLEDGE CAFES AND WEBINARS TO DELIVER THE KNOWLEDGE TO TRAINERS AND PRACTITIONERS ALL OVER EUROPE

Lead: COOSS, Participants: JOIN, EDE Duration: M12 - 23

Task Objectives:

- **Running webinars**
- **Running knowledge cafes**
- **Running workshops**

TASK 5.5: DELIVERABLES AND MILESTONES

D5.6.

- M3
- Report
- The training reports will summarise all other trainings and their outputs. One of the key aspect to be taken into consideration in the report will be the feedback from the training participants.

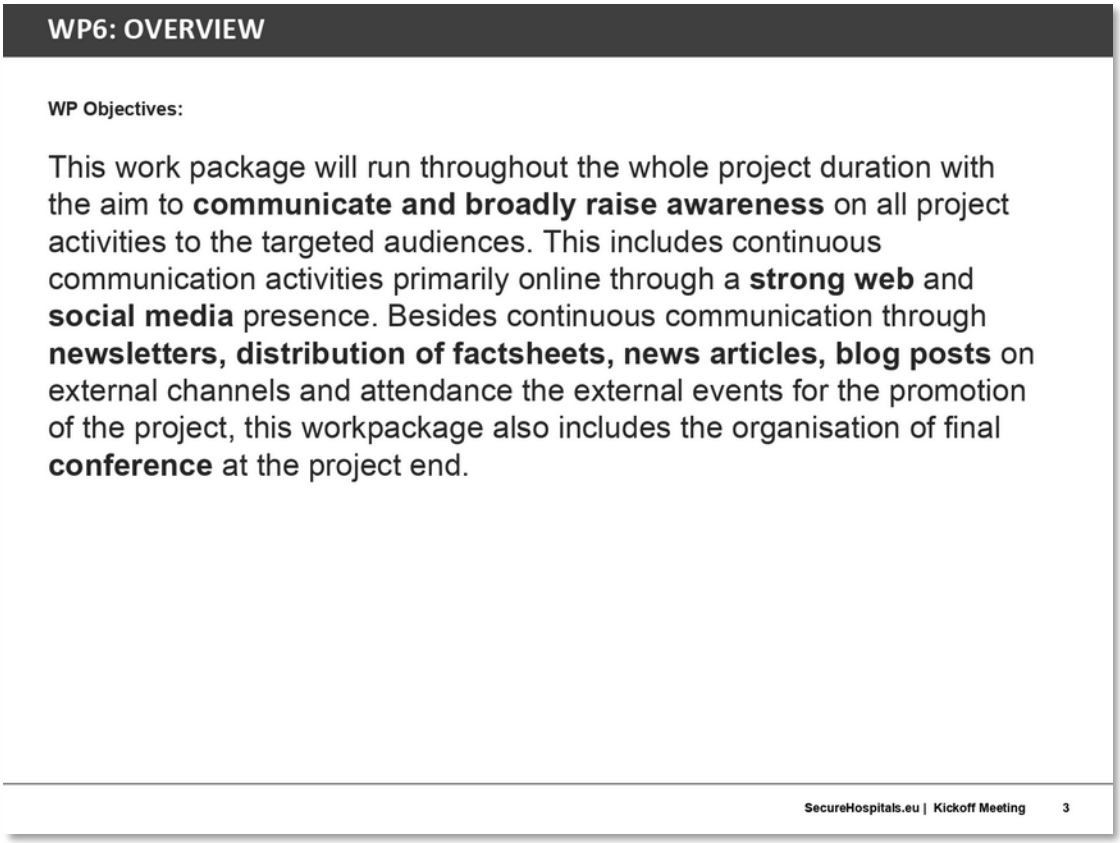
TASK 5.5: DIFFICULTIES AND SOLUTIONS

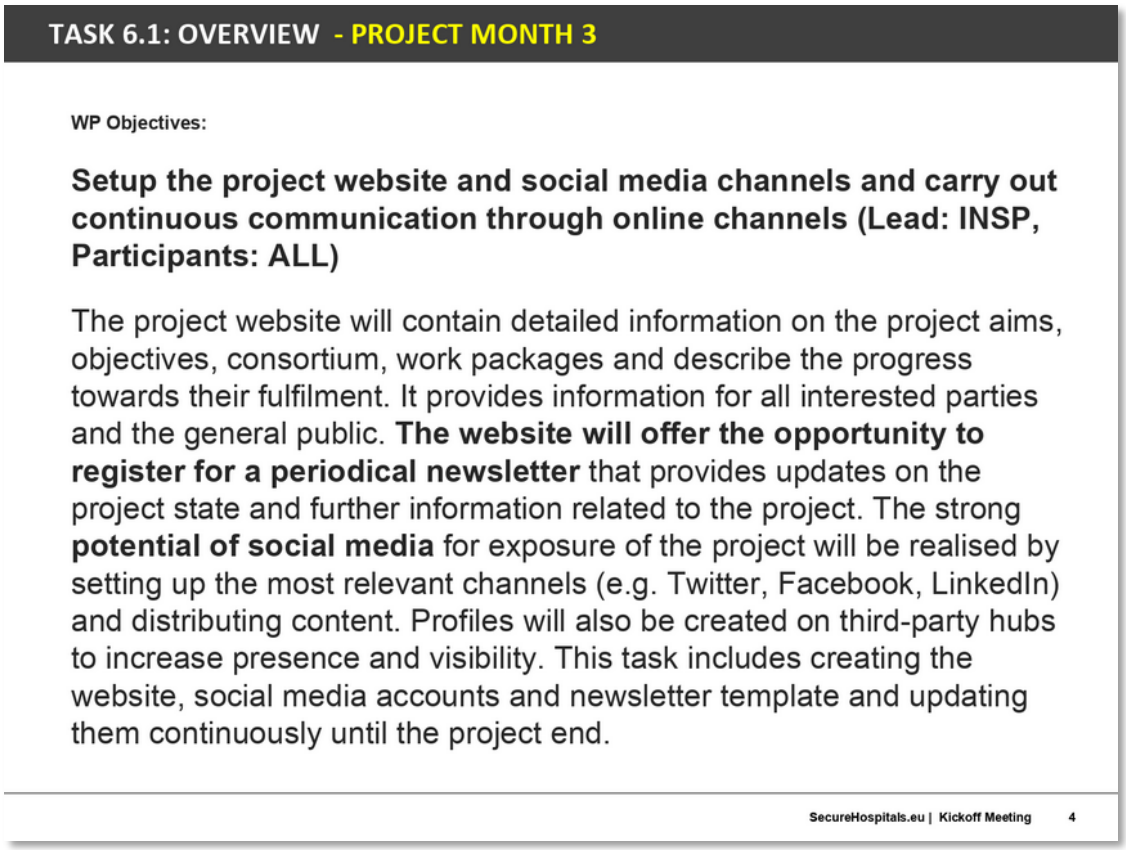
- Potential Obstacles
  - Low interest in the workshops
  - Availability of certified trainers in the consortium is unclear
  - Experts in cyber security are not always the best trainers for lay persons
- Strategies to overcome them
  - Offer courses for a small amount of money
  - Hire certified trainer
  - Cascading process?

Methodology:

- **Value-Proposition and Business Model Canvas for Stakeholderanalysis**
- **Communication plan for motivation and raising interest.**
- **Evaluation of summer school for the report with a short feedback form**

16:30 WP6 COMMUNICATE: Awareness Raising on Project Activities and Promotion of the Hub – by **EAN**





TASK 6.2: OVERVIEW - PROJECT MONTH 5

WP Objectives:

Send out newsletters, distribute factsheets, leaflets and other infographics to raise awareness on the project activities (Lead: EAN, Participants: ALL)

This task includes design and other creative activities to build **infographics, short videos, factsheets, awareness sheets, leaflets** and other types of visualisations for making project outputs more visually attractive and fit for wide dissemination. It also includes all activities to provide stakeholders with **meaningful information** on project status and outcomes in the form of updates, factsheets, newsletters, etc. Materials will be disseminated on a rolling basis throughout the project duration.

SecureHospitals.eu | Kickoff Meeting 5

TASK 6.3: OVERVIEW

WP Objectives:

Communicate to the scientific community by attending external events and conferences and publishing on external blogs and media (Lead: EUR, Participants: INSP, FPHAG, COOS, SAM, JOIN, EAN)

To increase the outreach of the communication to the scientific community, this task foresees publishing information sources on the project in **external blogs, news outlets and science magazines targeting research** and innovation practitioners all over Europe.

SecureHospitals.eu | Kickoff Meeting 6

TASK 6.4: OVERVIEW

WP Objectives:

Provide a final exploitation strategy for long-term exploitation of the project results and the sustainability of the online training hub (Lead: INSP, Participants: ALL)

To increase the outreach of the communication to the scientific community, this task foresees publishing information sources on the project in external blogs, news outlets and science magazines targeting research and innovation practitioners all over Europe.

SecureHospitals.eu | Kickoff Meeting 7

TASK 6.5: OVERVIEW

WP Objectives:

Organize the final 'Cybersecurity in Hospitals Awareness Conference' as a crucial event on the topic in close linkage with stakeholders and interest groups (Lead: EAN, Participants: INSP, EUR, FPHAG, COOS, SAM, JOIN)

At the end of the project, a final conference will be organised at the European level seeking to include most of the trainers and practitioners trained during the projects and additional stakeholders in the research and innovation field. The conference will provide a space for reflecting on the impacts of the trainings carried out within the project, discuss on the expansion, sustainability and exploitation of the trainer network on the web hub www.securehospitals.eu primarily through the actively engagement of trainers in the community of practice as well as strong synergies with the consortia of relevant actions.

? Place, number of participants

SecureHospitals.eu | Kickoff Meeting 8

TASK 6.1: DELIVERABLES AND MILESTONES

D6.1

Project website, social media accounts and communication channels (project month 3)

Lead: INSP

This deliverable will report on the project website development as well as the creation of the social media channels, newsletter template and other document templates containing the official project logo, reference to EU funding (including number of grant agreement) and logos of consortium partners.

MS 2

Project website and social media channels created **(project month 3)**

SecureHospitals.eu | Kickoff Meeting 9

TASK 6.2: DELIVERABLES AND MILESTONES

D6.2

Dissemination materials (project month 5)

Lead: EAN

This deliverable will include the evidence on the first project materials (factsheets etc.) produced in the first five months that will serve for raising awareness on the project. As the project progresses the printed materials will be adapted accordingly.

D6.3

Dissemination activities report (project month 26) Lead: EAN

This deliverable will detail all dissemination materials produced during the project, and communication activities through newsletter, web presence and the social media channels. The report will describe the processes behind the communication activities and the describe if the outcomes of these activities meet the pre-defined key performance indicators.

SecureHospitals.eu | Kickoff Meeting 10

WP6: METHODOLOGY

Methodology and templates

- Database of contacts (stakeholders, realted experts)
  - Structure of the contatcs
- Corespondence and communication layout
- Project logo
- GDPR (compliance with using the data)
- Mentions and presence in external media during the project timeline
  - Which media, countries, contacts from project partners
    - LIST OF CONTACTS OF MEDIA IN PARTICULAR COUNTRIES
- Subscribers to the SecureHospitals.eu Newsletter
  - ? Which countries, contacts from project partners
  - At the website, thourgh partners contacts,
- EAN GA meeting – Utrecht – April 2019
- EAN EB meeting – Stockholm – June 2019

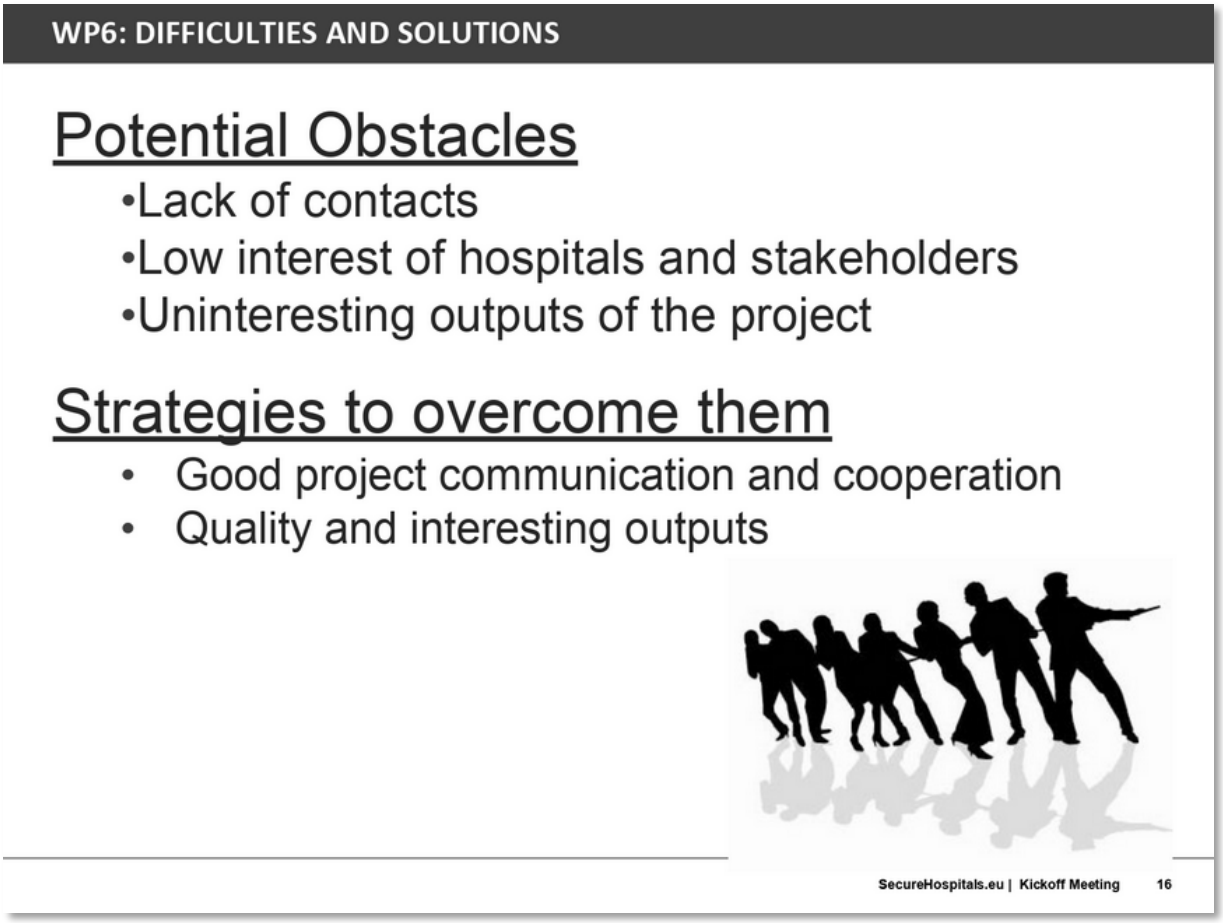
SecureHospitals.eu | Kickoff Meeting 14

TASK 6.2: WORK FLOW AND DISTRIBUTION

What are the commitment for the next months?

Commitment	Partners responsibles	Deadline
D6.1 Project website, social media accounts and communication channels	INSP	M3
D6.2 Dissemination materials	EAN	M5

SecureHospitals.eu | Kickoff Meeting 15



WP1: MANAGE: INSP

In the work package discussion, INSP presented things to keep in mind regarding the main project management, addressing aspects such as the role of the coordinator, communication within the project, quality assurance, conference calls and consortium meetings, reports, and the Collabto system.

Coordinator Role & Responsibilities:

- Responsibility of constant monitoring, assurance to sticking to the project plan
- Submit deliverables: It is important to send deliverables early on, because the exact time of upload will be registered and it will be noted if something is delivered too late
- The coordinator is the single point of contact for the Project officer – all communication with the European Commission is going through INSP. If problems appear, members of the consortium can contact INSP and they will forward them to the EC.

NOT responsibilities of the coordinator are:

- Financial reporting for the partner organisations – BUT they will be helping and providing material. However, the consortium partners have to be aware of the budget and manage it themselves. The financial report will be collected in a system and each partner will be informed by INSP what has to be submitted, what information is needed etc. For all staff members who aren't working 100% there needs to be a time sheet, but they don't have to be submitted (also contracts).

- Allocating subtasks – BUT support and help when problems come up. It is very important to keep the deadlines and inform about problems as early as possible.
- Output – BUT each deliverable will be checked in detail by the coordinator.

Communication:

- For general rules see document Communication Guidelines
- Respect:
  - Respect the roles of partners (WP leads/task leads) – each of these roles bring along certain responsibilities that should be respected, as well as decisions made by the leads.
  - Respect skills, knowledge and experience of partners which can be valuable. Don't exclude knowledge from different perspectives.
  - Respect different perspectives and approaches.
  - Trustful and respectful communication.

- Responsibilities:
  - Awareness on DoA and project plan: Look at the plan and see if the outcomes fit the plan.
  - Full lead of own work packages and deliverables: The project needs each of the partners to be actively involved in creating outcome, deliverables etc. – there should be strong support and active feedback to the partners, especially from partners who are not leading WPs.
  - Keeping review and quality assurance.

- Commitment:
  - Participation in calls and meetings.
  - Keeping deadlines.
  - Being proactive and self-driven.
  - High quality.
  - Inform INSP if there is a problem, especially the WP leads.

- Quality assurance:
  - Every partner should try to make draft versions of deliverables accessible as early as possible, but at least one month prior to the deadline. If it is possible to produce something earlier this would help to speed up things.
  - See SecureHospitals.eu Quality Assurance Checklist.
  - Every deliverable should include an Executive Summary at the beginning. INSP will provide a template for the deliverables.
  - Make the deliverables available for all partners to gather valuable feedback and inputs. There is also one resigned reviewer for every deliverable (= internal peer review).

4.2 Day 2 (25.01.2019)

The second day started with a recap from the first day, the description of another set of administrative procedures and assignment of roles for quality assurance as described in the following table.

No.	Title	Lead	Due date	Review
D1.1	Kick-off meeting report	INSP	M2 / Jan 2019	ALL
D2.1	Stakeholder involvement roadmap and engagement strategy	COOSS	M3 / Feb 2019	INSP
D5.1	Training Strategy 1	JOIN	M3 / Feb 2019	TLX
D6.1	Project website, social media accounts and communication channels	INSP	M3 / Feb 2019	EAN
D2.2	Current perceptions and trends on cybersecurity in hospitals	EAN	M5 / Apr 2019	JOIN
D6.2	Dissemination materials	EAN	M5 / Apr 2019	SAM
D1.2	Data Management Plan	TLX	M6 / May 2019	EUR
D3.1	Cybersecurity in hospitals Knowledge Map	FPHAG	M6 / May 2019	JOIN
D5.2	Promotional materials and registration forms	EUR	M6 / May 2019	TLX
D7.1	H - Requirement No. 1	INSP	M6 / May 2019	FPHAG
D7.2	POPD - Requirement No. 2	INSP	M6 / May 2019	TLX
D3.2	European project and stakeholders on cybersecurity in hospitals report	JOIN	M7 / Jun 2019	TLX
D4.1	Cybersecurity in hospitals courses and programmes collection	FPHAG	M7 / Jun 2019	EUR
D2.3	Online Awareness and Information Hub www.securehospitals.eu	INSP	M8 / Jul 2019	EAN
D3.3	State-of-the art and potentials for eLearning and Approaches in Cybersecurity in hospitals training report	INSP	M8 / Jul 2019	COOS
D4.2	Trainer interviews and workshops report	TLX	M8 / Jul 2019	COOS
D3.4	Cybersecurity in hospitals Knowledge Baseline Report	EUR	M9 / Aug2019	TLX
D2.4	Relevant cybersecurity projects list and liaisons overview	INSP	M10 / Sep 2019	SAM
D4.3	New cybersecurity in hospitals curricula and materials and quality assurance report	FPHAG	M10 / Sep2019	INSP
D5.3	Training Strategy 2	JOIN	M10 / Sep 2019	COOS
D4.4	Step-by-step guide for the development of new course curricula	EUR	M13 / Dec 2019	COOS
D5.4	SecureHospitals.eu MOOC report	EUR	M15 / Feb 2020	INSP
D5.5	Cybersecurity in Hospitals Summer School report	JOIN	M20 / Jul 2020	FPHAG
D5.6	Webinars and local trainings report	COOSS	M23 / Oct 2020	INSP
D6.3	Dissemination activities report	EAN	M24 / Nov 2020	EUR
D6.4	Publication and presentation overview list	EUR	M26 / Jan 2021	SAM
D6.5	Securehospitals.eu exploitation plan	INSP	M26 / Jan2021	FPHAG
D6.6	Cybersecurity in Hospitals Awareness Conference summary report	EAN	M26 / Jan 2021	JOIN

Conference Calls & Meetings:

- There will be a conference call every second week for the first four months on **Tuesday 11:00 CET, starting on 5.01.2019.**
- The next physical full consortium meeting will be organised by COOSS in Italy by end of May/beginning of June **2019** (an exact date will be set soon).

Good Practices in Grant management:

- The guidelines are also available in the Collabto system.
  - INSP will be responsible for risk management and communicate every identified risk to the consortium. If e.g. a partner doesn't respond, the consortium together has to agree on how to proceed.

Reports:

- At project period one in December 2019 a financial and technical report shall be delivered. Internal reporting should be delivered in March 2017: Which kinds of resources have been used? Is everything more or less as scheduled? Too much or too little consumption?

Ethics:

- Every deliverable will be checked by the EC. Every partner is therefore urged to follow the guidelines!

Collabto system:

- Most of the relevant information is collected there; also further details and links as well as a calendar.
- WP leads should discuss issues via the forum rather than via email.
- Correct naming of documents is important.

Working Session 1

The first working session addressed the T2.1 and T5.1 which are closely related to each other. The team split in two groups rotating in a world café model, in order to provide their inputs for both topics, and then results were discussed in plenum. Synergies but also distinctions between both tasks were explained and a final plan was made regarding the content of their deliverables and contributions from each of the partners.

Working Session 2

The second working session addressed T3.1 and 4.1. The teams discussed on the types of knowledge materials and trainings to be collected and the means for collecting, storing and analysing the materials. An overall outline of all upcoming deliverables was made and all open questions discussed regarding upcoming tasks had the chance to be discussed in more detail.

5. Action Points

At the SecureHospitals.eu kick-off meeting, members of all participating institutions were present and able to contribute valuable input regarding the overall project, the different objectives and tasks and their challenges. First decisions concerning the first steps towards the deliverables and distribution of work in the work packages were made.

Immediate actions point:

Item	Responsible	Due Date
Create the final project logo reflecting the consortium inputs	INSP	31.01.2019
Launch the project website and social media channels	INSP	31.01.2019
Create other project identity materials (factsheets etc.)	INSP	31.01.2019
Develop a work division for task 2.1 to collect stakeholders in the existing Excel sheet.	COOSS	31.01.2019
Create a Zotero page for collecting relevant literature for T3.1	EUR	31.01.2019
Check for additional stakeholders to include in the Expert and Advisory Board	All partners	05.02.2019
Detect and identify stakeholders, organisations and institutions for the stakeholder mapping.	All partners	05.02.2019

Other points raised and discussed during the second day include:

- Creating an agreement among all partners regarding the collection, storage and use of the personal data that will be collected in the project as a means for achieving its objectives. The agreement will be drafted by TLX and will be sent for review to all partners. In the next consortium call the partners will have the chance to discuss on the agreement and sign it prior to the collection of major amounts of personal data.
- EUR shall identify the costs of the MOOC based on its available frameworks and identify the potential for its creation within the resources available in the project. In case the estimated costs exceed the amount of the budget allocated in the project for the creation of the MOOC, co-funding opportunities will be sought in order to be able to deliver a quality product.

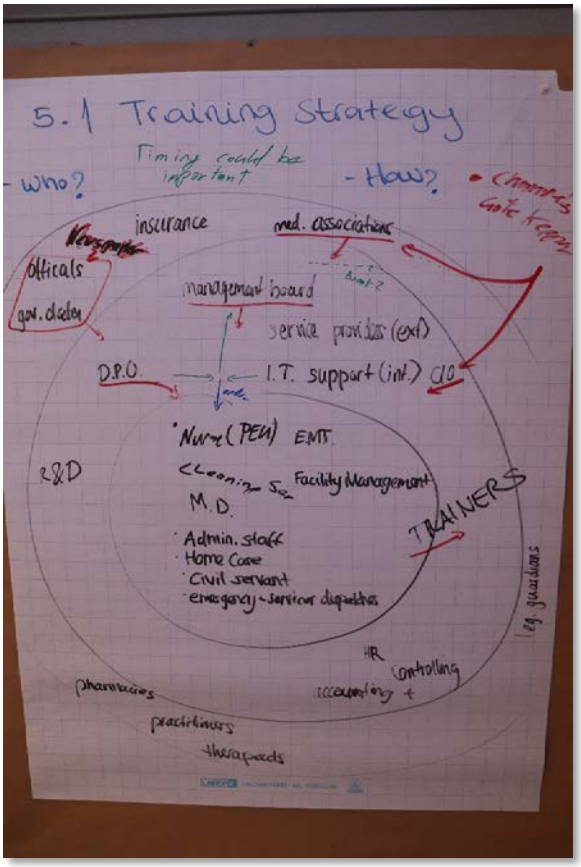
The partners left the kick-off meeting with a better understanding about their respective roles and responsibilities, and the different tasks and deliverables ahead. They also got to know each other and were able to establish relationships among the consortium members.

During the meeting, a lot of different questions were discussed and though not each may have been answered, the main issues were resolved. Each consortium member had the chance to present their position on these open questions and the consortium will continue to discuss open questions in conference calls every second week on Wednesday until the next consortium meeting beginning of February 2019.

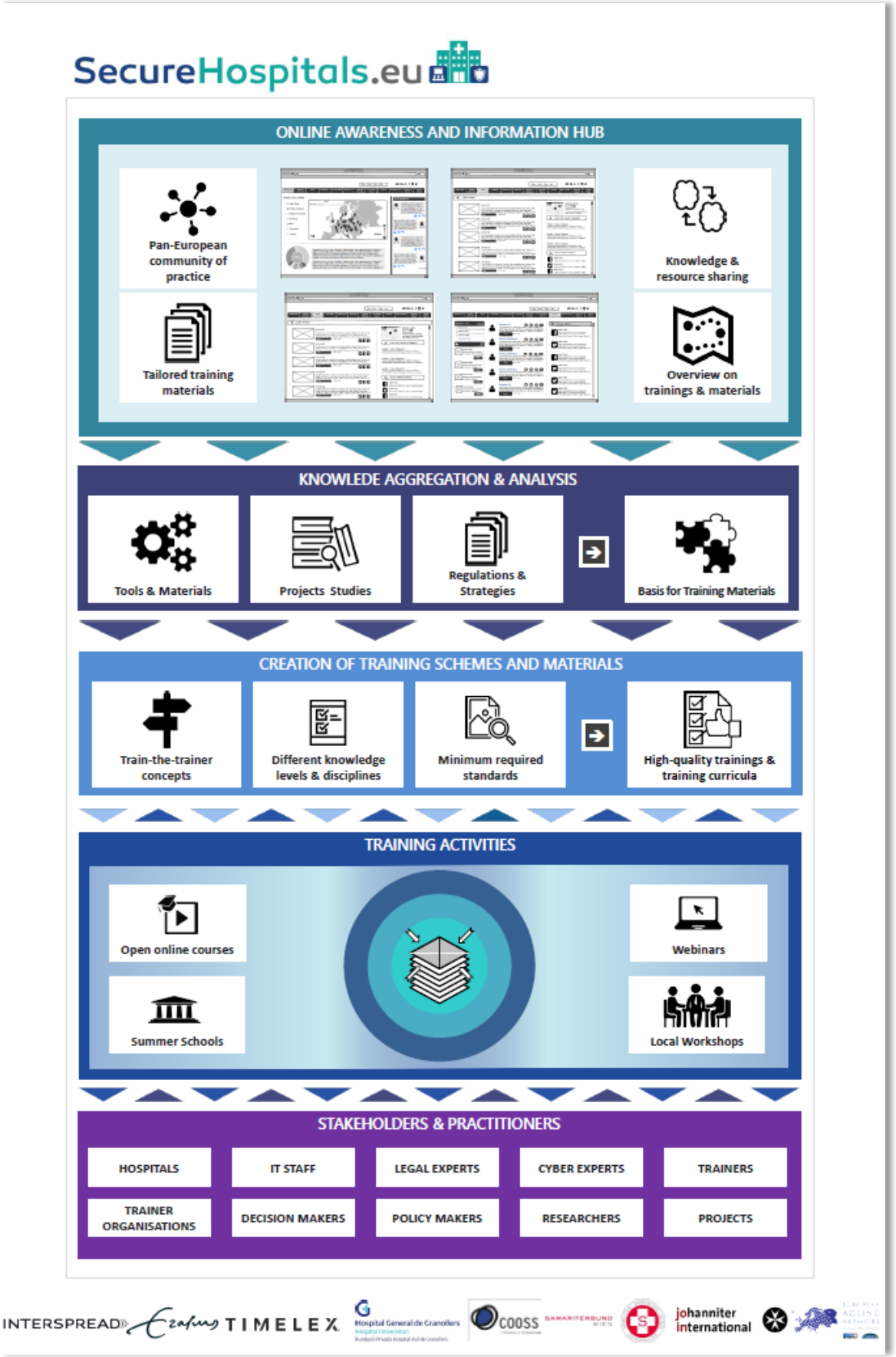
6. Impressions

Photos from the meeting.


2.1. Stakeholdes involvement roadmap
- who?
- How?
Hospitals –
ES: Agreements with Hospitals in Barcellona
Mutual help
1) who has a problem
2) who has a solution
CZ: EAN Network
Hospitals in CZ
Contacts with trainers in CZ
different invitation letters
Medical associations
Policy makers
Hospitals
Researchers
Trainers
NL (region)
AT: trainers
Home care org.
Paramedical prof.
Policymakers
BE: hospitals in EU
Trainers
Proposal: to identify risks and problems for each category (from the literature)
to justify why we need to involve them
to invite them to join because we know their problems
to base their involvement into their needs


5.1 Training Strategy
Timing could be important
- Who?
- How?
insurance
med. associations
Officals
gov. dicision
management board
service provider (ext)
D.P.O
I.T. support (int.)
CIO
Nurse (PEN) EMT
R&D
Facility Management
M.D.
Admin. staff
Home Care
Civil servant
emergency - service dispatches
TRAINERS
HR
(controlling
pharmacies
practitioners
therapeuds
eg guardians

7. Print materials



SecureHospitals.eu

#	WP	Title	Lead	Nature	Dissemination	Due date
D1.1	WP1	Kick-off meeting report	INSP	Report	Confidental	M2 / January 2019
D1.2	WP1	Data Management Plan	TLX	ORDP	Public	M6 / May 2019
D1.3	WP1	Status report	INSP	Report	Confidential	M14 / January 2020
D1.4	WP1	Final project documentation	INSP	Report	Confidential	M26 / January 2021
D2.1	WP2	Stakeholder involvement roadmap and engagement strategy	COOSS	Report	Public	M3 / February 2019
D2.2	WP2	Current perceptions and trends on cybersecurity in hospitals	EAN	Other	Public	M5 / April 2019
D2.3	WP2	Online Awareness and Information Hub www.securehospitals.eu	INSP	Other	Public	M8 / July 2019
D2.4	WP2	Relevant cybersecurity projects list and liaisons overview	INSP	Other	Public	M10 / September 2019
D3.1	WP3	Cybersecurity in hospitals Knowledge Map	FPHAG	Other	Confidental	M6 / May 2019
D3.2	WP3	European project and stakeholders on cybersecurity in hospitals report	JOIN	Report	Confidential	M7 / June 2019
D3.3	WP3	State-of-the art and potentials for eLearning and Approaches in Cybersecuri	INSP	Report	Confidental	M8 / July 2019
D3.4	WP3	Cybersecurity in hospitals Knowledge Baseline Report	EUR	Report	Public	M9 / August 2019
D4.1	WP4	Cybersecurity in hospitals courses and programmes collection	FPHAG	Report	Public	M7 / June 2019
D4.2	WP4	Trainer interviews and workshops report	TLX	Report	Public	M8 / July 2019
D4.3	WP4	New cybersecurity in hospitals curricula and materials and quality assura	FPHAG	Report	Public	M10 / September 2019
D4.4	WP4	Step-by-step guide for the development of new course curricula	EUR	Report	Public	M13 / December 2019
D5.1	WP5	Training Strategy 1	JOIN	Report	Public	M3 / February 2019
D5.2	WP5	Promotional materials and registration forms	EUR	Other	Public	M6 / May 2019
D5.3	WP5	Training Strategy 2	JOIN	Other	Public	M10 / September 2019
D5.4	WP5	SecureHospitals.eu MOOC report	EUR	Report	Public	M15 / February 2020
D5.5	WP5	Cybersecurity in Hospitals Summer School report	JOIN	Report	Public	M20 / July 2020
D5.6	WP5	Webinars and local trainings report	COOSS	Report	Public	M23 / December 2020
D6.1	WP6	Project website, social media accounts and communication channels	INSP	Other	Public	M3 / February 2019
D6.2	WP6	Dissemination materials	EAN	Other	Public	M5 / April 2019
D6.3	WP7	Dissemination activities report	EAN	Other	Public	M24 / November 2020
D6.4	WP7	Publication and presentation overview list	EUR	Other	Public	M26 / January 2021
D6.5	WP7	Securehospitals.eu exploitation plan	INSP	Report	Confidential	M26 / January 2021
D6.6	WP7	Cybersecurity in Hospitals Awareness Conference summary report	EAN	Report	Public	M26 / January 2021
D7.1	WP7	H - Requirement No. 1	INSP	Ethics	Public	M6 / May 2019
D7.2	WP7	POPD - Requirement No. 2	INSP	Ethics	Public	M6 / May 2019

Number	WP	Title	Lead	Nature	Dissemination	Due date
D1.1	WP1	Kick-off meeting report	INSP	Report	Confidental	M2 / January 2019
D2.1	WP2	Stakeholder involvement roadmap and engagement strategy	COOSS	Report	Public	M3 / February 2019
D5.1	WP5	Training Strategy 1	JOIN	Report	Public	M3 / February 2019
D6.1	WP6	Project website, social media accounts and communication channels	INSP	Other	Public	M3 / February 2019
D2.2	WP2	Current perceptions and trends on cybersecurity in hospitals	EAN	Other	Public	M5 / April 2019
D6.2	WP6	Dissemination materials	EAN	Other	Public	M5 / April 2019
D1.2	WP1	Data Management Plan	TLX	ORDP	Public	M6 / May 2019
D3.1	WP3	Cybersecurity in hospitals Knowledge Map	FPHAG	Other	Confidental	M6 / May 2019
D5.2	WP5	Promotional materials and registration forms	EUR	Other	Public	M6 / May 2019
D7.1	WP7	H - Requirement No. 1	INSP	Ethics	Public	M6 / May 2019
D7.2	WP7	POPD - Requirement No. 2	INSP	Ethics	Public	M6 / May 2019
D3.2	WP3	European project and stakeholders on cybersecurity in hospitals report	JOIN	Report	Confidential	M7 / June 2019
D4.1	WP4	Cybersecurity in hospitals courses and programmes collection	FPHAG	Report	Public	M7 / June 2019
D2.3	WP2	Online Awareness and Information Hub www.securehospitals.eu	INSP	Other	Public	M8 / July 2019
D3.3	WP3	State-of-the art and potentials for eLearning and Approaches in Cybersecuri	INSP	Report	Confidental	M8 / July 2019
D4.2	WP4	Trainer interviews and workshops report	TLX	Report	Public	M8 / July 2019
D3.4	WP3	Cybersecurity in hospitals Knowledge Baseline Report	EUR	Report	Public	M9 / August 2019
D2.4	WP2	Relevant cybersecurity projects list and liaisons overview	INSP	Other	Public	M10 / September 2019
D4.3	WP4	New cybersecurity in hospitals curricula and materials and quality assurai	FPHAG	Report	Public	M10 / September 2019
D5.3	WP5	Training Strategy 2	JOIN	Other	Public	M10 / September 2019
D4.4	WP4	Step-by-step guide for the development of new course curricula	EUR	Report	Public	M13 / December 2019
D5.4	WP5	SecureHospitals.eu MOOC report	EUR	Report	Public	M15 / February 2020
D5.5	WP5	Cybersecurity in Hospitals Summer School report	JOIN	Report	Public	M20 / July 2020
D5.6	WP5	Webinars and local trainings report	COOSS	Report	Public	M23 / October 2020
D6.3	WP7	Dissemination activities report	EAN	Other	Public	M24 / November 2020
D6.4	WP7	Publication and presentation overview list	EUR	Other	Public	M26 / January 2021
D6.5	WP7	Securehospitals.eu exploitation plan	INSP	Report	Confidential	M26 / January 2021
D6.6	WP7	Cybersecurity in Hospitals Awareness Conference summary report	EAN	Report	Public	M26 / January 2021

Number	Name	Lead	Due date
M1	Kick-off meeting	INSP	M2 / January 2019
M2	Project website and social media channels created	INSP	M3 / February 2019
M3	Knowledge aggregation completed	EUR	M9 / August 2019
M4	Creation of the open online information hub completed	INSP	M11 / October 2019
M5	Creation of training schemes and materials completed	EUR	M13/ December 2019
M6	MOOC completed	EUR	M15 / February 2020
M7	Summer school completed	JOIN	M20 / July 2020
M8	All training activities completed	COOSS	M22 / September 2020
M9	SecureHospitals.eu conference completed	EAN	M26 / January 2021
M10	Project finalised and documented	INSP	M26 / January 2021

SecureHospitals.eu