Please check our wiki for help on navigating the form.

Horizon 2020

Call: H2020-SC1-FA-DTS-2018-2020

(Trusted digital solutions and Cybersecurity in Health and Care)

Topic: SU-TDS-03-2018

Type of action: CSA

Proposal number: SEP-210514178

Proposal acronym: SecureHospitals.eu

Deadline Id: H2020-SC1-FA-DTS-2018-1

Table of contents

Section	*Title*	*Action*
1	General information	
2	Participants & contacts	
3	Budget	
4	Ethics	
5	Call-specific questions	

How to fill in the forms

The administrative forms must be filled in for each proposal using the templates available in the submission system. Some data fields in the administrative forms are pre-filled based on the steps in the submission wizard.

1 - General information

Topic	SU-TDS-03-2018	Type of Action	CSA
Call Identifier	H2020-SC1-FA-DTS-2018-2020	Deadline Id	H2020-SC1-FA-DTS-2018-1

Acronym	SecureHospitals.eu
Proposal title	RAISING AWARENESS ON CYBERSECURITY IN HOSPITALS ACROSS EUROPE AND BOOSTING TRAINING INITIATIVES DRIVEN BY AN ONLINE INFORMATION HUB

Note that for technical reasons, the following characters are not accepted in the Proposal Title and will be removed: < > " &

Duration in months	*26*
Fixed keyword 1	eHealth
Fixed keyword 2	Cybersecurity
Free keywords	*Cybersecurity; Data Protection; Hospitals; Care Centres; Trainings; MOOC; awareness raising; Training; Information hub; cyber-attack prevention; risk and protection opportunities*

Abstract

Cybercrime has recently shifted from attacking big corporations to smaller industries, like financial services as well as the healthcare sector. Especially in the last area the trend is rising, where hackers are targeting patient health devices that are connected to the internet. Most cases include stealing patient information and encrypting it for ransom money. The big problem is interconnection, each application or device that runs on the networks represents a possible entry point for a cyber-physical attack. So far, most hackers infected hospital software with ransomware to prevent staff from accessing patient records or scheduling appointments. But capable terrorists would also be able, to render active medical devices not just useless, but deadly. Complete cybersecurity in the health sector is unachievable, and would exceed financial means; nevertheless, vital steps can be taken to minimize the risk of cyber- attacks against healthcare facilities. Around 85 percent of targeted cyber-attacks would be preventable if basic protection protocols would be established. The SecureHospitals.eu project seeks to raise awareness on risks and protection opportunities, setup training schemes and the initiate training sessions for IT staff working in hospitals. Through several training approaches, the project will boost the level of training in cybersecurity in Europe, improve the knowledge of staff and in turn contribute to decreased vulnerabilities against cyberthreats and increased patient trust and safety.

Remaining characters 475

Has this proposal (or a very similar one) been submitted in the past 2 years in response to a call for proposals under Horizon 2020 or any other EU programme(s)? ○ Yes ◉ No

Please give the proposal reference or contract number.	
xxxxxx-x	

Declarations

1) The coordinator declares to have the explicit consent of all applicants on their participation and on the content of this proposal.	☒
2) The information contained in this proposal is correct and complete.	☒
3) This proposal complies with ethical principles (including the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity — and including, in particular, avoiding fabrication, falsification, plagiarism or other research misconduct).	☒

4) The coordinator confirms:

- to have carried out the self-check of the financial capacity of the organisation on http://ec.europa.eu/research/participants/portal/desktop/en/organisations/lfv.html or to be covered by a financial viability check in an EU project for the last closed financial year. Where the result was "weak" or "insufficient", the coordinator confirms being aware of the measures that may be imposed in accordance with the H2020 Grants Manual (Chapter on Financial capacity check); or	◉
- is exempt from the financial capacity check being a public body including international organisations, higher or secondary education establishment or a legal entity, whose viability is guaranteed by a Member State or associated country, as defined in the H2020 Grants Manual (Chapter on Financial capacity check); or	○
- as sole participant in the proposal is exempt from the financial capacity check.	○

5) The coordinator hereby declares that each applicant has confirmed:

- they are fully eligible in accordance with the criteria set out in the specific call for proposals; and	☒
- they have the financial and operational capacity to carry out the proposed action.	☒

The coordinator is only responsible for the correctness of the information relating to his/her own organisation. Each applicant remains responsible for the correctness of the information related to him and declared above. Where the proposal to be retained for EU funding, the coordinator and each beneficiary applicant will be required to present a formal declaration in this respect.

According to Article 131 of the Financial Regulation of 25 October 2012 on the financial rules applicable to the general budget of the Union (Official Journal L 298 of 26.10.2012, p. 1) and Article 145 of its Rules of Application (Official Journal L 362, 31.12.2012, p.1) applicants found guilty of misrepresentation may be subject to administrative and financial penalties under certain conditions.

Personal data protection

The assessment of your grant application will involve the collection and processing of personal data (such as your name, address and CV), which will be performed pursuant to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Unless indicated otherwise, your replies to the questions in this form and any personal data requested are required to assess your grant application in accordance with the specifications of the call for proposals and will be processed solely for that purpose. Details concerning the purposes and means of the processing of your personal data as well as information on how to exercise your rights are available in the privacy statement. Applicants may lodge a complaint about the processing of their personal data with the European Data Protection Supervisor at any time.

Your personal data may be registered in the Early Detection and Exclusion system of the European Commission (EDES), the new system established by the Commission to reinforce the protection of the Union's financial interests and to ensure sound financial management, in accordance with the provisions of articles 105a and 108 of the revised EU Financial Regulation (FR) (Regulation (EU, EURATOM) 2015/1929 of the European Parliament and of the Council of 28 October 2015 amending Regulation (EU, EURATOM) No 966/2012) and articles 143 - 144 of the corresponding Rules of Application (RAP) (COMMISSION DELEGATED REGULATION (EU) 2015/2462 of 30 October 2015 amending Delegated Regulation (EU) No 1268/2012) for more information see the Privacy statement for the EDES Database.

2 - Participants & contacts

#	Participant Legal Name	Country	Action
1	INTERSPREAD GmbH	Austria	
2	ERASMUS UNIVERSITEIT ROTTERDAM	NL	
3	TIME.LEX	BE	
4	FUNDACION PRIVADA HOSPITAL ASIL DEGRANOLLERS	ES	
5	COOPERATIVA SOCIALE COOSS MARCHE ONLUS SOCIETA COOPERATIVA PER AZIONI	IT	
6	ARBEITER SAMARITER BUND WIEN GESUNDHEITS UND SOZIALE DIENSTE GEMEINNUTZIGE GMBH	AT	
7	Johanniter International	BE	
8	European Association for Directors and Providers of Long-Term Care Services for the Elderly a.s.b.l.	LU	

2 - Administrative data of participating organisations

PIC	***Legal name***
949361020	*INTERSPREAD GmbH*

Short name: INSP

Address of the organisation

Street Holochergasse 20/4

Town Wien

Postcode 1150

Country Austria

Webpage www.interspread.com

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....no

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....no

Legal person .....yes

Industry (private for profit).....yes

Enterprise Data

SME self-declared status.....31/12/2015 - yes

SME self-assessment .....31/12/2015 - yes

SME validation sme..... unknown

Based on the above details of the Beneficiary Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Research & Development ☐ not applicable

☒ Same as proposing organisation's address

Street: Holochergasse 20/4

Town: Wien

Postcode: 1150

Country: Austria

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr. Sex: (•) Male ( ) Female

First name: **Florian** Last name: **Huber**

E-Mail: **florian.huber@interspread.com**

Position in org.: Research Manager

Department: Research and Innovation ☐ Same as organisation name

☒ Same as proposing organisation's address

Street: Holochergasse 20/4

Town: Wien Post code: 1150

Country: Austria

Website:

Phone: +xxx xxxxxxxxx Phone 2: +xxx xxxxxxxxx Fax: +xxx xxxxxxxxx

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Flora	Strohmeier	flora.strohmeier@interspread.com	+xxx xxxxxxxxx
Julia	Haller	julia.haller@interspread.com	+xxx xxxxxxxxx

PIC	***Legal name***
999839335	*ERASMUS UNIVERSITEIT ROTTERDAM*

Short name: EUR

Address of the organisation

Street BURGEMEESTER OUDLAAN 50

Town ROTTERDAM

Postcode 3062 PA

Country Netherlands

Webpage www.eur.nl

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....yes

Non-profit .....yes

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....yes

Research organisation .....yes

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status.....01/10/2008 - no

SME self-assessment ..... unknown

SME validation sme.....01/10/2008 - no

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Department of Media and Communication ☐ not applicable

☐ Same as proposing organisation's address

Street: P.O. Box 1738

Town: Rotterdam

Postcode: 3000 DR

Country: Netherlands

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr.

Sex: (•) Male ( ) Female

First name: **Jason**

Last name: **Pridmore**

E-Mail: **pridmore@eshcc.eur.nl**

Position in org.: Assistant Professor

Department: Department of Media and Communication

☐ Same as organisation name

☐ Same as proposing organisation's address

Street: P.O. Box 1738

Town: Rotterdam

Post code: 3000 DR

Country: Netherlands

Website: https://www.eshcc.eur.nl/english/media/

Phone: +31 10 4089133

Phone 2: *+xxx xxxxxxxxx*

Fax: *+xxx xxxxxxxxx*

PIC	***Legal name***
991228063	*TIME.LEX*

Short name: TLX

Address of the organisation

Street JOSEPH STEVENSSTRAAT 7

Town BRUSSEL

Postcode 1000

Country Belgium

Webpage www.timelex.eu

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....no

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....no

Legal person .....yes

Industry (private for profit).....yes

Enterprise Data

SME self-declared status.....30/06/2017 - yes

SME self-assessment .....30/06/2017 - yes

SME validation sme.....18/06/2007 - yes

Based on the above details of the Beneficiary Registry the organisation is an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

No department involved

Department name: *Name of the department/institute carrying out the work.* ☒ not applicable

☐ Same as proposing organisation's address

Street: *Please enter street name and number.*

Town: *Please enter the name of the town.*

Postcode: *Area code.*

Country: *Please select a country*

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Mr. Sex: (•) Male ( ) Female

First name: **Jos** Last name: **Dumortier**

E-Mail: **jos.dumortier@timelex.eu**

Position in org.: Project Manager

Department: TIME.LEX ☒ Same as organisation name

☒ Same as proposing organisation's address

Street: JOSEPH STEVENSSTRAAT 7

Town: BRUSSEL Post code: 1000

Country: Belgium

Website: www.timelex.eu

Phone: +32 (0)2 893 20 95 Phone 2: *+xxx xxxxxxxxx* Fax: *+xxx xxxxxxxxx*

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Pieter	Gryffroy	pieter.gryffroy@timelex.eu	*0032 (0)2 893 20 95*

PIC	***Legal name***
989783830	*FUNDACION PRIVADA HOSPITAL ASIL DEGRANOLLERS*

Short name: FHAG

Address of the organisation

Street AVENIDA FRANCESC RIBAS S N

Town GRANOLLERS

Postcode 08402

Country Spain

Webpage http://www.fphag.cat/

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....yes

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....yes

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status.....17/05/2005 - no

SME self-assessment ..... unknown

SME validation sme.....17/05/2005 - no

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Research and Innovation Area ☐ not applicable

☒ Same as proposing organisation's address

Street: AVENIDA FRANCESC RIBAS S N

Town: GRANOLLERS

Postcode: 08402

Country: Spain

Department 2

Department name: Information Systems Direction ☐ not applicable

☒ Same as proposing organisation's address

Street: AVENIDA FRANCESC RIBAS S N

Town: GRANOLLERS

Postcode: 08402

Country: Spain

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr. | Sex: ○ Male ◉ Female

First name: **Diana** | Last name: **Navarro**

E-Mail: **diananavarro@fhag.es**

Position in org.: head of research and innovation

Department: research and innovation area ☐ Same as organisation name

☒ Same as proposing organisation's address

Street: AVENIDA FRANCESC RIBAS S N

Town: GRANOLLERS | Post code: 08402

Country: Spain

Website: www.fhag.es

Phone: +34-938425000 | Phone 2: +34-675741778 | Fax: +xxx xxxxxxxxx

Other contact persons

First Name	*Last Name*	*E-mail*	*Phone*
anna	benavent	abenavent@fhag.es	+xxx xxxxxxxxx
mercè	ratera	mratera@fhag.es	+xxx xxxxxxxxx

PIC	***Legal name***
999631464	*COOPERATIVA SOCIALE COOSS MARCHE ONLUS SOCIETA COOPERATIVA PER AZIONI*

Short name: COOSS

Address of the organisation

Street VIA SAFFI 4

Town ANCONA

Postcode 60121

Country Italy

Webpage www.cooss.marche.it

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....yes

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....yes

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status.....25/06/2014 - no

SME self-assessment ..... unknown

SME validation sme..... unknown

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Research and Training ☐ not applicable

☒ Same as proposing organisation's address

Street: VIA SAFFI 4

Town: ANCONA

Postcode: 60121

Country: Italy

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr. | Sex: ○ Male ◉ Female

First name: **Francesca** | Last name: **Cesaroni**

E-Mail: **f.cesaroni@cooss.marche.it**

Position in org.: Project manager

Department: Research and Training ☐ Same as organisation name

☒ Same as proposing organisation's address

Street: VIA SAFFI 4

Town: ANCONA | Post code: 60121

Country: Italy

Website: www.cooss.it

Phone: +39 07150103212 | Phone 2: +xxx xxxxxxxxx | Fax: +39 07150103206

PIC	***Legal name***
953977735	*ARBEITER SAMARITER BUND WIEN GESUNDHEITS UND SOZIALE DIENSTE GEMEINNUTZIGE G*

Short name: SAM

Address of the organisation

Street PILLERGRASSE 24

Town WIEN

Postcode 1150

Country Austria

Webpage www.samariterwien.at

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....yes

International organisation .....no

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....no

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status.....12/08/2001 - no

SME self-assessment ..... unknown

SME validation sme.....12/08/2001 - no

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Research and Training ☐ not applicable

☒ Same as proposing organisation's address

Street: PILLERGRASSE 24

Town: WIEN

Postcode: 1150

Country: Austria

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Dr. Sex: ○ Male ◉ Female

First name: **Petra** Last name: **Hellmich**

E-Mail: **petra.hellmich@samariterbund.net**

Position in org.: Head of Department

Department: Department of Home Care Services ☐ Same as organisation name

☒ Same as proposing organisation's address

Street: PILLERGRASSE 24

Town: WIEN Post code: 1150

Country: Austria

Website:

Phone: +xxx xxxxxxxxx Phone 2: +xxx xxxxxxxxx Fax: +xxx xxxxxxxxx

Other contact persons

First Name	*Last Name*	*E-mail*	*Phone*
Sigrid	Panovsky	sigrid.panovsky@samariterbund.net	+xxx xxxxxxxxx

PIC	***Legal name***
940895054	*Johanniter International*

Short name: JOIN

Address of the organisation

Street Rue Joseph II 166

Town Brussels

Postcode 1000

Country Belgium

Webpage www.johanniter.org

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....yes

International organisation .....yes

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....no

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status.....14/06/2006 - no

SME self-assessment ..... unknown

SME validation sme..... unknown

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Head Office ☐ not applicable

☒ Same as proposing organisation's address

Street: Rue Joseph II 166

Town: Brussels

Postcode: 1000

Country: Belgium

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Mr. Sex: (•) Male ( ) Female

First name: **Joachim** Last name: **Berney**

E-Mail: **joachim.berney@johanniter.org**

Position in org.: General Manager

Department: HEad Office ☐ Same as organisation name

☒ Same as proposing organisation's address

Street: Rue Joseph II 166

Town: Brussels Post code: 1000

Country: Belgium

Website: www.johanniter.org

Phone: +32 (0) 2 282 1045 Phone 2: *+xxx xxxxxxxxx* Fax: *+xxx xxxxxxxxx*

Other contact persons

First Name	***Last Name***	***E-mail***	***Phone***
Georg	Aumayr	georg.aumayr@johanniter.at	*+43 676 83 112 814*

PIC	***Legal name***
953335692	*European Association for Directors and Providers of Long-Term Care Services for the Elderly a.s.b.l.*

Short name: EDE

Address of the organisation

Street avenue Marie-Thérèse 11

Town Luxembourg

Postcode 2132

Country Luxembourg

Webpage www.ede-eu.org

Legal Status of your organisation

Research and Innovation legal statuses

Public body .....no

Non-profit .....yes

International organisation .....yes

International organisation of European interest .....no

Secondary or Higher education establishment .....no

Research organisation .....no

Legal person .....yes

Industry (private for profit).....no

Enterprise Data

SME self-declared status..... unknown

SME self-assessment ..... unknown

SME validation sme..... unknown

Based on the above details of the Beneficiary Registry the organisation is not an SME (small- and medium-sized enterprise) for the call.

Department(s) carrying out the proposed work

Department 1

Department name: Research and Training ☐ not applicable

☒ Same as proposing organisation's address

Street: avenue Marie-Thérèse 11

Town: Luxembourg

Postcode: 2132

Country: Luxembourg

Dependencies with other proposal participants

Character of dependence	***Participant***	

Person in charge of the proposal

The name and e-mail of contact persons are read-only in the administrative form, only additional details can be edited here. To give access rights and basic contact details of contact persons, please go back to Step 4 of the submission wizard and save the changes.

Title: Mr.

Sex: (•) Male ( ) Female

First name: **Karel**

Last name: **Vostry**

E-Mail: **info@ede-eu.org**

Position in org.: Secretary

Department: European Association for Directors and Providers of Long-Term Care Service

☒ Same as organisation name

☐ Same as proposing organisation's address

Street: Na Pankráci 30

Town: Prague

Post code: 14000

Country: Czech Republic

Website: www.ede-eu.org

Phone: *+xxx xxxxxxxxx*

Phone 2: *+xxx xxxxxxxxx*

Fax: *+xxx xxxxxxxxx*

3 - Budget

No	Participant	Country	(A) Direct personnel costs/€	(B) Other direct costs/€	(C) Direct costs of sub-contracting/€	(D) Direct costs of providing financial support to third parties/€	(E) Costs of inkind contributions not used on the beneficiary's premises/€	(F) Indirect Costs / € (=0.25(A+B-E))	(G) Special unit costs covering direct & indirect costs / €	(H) Total estimated eligible costs / € (=A+B+C+D+F+G)	(I) Reimburse-ment rate (%)	(J) Max.EU Contribution / € (=H*I)	(K) Requested EU Contribution/ €
1	Interspread Gmbh	AT	180000	28000	0	0	0	52000,00	0	260000,00	100	260000,00	260000,00
2	Erasmus Universiteit Rotterdam	NL	97500	17000	0	0	0	28625,00	0	143125,00	100	143125,00	143125,00
3	Time.lex	BE	52800	15000	0	0	0	16950,00	0	84750,00	100	84750,00	84750,00
4	Fundacion Privada Hospital Asil	ES	83700	16000	0	0	0	24925,00	0	124625,00	100	124625,00	124625,00
5	Cooperativa Sociale Cooss Marche Onlus	IT	45150	20000	0	0	0	16287,50	0	81437,50	100	81437,50	81437,50
6	Arbeiter Samariter Bund Wien	AT	48000	16000	0	0	0	16000,00	0	80000,00	100	80000,00	80000,00
7	Johanniter International	BE	71300	20000	0	0	0	22825,00	0	114125,00	100	114125,00	114125,00
8	European Association For Directors	LU	66000	22000	0	0	0	22000,00	0	110000,00	100	110000,00	110000,00
	Total		644450	154000	0	0	0	199612,50	0	998062,50		998062,50	998062,50

4 - Ethics

1. HUMAN EMBRYOS/FOETUSES		Page
Does your research involve Human Embryonic Stem Cells (hESCs)?	○ Yes ◉ No	
Does your research involve the use of human embryos?	○ Yes ◉ No	
Does your research involve the use of human foetal tissues / cells?	○ Yes ◉ No	
2. HUMANS		**Page**
Does your research involve human participants?	○ Yes ◉ No	
Does your research involve physical interventions on the study participants?	○ Yes ◉ No	
3. HUMAN CELLS / TISSUES		**Page**
Does your research involve human cells or tissues (other than from Human Embryos/ Foetuses, i.e. section 1)?	○ Yes ◉ No	
4. PERSONAL DATA		**Page**
Does your research involve personal data collection and/or processing?	◉ Yes ○ No	74
Does it involve the collection and/or processing of sensitive personal data (e.g: health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction)?	○ Yes ◉ No	
Does it involve processing of genetic information?	○ Yes ◉ No	
Does it involve tracking or observation of participants?	○ Yes ◉ No	
Does your research involve further processing of previously collected personal data (secondary use)?	○ Yes ◉ No	
5. ANIMALS		**Page**
Does your research involve animals?	○ Yes ◉ No	
6. THIRD COUNTRIES		**Page**
In case non-EU countries are involved, do the research related activities undertaken in these countries raise potential ethics issues?	○ Yes ◉ No	
Do you plan to use local resources (e.g. animal and/or human tissue samples, genetic material, live animals, human remains, materials of historical value, endangered fauna or flora samples, etc.)?	○ Yes ◉ No	
Do you plan to import any material - including personal data - from non-EU countries into the EU?	○ Yes ◉ No	

Do you plan to export any material - including personal data - from the EU to non-EU countries?	◯ Yes ◉ No	
In case your research involves low and/or lower middle income countries, are any benefits-sharing actions planned?	◯ Yes ◉ No	
Could the situation in the country put the individuals taking part in the research at risk?	◯ Yes ◉ No	
7. ENVIRONMENT & HEALTH and SAFETY		Page
Does your research involve the use of elements that may cause harm to the environment, to animals or plants?	◯ Yes ◉ No	
Does your research deal with endangered fauna and/or flora and/or protected areas?	◯ Yes ◉ No	
Does your research involve the use of elements that may cause harm to humans, including research staff?	◯ Yes ◉ No	
8. DUAL USE		Page
Does your research involve dual-use items in the sense of Regulation 428/2009, or other items for which an authorisation is required?	◯ Yes ◉ No	
9. EXCLUSIVE FOCUS ON CIVIL APPLICATIONS		Page
Could your research raise concerns regarding the exclusive focus on civil applications?	◯ Yes ◉ No	
10. MISUSE		Page
Does your research have the potential for misuse of research results?	◯ Yes ◉ No	
11. OTHER ETHICS ISSUES		Page
Are there any other ethics issues that should be taken into consideration? Please specify	◯ Yes ◉ No	

I confirm that I have taken into account all ethics issues described above and that, if any ethics issues apply, I will complete the ethics self-assessment and attach the required documents. ☒

How to Complete your Ethics Self-Assessment

5 - Call-specific questions

Extended Open Research Data Pilot in Horizon 2020

If selected, applicants will by default participate in the Pilot on Open Research Data in Horizon 2020[1] , which aims to improve and maximise access to and re-use of research data generated by actions.

However, participation in the Pilot is flexible in the sense that it does not mean that all research data needs to be open. After the action has started, participants will formulate a Data Management Plan (DMP), which should address the relevant aspects of making data FAIR – findable, accessible, interoperable and re-usable, including what data the project will generate, whether and how it will be made accessible for verification and re-use, and how it will be curated and preserved. Through this DMP projects can define certain datasets to remain closed according to the principle "as open as possible, as closed as necessary". A Data Management Plan does not have to be submitted at the proposal stage.

Furthermore, applicants also have the possibility to opt out of this Pilot completely at any stage (before or after the grant signature). In this case, applicants must indicate a reason for this choice (see options below).

Please note that participation in this Pilot does not constitute part of the evaluation process. Proposals will not be penalised for opting out.

We wish to opt out of the Pilot on Open Research Data in Horizon 2020.	○ Yes	◉ No

Further guidance on open access and research data management is available on the participant portal: http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-dissemination_en.htm and in general annex L of the Work Programme.

[1] *According to article 43.2 of Regulation (EU) No 1290/2013 of the European Parliament and of the Council, of 11 December 2013, laying down the rules for participation and dissemination in "Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020)" and repealing Regulation (EC) No 1906/2006.*

HORIZON 2020 | COORDINATION AND SUPPORT ACTION (CSA) | SU-TDS-03-2018

TECHNICAL ANNEX | SECTION 1-3

SecureHospitals.eu

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

Topic: Raising awareness and developing training schemes on cybersecurity in hospitals

Coordinator Contact: Dr. Florian Huber INTERSPREAD GmbH, florian.huber@interspread.com

List of Participants:

NO.	PARTICIPANT ORGANISATION NAME	ACRONYM	COUNTRY
1	**INTERSPREAD GMBH** (COORDINATOR) RESEARCH AND DEVELOPMENT DEPARTMENT	**INSP**	AUSTRIA
2	**ERASMUS UNIVERSITEIT ROTTERDAM** DEPARTMENT OF MEDIA AND COMMUNICATION	**EUR**	NETHERLANDS
3	**TIME.LEX CVBA** N/A	**TLX**	BELGIUM
4	**FUNDACIÓ PRIVADA HOSPITAL ASIL DE GRANOLLERS** RESEARCH AND INNOVATION UNIT	**FPHAG**	SPAIN
5	**COOSS MARCHE ONLUS** RESEARCH & TRAINING DEPARTMENT	**COOSS**	ITALY
6	**ARBEITER-SAMARITER-BUND WIEN GESUNDHEITS- UND SOZIALE DIENSTE GEMEINNÜTZIGE GMBH** DEPARTMENT OF HOME CARE SERVICES	**SAM**	AUSTRIA
7	**JOHANNITER INTERNATIONAL** N/A	**JOIN**	BELGIUM
8	**EUROPEAN ASSOCIATION FOR DIRECTORS AND PROVIDERS OF LONG-TERM CARE SERVICES FOR THE ELDERLY (E.D.E.) ABSL.**	**EDE**	CZECH REPUBLIC

***Coordination**

This proposal version was submitted by **Flora Strohmeier** on **25/04/2018 13:32:54** Brussels Local Time. Issued by the Participant Portal Submission Service.

ABSTRACT

Cybercrime has recently shifted from attacking big corporations to smaller industries, like financial services as well as the healthcare sector. Especially in the last area the trend is rising, where hackers are targeting patient health devices that are connected to the internet. Most cases include stealing patient information and encrypting it for ransom money. The big problem is interconnection, each application or device that runs on the networks represents a possible entry point for a cyber-physical attack. So far, most hackers infected hospital software with ransomware to prevent staff from accessing patient records or scheduling appointments. But capable terrorists would also be able, to render active medical devices not just useless, but deadly. Complete cybersecurity in the health sector is unachievable, and would exceed financial means; nevertheless, vital steps can be taken to minimize the risk of cyber- attacks against healthcare facilities. Around 85 percent of targeted cyber-attacks would be preventable if basic protection protocols would be established. The SecureHospitals.eu project seeks to raise awareness on risks and protection opportunities, setup training schemes and the initiate training sessions for IT staff working in hospitals. Through several training approaches, the project will boost the level of training in cybersecurity in Europe, improve the knowledge of staff and in turn contribute to decreased vulnerabilities against cyberthreats and increased patient trust and safety.

Keywords: Cybersecurity; Data Protection; Hospitals; Care Centres; Trainings; MOOC;

Table of Contents

1. EXCELLENCE 4

1.1 Objectives 4

1.1.1 Project Background and Challenges 4
1.1.2 Main Objectives 6
1.1.3 Detailed Description of the Objectives 6

1.2 Relation to the work programme 8

1.3 Concept and Methodology 9

1.3.1 Concept Graph 9
1.3.2 Overall Concept and Methodology 10
1.3.3 Links to other projects and activities 17
1.3.4 Further aspects and considerations 21

2. IMPACTS 22

2.1 Expected impacts 22

2.2 Measures to maximise impact 23

2.2.1 Dissemination and Exploitation of Results 23
2.2.2 Dissemination and Exploitation Strategy 23
2.2.3 Data and Knowledge Strategy 25
2.2.4 Communication activities 27

3. IMPLEMENTATION 29

3.1 Work plan, Work packages, Deliverables and Milestones 29

3.2 Management structure and procedures 43

3.2.1 Project Committee 44
3.2.2 Coordinator 44
3.2.3 Expert & Advisory Board (EAB) 44
3.2.4 Decision making mechanism 44
3.2.5 Conflict resolution 45
3.2.6 Risk & Innovation Management 45
3.2.7 Milestones and Critical Risks 45

3.3 Consortium as a whole 47

3.4 Resources to be committed 48

3.4.1 Summary of staff effort and resource distribution 49
3.4.2 Other costs 49

1. EXCELLENCE

1.1 Objectives

1.1.1 Project Background and Challenges

In the global race for economic competitiveness, the digital readiness of economies has become a key factor. Therefore, with growing digitalisation, cybersecurity has become an increasingly important safety issue. Larger industries or governments have already experienced frequent cyberattacks over the last decade, with the trend growing. In fact, everyone is affected by the connection of the World Wide Web and therefore needs to adept to threats from outside.

Now, cybercrime has shifted from attacking big cooperation's to smaller industries, like financial services and especially the healthcare sector. Especially in the latter the trend is rising, the healthcare network has now become the most targeted sector globally:

In 2015 alone, over 110 million patients in the US had their data compromised and 81% of surveyed organisations where victim of an attack.[1] A report by CynergisTek, an industry leader in health information privacy revealed that in 2016 healthcare providers experienced a 320% increase of hacker attacks. This year was also the first in which a major American hospital was victim of ransomware.[2] Aside from that, many smaller institutions and clinics were targets of frequent hacker attacks. Data breaches cost the health care industry approximately $5.6 billion every year, according to Becker's Hospital Review.[3]

The healthcare industry has now become the primary target of hackers, the reason for this shift from other industries is clear: While attack-experienced actors where more involved in implementing cybersecurity, so far, the topic has never been a big part of the agenda in healthcare, and therefore not received much attention in the first place. As a result, cybersecurity in healthcare is generally barely present, therefore huge security gaps are left for hackers to enter.

Another reason for this shift is the possible high profit for the data. Other than banks, hospitals have valuable data stored, that can be stolen and separately sold online. It can also be used for fraudulent schemes; criminals can use stolen medical data for decades before it´s discovered. Blackmailing the hospital is another option, making patients data 60 times costlier than credit cards. [4]

A third important aspect is the interconnectivity of hospitals and the medical devices within. Since most medical electronics are connected through the World Wide Web, they can easily be hacked and therefore used as gateways attack other devices as well. They can however, also be manipulated themselves: So far, most hackers infected hospital software with ransomware to prevent staff from accessing patient records or scheduling appointments. But capable terrorists would also be able, to render active medical devices not just useless, but deadly.[5]

This makes perfectly clear that the healthcare industry needs drastically improve its cybersecurity: It is important to raise awareness and to create an IT-policy. At the same time, around 85 percent of targeted cyber-attacks would be preventable if basic protection protocols would be established. Studies suggest that internal actors are often the biggest factor of data leaks. Many employees are just unaware of the risks in data security, which makes proper staff training necessary. Since Cybersecurity is considered as an IT-problem, most employees don't care or don't understand their own role in this context. Sometimes

[1] https://www.bmj.com/content/358/bmj.j3179
[2] https://www.businesswire.com/news/home/20170215005465/en/CynergisTek-Releases-Redspin-Annual-Report-State-Cybersecurity
[3] https://healthinformatics.uic.edu/resources/articles/cybersecurity-how-can-it-be-improved-in-health-care/
[4] https://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html
[5] Ayala, L (2016) Cybersecurity for Hospitals and Healthcare Facilities: A Guide to Detection and Prevention. Fredericksburg, Virginia

even no one is in charge of IT security at all. In this regard the problem is often completely ignored. Therefore, the aspect of Human error, (which can encompass simple mis delivery of personal info, improper data management or even too public display of vital data is common.

Another aspect is conscious data breach by employees, mostly because of financial gains (like tax fraud) but also just for fun. Statistics show that 38% of security breaches are internal, with a 2015 study[6] from the University of Alabama at Birmingham revealing that three out of four companies view employee negligence as the greatest breach threat. The study also found that around 75% of employees upload classified work files to personal cloud accounts. Eighteen percent of healthcare employees would sell confidential data like login credentials or opting to install tracking software to third parties for less than $1000.

Many of the cyber breaches can be avoided completely if a simple security culture is established and the employees are more involved in the process. The importance of awareness raising and training the employees in security measures can be illustrated by some example figures: 38% of all breaches are internal. 75% of employees upload classified work files to personal cloud accounts.[7] KPMG has detected that most breaches concern false sharing of data with third parties, employee theft or inadequate firewalls.[8]

In this context, equipment, software and hardware should also be overlooked: It is important to understand how vital information is stolen by a hacker and what can be done to prevent that. Data can easily be acquired by detaching or even stealing medical equipment that is not properly supervised or secured. Another aspect in this is the transfer of data via attachable storage like USB, hard drives, CD etc. Outdated software or security measures are another big security issue: Old equipment is often set on default settings and passwords, which feature therefore already known exploits and openings for hackers.

To conclude, the existing challenges and threats can be summarized as follows:

Staff/Internal: Inside threats contribute the most to breaches. This can be due to ignorance or conscious mishandling data. Hospitals should establish a cybersecurity culture/department and raise awareness towards the issue. Frequent employee training, maintaining good computer habits and do´s and don'ts of handling patient's data should be long term projects within all institutions.

Software: Patches and software updates, as well as firewalls and antivirus programs should be mandatory. Intrusion detection systems should be installed and used. Frequent checking of unusual behavior of PCs (like shutdowns) should be monitored a reported immediately.

Interconnection: medical devices as well as the entire healthcare network itself are highly connected, therefore making it easy for a hacker to spread his influence. This interconnectivity brings therefore a challenge.

To respond to these challenges, the SecureHospitals.eu project seeks to create a community of practice, supported by online approaches to raise awareness on the threats and opportunities and boost the level and quality of training of IT staff in hospitals. The consortium represents a broad geographical representation and conglomeration of skills and experience in awareness raising and community building activities, technical developments, legal expertise on data protection, cybersecurity and IT as well as in conducting trainings to convey acquired knowledge. For a period of 26 months, the project seeks to engage all stakeholders in the IT security in healthcare in Europe to improve preparedness and the find common solutions against cyberthreats to patient data. The following sections provide an overview and detailed descriptions of the project objectives and the means of their implementation in work packages.

[6] http://www.verizon.com/about/news/new-report-puts-healthcare-cybersecurity-back-under-microscope
[7] https://businessdegrees.uab.edu/resources/infographics/promoting-data-security-in-the-workplace/
[8] KPMG, (2016) HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities.

1.1.2 Main Objectives

MAIN OBJECTIVES	
(O1)	**RAISE** awareness among decision makers and ICT practitioners in hospitals and care centres across Europe on the importance cybersecurity and continuous training of all affected staff.
(O2)	**AGGREGATE** all existing knowledge on cybersecurity in hospitals filtering the most relevant for the development of high quality trainings supported by innovative e-approaches.
(O3)	**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective uptake of knowledge on data protection and privacy and cybersecurity measures.
(O4)	**TRAIN** the trainers and practitioners all over Europe using different online and on-site training methods targeting stakeholders at the European and the local level.
(O5)	**COMMUNICATE** training needs, developments of the training schemes, project training initiatives and further awareness raising on the online awareness and information hub.

1.1.3 Detailed Description of the Objectives

O1 **RAISE** awareness among decision makers and ICT practitioners in hospitals and care centres across Europe on the importance cybersecurity and continuous training of all affected staff.

This objective is understood as an initial step for the achievement of the rest of the main actions and output aimed by the project. In order to the achieve a deep understanding on the status-quo of training and training materials in the field, this objective seeks to bring together all types of involved stakeholders – training providers, training seekers, decision makers at the hospitals level as well as researchers and policy makers in the area of cyber security, data protection, privacy etc. To do so, the aim will be to map all main stakeholders at the European and national level, and existing knowledge generated by related projects and initiatives. In order to stay up to date with additional knowledge produced by relevant sources, the aim of this objective will be to also to map all relevant knowledge sources (institutes, actors, stakeholders, projects etc.) that can be relevant for trainers to access information on new tools and recommendations in the future. An online awareness and information hub will be created aggregating all the knowledge and supporting the awareness raising activities across Europe and beyond. An extensive stakeholder collection and involvement roadmap lay the foundations of the awareness raising activities seeking to cover all healthcare centres in Europe, neighbouring regions and beyond.

The steps toward the achievement of this objective are set out in the tasks of Work Package 2: **INVOLVE: HOSPITALS AND PRACTITIONERS VIA AN ONLINE AWARENESS AND INFORMATION HUB**. The achievement of the objective is marked with Milestone **M4** in the workplan.

O2 **AGGREGATE** all existing knowledge on cybersecurity in hospitals filtering the most relevant for the development of high quality trainings supported by innovative e-approaches.

This objective is understood as an initial step for the achievement of the rest of the main actions and outputs aimed by the project. In order to the achieve a deep understanding of existing trainings of IT staff in hospitals, this objective seeks to map curricula of existing training courses and training providers. As knowledge providers on the topic – sought to be collected by the first objective – include different types of actors and types of relevant knowledge, e.g. data protection and privacy policies and regulations, cybersecurity measures, minimum requirements etc. it is essential for training seekers but also training providers to find structured knowledge sources that help in the development of new course curricula, and supportive training materials. The course collection resulting from this action will be implemented online in the open information hub and become a powerful tool for training seekers.

The steps toward the achievement of this objective are set out in the tasks of Work Package 3: **AGGREGATE: EXISTING KNOWLEDGE AND APPROACHES ON CYBERSECURITY IN HOSPITALS**. The achievement of the objective is marked with Milestone **M3** in the workplan.

O3	**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective uptake of knowledge on data protection and privacy and cybersecurity measures.

The aim of this objective is to build solid training schemes and materials considering the assessed needs of practitioners and gaps existing trainings. Current training materials seem to be either incomplete, using mainly traditional training forms that limit access to a small group of training seekers, or lacking tailor-made materials for various knowledge levels (basic, advance, trainer etc.), topics and counter measures. The training curricula and materials developed by the project seek to incorporate different training methods considered as novelty in the field (MOOCs, Webinars, m-learning etc.). The developed curricula and materials will be primarily used in for the training package delivered in the project. However, it also seeks to propose approaches outside the scope of the project such as m-Learning (mobile learning comprising any type of training offered through the use do mobile devices such as smartphone applications etc.). These materials will be available to trainers and training organisation that wish to develop new training methods and curricula. A crucial aspect that will be developed through the accomplishment of this objective is the development of the step-by-step tools for trainers to develop curricula that fit the needs of specific training seeker groups. To achieve this objective, the consortium will map and collect existing courses and training programmes on cyber security in hospitals and other healthcare centres collect insights from trainers and other experts that are involved in training design and delivery. The steps toward the achievement of this objective are set out in the tasks of Work Package 3: **CREATE: STRUCUTRED TRAINING SCHEMES AND CURRICULA FOR HOSPITAL STAFF AND TRAINERS**. The achievement of the objective is marked with Milestone **M5** in the workplan.

O4	**TRAIN** the trainers and practitioners all over Europe using different online and on-site training methods targeting stakeholders at the European and the local level.

This objective sets out the second main type of action in the proposal. The rationale behind it is to put in practice the produced training materials and in turn increase the uptake by the training providers and training seekers alike. The offered trainings will incorporate novel methods that ensure wide participation of training-seekers from different regions, levels of knowledge and genders. The design and running of a MOOC for training IT staff of various disciplines, will ensure that man and women researchers of senior and junior level from all over Europe can receive quality training fit for their needs. Besides the MOOC several webinars will train specific training seekers on specific issues related to cybersecurity in hospitals. Other trainings happening at the local level will build a wide community of newly trained IT staff working in hospitals and healthcare centres. The steps toward the achievement of this objective are set out in the tasks of Work Package 5: **BOOST: TRAINING INITIATIVES IN HOSPITALS AND INTEGRATION OF PROVIDERS AND COURSES.** The achievement of the objective is marked with Milestone **M6**, **M7** and **M8** in the workplan.

O5	**COMMUNICATE** training needs, developments of the training schemes, project training initiatives and further awareness raising on the online awareness and information hub.

In order to promote and extensive uptake of the developed training schemes and materials and a vast participation in the MOOC, the webinars but also in the rest of the training activities, the project seeks to use the full potential of communication and dissemination mechanisms to increase its impact in the field. To achieve this the project will maintain a strong online presence through a project website, social media accounts and presence in all potential online channels. Secondly, the aim will be to disseminate the results and activities in the scientific community by writing articles on external blogs, science magazines,

attending external events such as conferences and other networking spaces to present the project, share its findings etc. One of the integral parts of this objective will also be the organisation of a major conference targeting cybersecurity specialists, legal experts, trainers, officials responsible for training of staff at hospital level, higher level decision makers etc. to reflect on the project outcomes and set priorities for future needs and developments.

The steps toward the achievement of this objective are set out in the tasks of Work Package 6: **COMMUNICATE: AWARNESS RAISING ON PROJECT ACTIVITIES AND PROMOTION OF THE HUB.** The achievement of the objective is marked with Milestone **M2** and **M9** in the workplan.

1.2 Relation to the work programme

The SecureHospitals.eu project directly responds to the call SU-TDS-03-2018 for 'Raising awareness and developing training schemes on cybersecurity in hospitals'. As such, each of the objectives, actions and single task in the workplan were set out towards the fulfilment of the requirements put forward by the call. The following sections describe how the actions of SecureHospitals.eu respond to call text:

*	**Awareness raising of staff working in healthcare settings on security and data privacy**

Objective 1, implemented in Work Package 2, is fully dedicated to awareness raising activities at the primary stage of the project, seeking to involve all stakeholders in the creation of an open awareness and information hub. An extensive stakeholder collection and the involvement strategy will ensure the awareness raising activities are effective and target the full potential range of stakeholders in Europe. Besides the staff working in healthcare settings, the awareness raising campaigns will also address related stakeholders such as the officials responsible for the training of staff in hospitals, legal experts on cyber and data privacy issues, training designers, training providing organisations etc. The awareness raising activities in Objective 1/Work Package 2 are strongly interrelated to Objective 5/Work Package 6 that seeks to communicate the project aims and activities.

*	**Training of IT staff working in healthcare settings**

These activities are planned under Work package 5 which lays in the heart of the project in its second half. These activities will design and run a MOOC using a collaborative online interaction model for seeking to maximise outreach, interaction and participant feedback. A summer school, and several webinars and local events will be additionally organised to boost training of IT practitioners in healthcare settings and collect needs and priorities for the development of future training courses. The training initiatives will tackle the most burning issues related to cybersecurity in healthcare settings, such as minimising vulnerabilities, implementing to protective measures to data security breaches, building strategies for quick and effective responses in the case of attacks etc. General knowledge on handling patient data in line with the latest legal requirements also aims to be effectively conveyed by the SecureHospitals.eu training mechanisms.

*	**Proactive managerial and technological strategies to reduce vulnerabilities**

Objective 3 that will be implemented by Work Package 4 is dedicated to the design of new course curricula for the training of trainers as well as IT practitioners including its full spectrum of topics. One of the main focuses of the newly developed training schemes will be to develop internal strategies that reduce the vulnerably of hospitals in becoming victims of cyber-attacks. Reducing vulnerabilities consists on the proper training of IT staff on handling patient data and as well as effective measures and strategies for data protection. This work package will also conceptualise tools to be implemented online for helping trainers develop new courses and for helping practitioners assess training needs online.

1.3 Concept and Methodology

1.3.1 Concept Graph

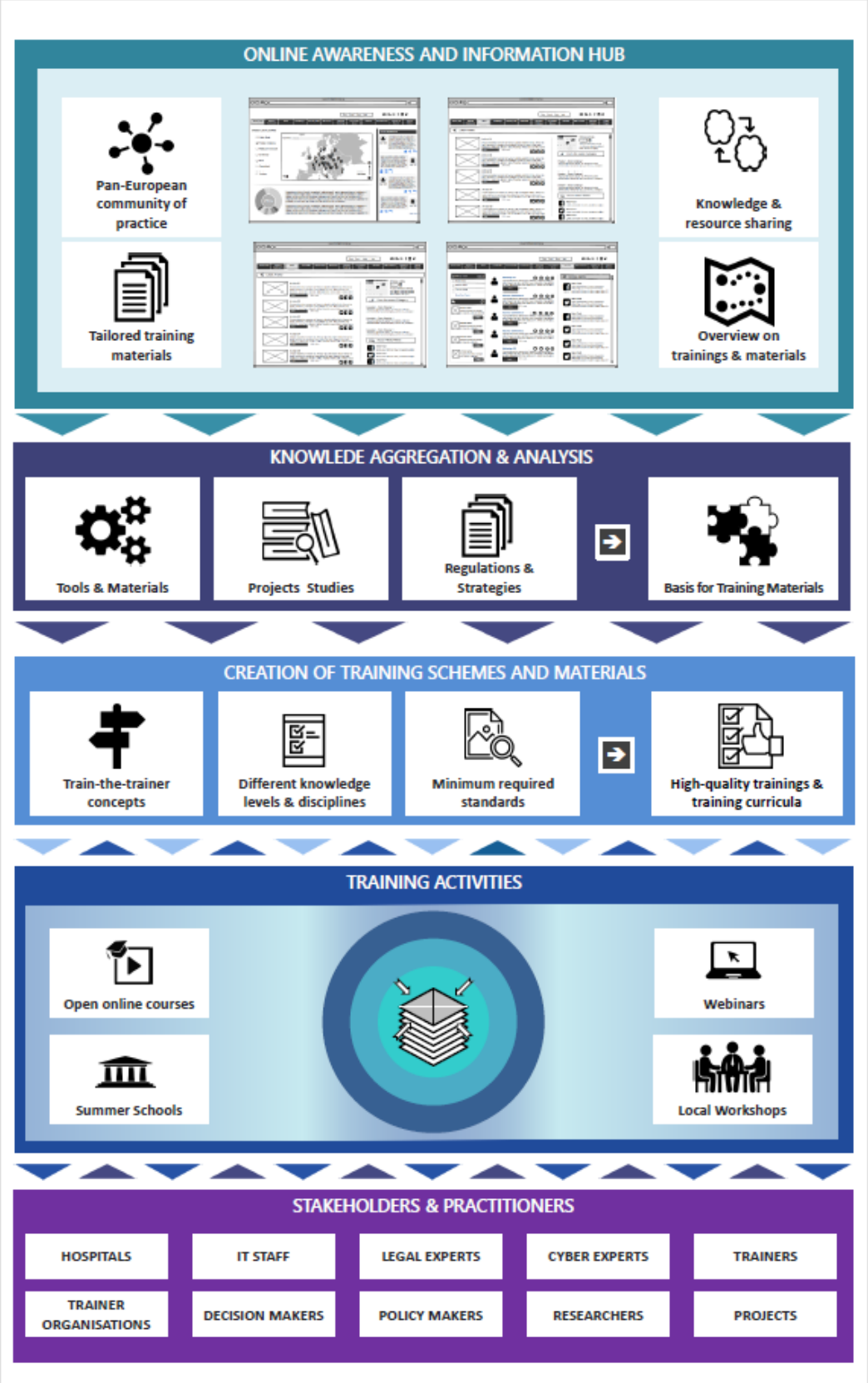


Figure 1: SecureHospitals.eu Concept Graph

1.3.2 Overall Concept and Methodology

A	AWARENESS RAISING AND COMMUNITY BUILDING

The primary action towards boosting training initiatives for cyber-security staff, improving the overall quality of training delivered and received and setting the priorities for future trainings and important topics, is to create a large community of stakeholders that share and receive information on the needs and actions. Besides extensive stakeholder collections and engagement through online communication means but also through direct involvement, the first project stage includes the development of an online setting that provides open information and awareness tools. The online information hub also seeks to supports the creation of an online community of practice brining together all involved stakeholder in the field of cyber security in the healthcare area. In the following sections, some exemplary parts of the online open information hub are visualized with the help of wireframes and mock-ups. SecureHospitals.eu will fulfil its role as a Coordination and Support Action by providing timely solutions and the means to implement these solutions for the challenges highlighted by stakeholder engagement. The online hub features various modules for knowledge and resource sharing based on these insights. These are planned and constructed as user-friendly and intuitive components for practitioners of at various career stages. The wireframes below illustrate the basic ideas of each module that will be developed within the SecureHospitals.eu.

1	Knowledge Base and Materials

This section will include the knowledge aggregated under objective 1 and delivered in its final format by task 3.4 in the form of a baseline report. The knowledge base will be interactive and include the following modules:

Library of resources: Including all knowledge materials relevant for trainers and practitioners mapped out. The resources will represent a basis for trainers to find a search for new training materials and also showcase theirs through uploading options.

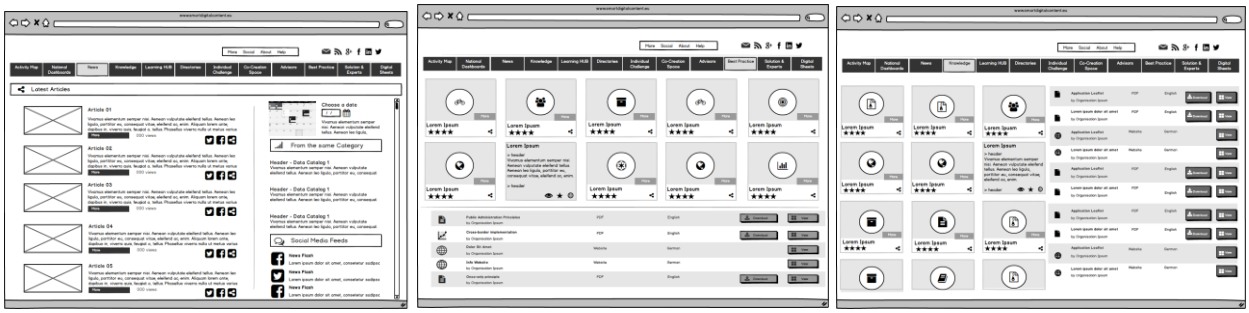


Figure 2: SecureHospitals.eu Knowledge Base Wireframes

2	Stakeholder Directories

Similar Initiatives and Projects: this section will map out all collected projects, training providers and materials relevant for training across Europe. These will act as information sources to trainers and practitioners to search for new sources of knowledge, activities and initiatives.

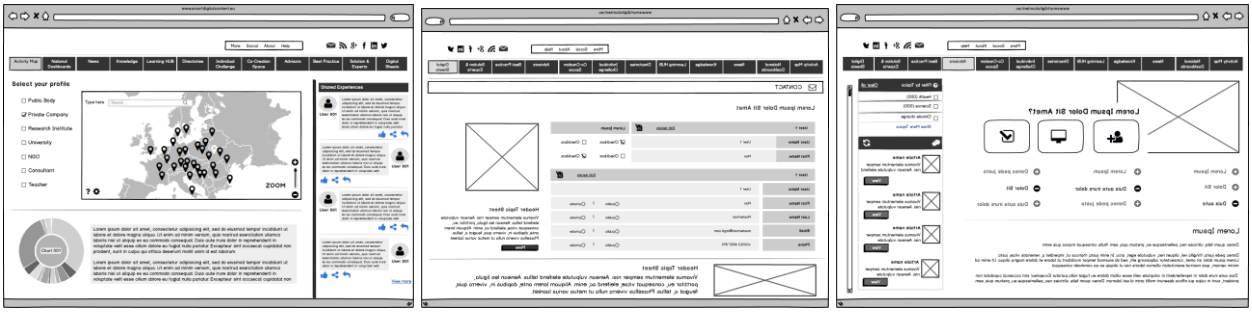


Figure 3: SecureHospitals.eu Stakeholder Directory Wireframes

3 Trainer and Trainer Organisation Profiles

Registration Forms will be the entry point of all actors in the cybersecurity in healthcare field. Training centres and other organisations offering courses, as well as trainers and solution providers (e-learning, digital solutions etc.) are one of the target groups which will be engaged during the project lifetime in order to ensure sustainability of the SecureHospitals.eu action beyond the funding timeframe.

Annotation Forms: Based on their expertise and portfolio each actor registering will be annotated by predefined parameters to ensure a good categorisation within the intelligence of the platform. Here they can also be connected to their network to support endorsement from peers.

Verification Dashboard: Project members and later platform hosts are verifying the registrations on based on categorisation and how robustly are they fitting to the requested course profiles in order to ensure the quality standards imposed by the community are properly upheld.

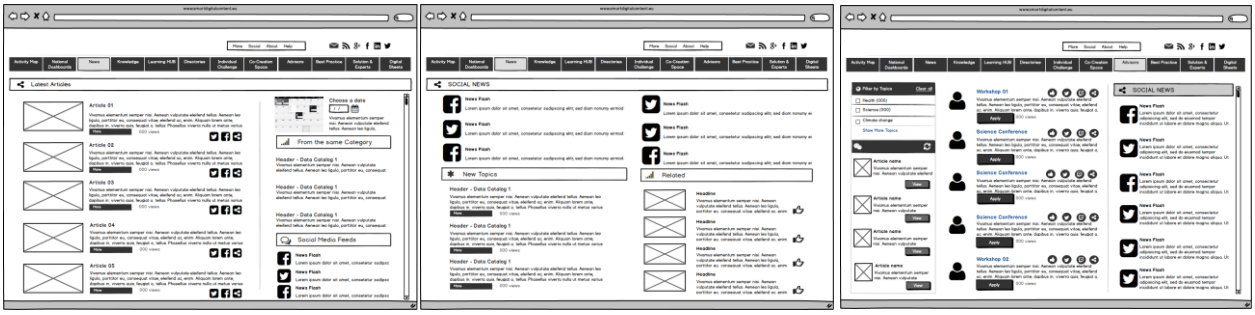


Figure 4: SecureHospitals.eu-Wireframes

4 Community of Practice

Figure 5: 'Community of Practice' Components

The term “Community of Practice” was proposed in 1991 by Jean Lave and Étienne Wenger when they debated the aspect of learning in the context of social relations. In doing so, they showed that - in addition to structures or models - participation in a community is crucial for knowledge acquisition.

The model of communities of practice is an attempt to show the "anatomy" of the interlocking of individual learning processes with those of the further development of the embedding social community. Therefore, the term describes a practice-oriented community of people who are informally connected, face similar tasks and want to learn from each other through interaction.

Structure: In the community of practice a certain structure is established, where everyone gets a specific role. This role is determined on the basis of their activity and the acceptance or rejection by other members. In this way an “Identity”, this is being formed by the distribution of tasks, which are being negotiated among the members. As a result, active and less active members, moderators and experts develop on the basis of the communication processes. These moderators should not be imagined as rigidly assigned positions within the network of communities of practice. They are also situational negotiated functions and tasks within the community. Sub-groups can also be formed or external persons can be integrated as guests.

Criteria: A list of criteria exists, which limit the idea of communities of practice and make it identifiable: The members participate in a joint undertaking ('Enterprise'), they build together in a tool pool ('Shared Repertoire of Tools'), they negotiate' standards and they participate in a common practice. In this practice, tasks are performed for the further development of the group but also of each individual who has joined this community for a specific reason. The criteria include but are not limited to: Having related enterprises, facing similar conditions, sharing historical roots, sharing artefacts, very quick setup of a problem to be discussed, local lore, shared stories, or inside jokes.

Benefits: Communities of practice offer a variety of benefits: Relationships within teams or between organizations are strengthened, the flow of communication is improved, implicit knowledge is made visible, and learning is faster and more efficient than in conventional training. Via the connections among the group within their community of practice, participants can acquire social capital in the process of sharing expertise that can provide value to the group and the individual.

Online Community: The online community of practice (also known as virtual community of practice) is a specific variation, which uses the World Wide Web. It meets the predefined criteria of Lave and Wenger and therefore includes active members in a specific area of interest. To assist in the creation, sharing and negotiation of knowledge, social structures are created online within the community. Since the original concept of a COP was based around situated learning, a debate exists whether virtual CoPs even can exist. In this context Wikipedia is mentioned as a possible virtual COP.

The SecureHospitals.eu community will include all types of stakeholders related to cybersecurity in healthcare settings, including the IT staff, the staff development officials, legal experts, trainers, training providers etc. Bringing all these types of stakeholders to discuss trends and needs will boost the quality of delivered training and in turn reduce vulnerabilities of healthcare centres to fall victims of cyber-attacks.

B KNOWLEDGE AGGREGATION

In order to acquire a detailed and comprehensive knowledge base for the development of training materials, a review of existing scientific literature, project reports and policies will be performed. The in-depth review of the materials and knowledge involves the analysis of legal frameworks, guidelines and existing best-practice measures for reducing vulnerability towards cyber-attacks. In parallel, contacts from major stakeholders will continue to be extensively collected. The knowledge and stakeholder directory are crucial for the empirical research as well as for the communication, dissemination and finally for the exploitation of the training materials through the organisation of project activities. This action is connected to Objective 1 and Work package 2 and the outcomes of the knowledge aggregation are measured with Milestone M3. Components of the knowledge base that will be implemented in the online information hub are described in detail below:

*	Awareness Raising and Empowerment

One important aspect for cybersecurity is the internal factor: Employees are responsible for managing, sharing and disposing vital data. Therefore, they are often a large part of the problem when it comes to mismanagement of data. This can be due to unawareness or conscious decision.

Staff awareness: Human error: One aspect is human error, which can have various reasons: Simple misdelivery of personal information, general improper data management or destruction of vital data, or even too public display. Employees need to be actively aware of these problems and that they could be abused by a possible intruder.
Staff awareness: Privacy and data sharing: Another aspect is conscious data breach, mostly because of financial gains (tax fraud) or just for fun. Statistics show that 38% of security breaches are internal, three out of four companies view employee negligence as the greatest breach threat. 75% of employees upload classified work files to personal cloud accounts.
IT-expertise group appointment: Many employees are generally unaware of the risks in data security - Since Cybersecurity is considered as an "IT-problem", other staffs does not care or does not understand its own important role. Sometimes even no one is in charge of it security at all and the problem is often completely ignored. Therefore, an elaborated plan needs to be established, that assigns everyone a certain role and displays the importance of the issue for everyone.
EU Data Protection Directive: The management (as well as the staff) needs to be aware of the binding regulations to prevent hefty fines. The common regulations should be taught.

*	Handbooks and Guidelines

Depending on the field, it can be helpful to have a comprehensive guideline at hand, that provides guidance in simple everyday tasks like data handling or understanding how to stop a hacker. The Handbook displays an overview of the possible challenges that need to be approached to make the hospital safer – as well as possibilities to overcome these problems.

How does a hacker work? When it comes to stealing private data from hospitals, a hacker has various techniques to reach his goal: Internet access, or direct theft are just a few of the gateways. A practical handbook can raise awareness about which gateways a hacker uses and how to minimise risk in those regards.

How to handle classified information: A big part of cybersecurity is to understand what an employee can do with private data – and what not. How to detect possible threats like fishing Emails? What kind of authorisation do I use? Who is allowed to ask information about a third party? It is important to understand how to handle delicate information – a guideline or checklist can display this in a comprehensive matter.

Reading the signs of an intruder: What happens if the hacker has already started his attack? An observant employee could already read the signs of a commenced attack and react to a possible threat before greater damage is done. The Guide could display what to look for on specific devices – from complicated machines like an X-ray to the simple computer. A checklist may display a quick summary of possible indicators for hacking (like frequent shutdowns etc.)

Establish a security culture: To start a comprehensive "security culture", where everyone is frequently taught and involved would be an important approach to the matter. This would take time and effort, but probably the most successful way to encircle al vital aspects and tackle the issue. A comprehensive guidebook would be a great support in this regard.

*	Best Practices and Case Studies

Even though the cyber security issue is quite a recent one, best practices have already been established throughout the entire industry that can be adapted for the health sector.

Backup files: If data is stolen, frequent backup-mechanics can help you to recover and evade possible ransom demands.

Secure authentication: Multifactor- or at least two-factor authentication techniques can secure valuable data from theft.

Firewall, antivirus and cyber hygiene: Keep your software safe, using frequent support programmes.

Education and awareness for employees: The unaware employee is still the biggest threat to cybersecurity.

Governance, plan establishment and regulations: Employ a dedicated cybersecurity department, regulate the cyber policies and create an incident response plan in case of a commenced attack.

*	**Risk Assessment & Checklist**

What does an employee need to be aware of? What is a possible threat and what is not? How to react, to make the problem not worse? Various checks should be done in frequent basis to ensure that your cybersecurity is up to date. Easy Checklists and evaluation techniques are a simple but important tool to keep the system going.

How to detect a possible attack: It is vital to detect an attack when you see one. Simple guidelines can help you to understand which gateways a hacker uses and where to look for indicators.

Software updates: To ensure maximum safety, it is vital that the software is kept up to date. This also includes passwords and frequent checks on the programs health.

General hardware protocols: How to handle valuable devices with care and to make sure that vital data cannot be stolen via external storage media like USB and hard drives.

*	**Smart Advice & Decision Support**

Cyberattacks have grown immensely in the health sector, therefore every advice and help that is available to this topic is needed.

Documenting and sharing among the health sector: A vital step to approach the issue would be to document every incident and to share it with the community. A cloud-based community could learn and work together on this issue and develop strategies.

Learning from other industries: Other segments, like the banking sector have far more experience when it comes to cybercrime and therefore made big advancements when it comes to protecting vital data of customers. Much of this knowledge may be partly adaptable for the health sector as well. Frequent cases, safety practices, and important tools could be listed online.

Interconnected help: Depending on institution, the needs or dimensions of cybersecurity may vary. Especially smaller companies lack the resources to successfully approach the issue but are still possible gateways for hackers to enter and spread through the entire system. A support platform that connects the different institutions could help to overcome those shortcomings.

*	**Technical Approaches & Solutions**

To approach cybersecurity in hospitals, the technical infrastructure is crucial. It is necessary to understand its components and how to use them for protection. Various programs are helpful to approach this topic:

Antivirus tools: Antivirus tools are mandatory for every system and should be updated frequently.

Screening tools, or network protocol analyser, intrusion prevention system: Specialised programs can help you to understand detailed information about what is happening on your network, and therefore detect possible irregularities and threats. If odd events like unauthorised logins, irregular processes or spontaneous shutdowns occur, your tools are the best way to stop an attack.

Hardware and updates: The best way to keep your system safe would be to buy the newest hardware with the best security protocols. Since this is not always possible, it is absolutely mandatory to update/change

your systems and passwords on a frequent basis. A system set on default (with the default password) is the easiest to enter.

Interconnectivity: With the wireless connectivity of (most) devices, every machine becomes a possible gate for a hacker, from which the entire system can be approached. Therefore, disconnecting the device, at least using some kind of encryption should be mandatory.

C CREATION OF TRAINING SCHEMES AND CURRICULA

On the grounds of the knowledge provided by the collected EU policies and directives, publications and tools, the review of the existing courses and the inputs of trainers and training seekers, the next type of action within the project will be the creation of training materials and creation of solid grounds for higher quality trainings that address the most burning needs of IT practitioners in charge of patient data in healthcare settings. Novel training schemes and curricula will be developed and put in practice within various series of training activities within the project. Minimum required standards for the delivery of courses to trainers (train the trainer courses) and to practitioners of different levels, required qualifications for trainers and tools for supporting trainers online will be developed within this major action of creation. The action is related to Objective 2 and Work package 3. The completion of this action is marked with Milestone M4 in the workplan.

D TRAINING ACTIVITIES

To exploit the developed training materials and have an impact on lowing the vulnerability of healthcare setting to fall victim of cyber-security attacks, the second stage of the project is dedicated to the delivery of a long list of trainings across various regions, targeting various audiences and delivered in various ways. The types of trainings provided by SecureHospitals.eu target trainers and practitioners, especially those at early career stage. The geographical representation of the consortium will ensure that the local training will be conducted in multiple countries. Some of the consortium partners have links and are able to deliver training also in neighbouring counties, which will increase the geographical area in which trainings take place to at least 1 countries.

The trainings planned to target stakeholders at the European level include the MOOC, the summer school and the webinars. Locally all partners will organise for additional trainings each, that will have the form of workshops. The following sections describe the methodology of each of the training activities planned within the project. A more detailed plan for the training delivery and targeted audiences will be developed within the project and include two iterations. The overall stakeholder engagement and training activities correspond to Objective 4 and Work Package 5. The completion of the MOOC, summer school as well as the webinars and local trainings constitute the major milestones of this action and are marked with M6, M7 and M8 in the workplan.

1 Massive Open Online Course

Massive open online courses (MOOCs) are an evolution of Open Educational Resources (OER) with the aim to make educational materials accessible to everyone. The number of participants attending one course is unlimited. As such they contribute to Goal 4 of the SDG to improve the provision of free education to men and women across the globe. Educational materials in MOOCs may include texts, infographics, publication links, video lectures, assessment methods in the form of quizzes but also in open questions and online collaborations spaces such as discussion boards where course participants can interact with each other and with the course facilitators. The existence of a collaborative environment, a course facilitator and open assessment differentiates among two types of MOOCS:

▪ Self-paced courses (asynchronous) are courses in which the material can be accessed anytime. The assessment method may be through multiple choice questions, drag and drop menus etc. and the certificate can be acquired at any time.

▪ Instructor-paced courses (synchronous) have a definite starting and ending date and are facilitated by an instructor who takes the audience through all lessons in a linear way. The assessment methods can be a combination of multiple choice questions and open parts (essays) which are evaluated by the instructor at the end of the term. All materials remain online accessible also after the end of the course, however receiving a certificate is no longer possible since the instructor cannot evaluate open assignments. The collaborative environment is also active only during the course duration. After the termination enrolled users can view all discussion boards but no longer contribute to the content.

According to the pedagogical model employed, MOOCs can also be divided into two further categories:

▪ cMOOCs: The "c" in this term refers to the connectivist pedagogy based on the practice of having open and collaborative materials that enable learners to shape the content by opening discussions and working on joint projects. The collaborative aspect means that such courses are not self-paced and have a start and end date. The four major sorts of activities that can have a benefit for learners are defined as: aggregating information (rather than predefining it), remixing, re-purposing, and feeding-forward (or making it relevant for future use). Connectivist MOOCs can better support collaborative dialogue and knowledge building.

▪ xMOOCs: or expert-led MOOCs follow the traditional pedagogy of having a fixed syllabus and materials predefined by an expert who is the course instructor. The interaction between the course participants is limited to technical questions and discussion forums for the participants to collaborate may not exist. Prpić at al. argue that xMOOCs are courses that employ elements of an MOOC but in effect are branded IT platforms that offer content distribution.

Both forms of MOOCs, but especially the cMOOCs represent a modern phenomenon of the early 2000s, with the OpenCourseWare (OCW) movement first started by the University of Tübingen. Though the MOOCs phenomenon started in the academic field many international organisations and initiatives are now embracing it on issues of global importance. One example of this is the SDG Academy which offers MOOCs revolving around the topics of SDGs. Many non-profit and for-profit consortia or universities, foundations or corporates have built extensive platforms offering MOOCs on a broad spectrum of fields. Besides the fact that they are free and open to everyone, some of the benefits of using MOOC include:

▪ **Diverse and adaptable**: The components used in the lectures can be reused and even reengineered to suit the individual needs of learning.

▪ **Alternative approaches**: New and different issues can be addressed in MOOCs as an alternative to mainstream topics. For example, NGOs can also teach about topics of global importance.

▪ **Better standards**: Many third world countries may not afford the necessary resources or the facilities to provide proper quality education. With MOOCs everyone can learn on a high level, regardless of income and infrastructure.

The SecureHospitals.eu MOOC will be developed as cMOOC involving a synchronous instructor-paced method allowing online collaboration, feedback from the participants and remixing and repurposing of the content.

2 Summer School

Summer schools offer extra-curricular training in a more relaxed atmosphere for transferring additional knowledge in a concentrated and focused manner.

The Gendemy.eu summer school will transfer existing knowledge about cybersecurity measures in healthcare settings. The curriculum of the summer school will comprise elements relevant for trainers as well as for IT practitioners in healthcare. Parts of the curriculum involve lectures on data protection and privacy regulations, and hands-on experiences in implementing cyber protection measures.

3 Webinars

Webinars stand for a combination of the terms “Web” and “Seminar”. In other words, they are traditional seminars broadcasted live on the web seeking to reach massive audiences. Webinars might mean that the seminar is held in front of a physical audience and also broadcasted online to a broader audience which can participate by typing questions online, or it can be held from a referent to a fully online audience thus creating the so-called **virtual classroom**. Contrary to Webinars are **Webcasts** which involve streaming the educational session online however without giving opportunity to the viewers to be engaged by asking questions or making suggestions that are integrated in the conversation. Technological tools enabling webinars are so-called **videoconferencing tools** such as AdobeConnect, Cisco Webex etc. Such tools allow the referent to share slides or the screen, stream a video stored in the computer or online (YouTube videos), talk to the audience and simultaneously type in a chat, conduct surveys and polls etc.

The SecureHospitals.eu seeks to boost training initiatives by creating participative settings that train stakeholders but at the same time set agendas and priorities for additional trainings. The SecureHospitals.eu webinars will thus be interactive and the produce rich results stemming from the questions and comments of the participants.

4	Workshops

Workshops are events of educational character involving a brief introduction to a special topic usually outside of the immediate area of expertise of the attendees, with the aim to trigger critical thinking, discussion and debate among them and reach a consensus about important decisions, conflictual matters or concepts. Moderated by consortium experts in each of the member-states, the workshops will seek to convey highly relevant knowledge to the participants and related needs, gaps and opportunities in cybersecurity and collect proposed measures. The topics of workshops will revolve around the different dimensions of cybersecurity and data protection in general and in healthcare settings in particular. The comprehensive trainings, paired with workshops offer the best option to overcome vulnerabilities in the system and to prepare your staff in every possible way. The workshops will focus on three levels:

Software and hardware: How to handle your devices the correct way, update the software or passwords, use encryption and prevent equipment from stealing.

Safe data sharing: Learn how to detect possible phishing mails, fake requests and important privacy measures.

Internal behaviour: How to prevent insider threats, cooperate with each other and report breaches. Also, what is not okay, when it comes to data handling.

In each of the sessions, participants will be asked to fill out questionnaires to evaluate the training and suggests ways of improvement. Evaluations and suggestions from the first training will help in enhancing the next sessions and making it fit more to the needs of the practitioners.

1.3.3 Links to other projects and activities

This section describes some projects that are linked to the SU-TDS-03-2018 project, however some of which are focusing on related topics such as Security in eHealth (KONFIDO), security and regulatory challenges in health data exchange (SHiELD), privacy-preserving analytics of Information in healthcare (SODA), Critical Infrastructure Protection (ECOSSIAN), linked data medical information space (Linked2Safety) and others. The linkages to these projects highlight that the SU-TDS-02-2018 consortium not only knows about engaging and involving stakeholders to achieve the projects ambitious goals, they also showcase potentials for synergies and knowledge exchange. The following table lists a selection of these projects:

Table 1: Related Research Projects

SHORT FACTS	PROJECT DESCRIPTION
KONFIDO **Call: H2020 DS-03-2016** Increasing digital security of health-related data on a systemic level **Duration:** Nov. 2016 – Oct. 2019 **Grant agreement no.:** 727528. **Funding:** 5 Mio.	**KONFIDO – Secure and Trusted Paradigm for Interoperable eHealth Services,** a Horizon 2020 project, aims to advance the state-of-the-art of eHealth technology with respect to four key dimensions of digital security: data preservation, data access and modification, data exchange and interoperability and compliance. The project is aiming 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 legal and ethical way, both at national and European levels. The approach will be implemented in a technological framework that relies on six technology pillars: 1) security extensions provided by main CPU vendors; 2) security solutions based on photonic technologies; 3) homomorphic encryption mechanisms; 4) customised STORK-compliant eID support; 5) customized extensions of selected SIEM solutions; and 6) disruptive logging and auditing mechanisms. The usability of the proposed solutions will be tested in a realistic setup, deployed on top of a federated cloud infrastructure, where data will be exchanged and services interoperate cross-border. Experimental evidence will be collected, proving that KONFIDO solutions provide effective protection even against attacks by privileged software (e.g. the Operating System or the Hypervisor) or privileged users (e.g. the System Administrator or the Cloud Provider). **MAIN OUTCOMES:** Legal & Policy Assessment and requirements, gap analysis, user requirements, validation & evaluation of pilots
 **Call: H2020 DS-03-2016** Increasing digital security of health-related data on a systemic level **Duration:** Jan. 2017 – Dec. 2019 **Grant agreement no.:** 727301. **Funding:** 4 Mio.	**SHiELD – European Security in Health Data Exchange** will unlock the value of health data to European citizens and businesses by overcoming security and regulatory challenges that today prevent this data being exchanged with those who need it. This will make it possible to provide better health care to mobile citizens across European borders and facilitate legitimate commercial uses of health data. SHiELD case studies will address cross border scenarios in which a citizen needs health care while in one Member State, and care givers need access to their health data from different Member States. SHiELD will also consider how commercial providers of lifestyle services or wearable sensors may be involved in such data exchanges. SHiELD will thereby also create opportunities for using health data to create such products and services addressing the common European market. The exchange of health data between systems is already possible, but it rarely happens. One reason is concerns about the potential security risks in the resulting end-to-end system, especially if it includes or is connected to insecure mobile devices. Another is the problem of ensuring compliance with regulations especially if the end-toend system spans multiple jurisdictions or involves different types of systems (e.g. for health care and lifestyle applications). Overcoming these barriers is the specific focus for SHiELD. **MAIN OUTCOMES:** Models and analysis tools for automated identification of end-to-end security risks in compliance issues and supporting privacy 'by design', open

	and extensible data exchange architecture, developed security mechanisms, faster and more cost-effective methods to verify and monitor compliance with regulations.
SODA Scalable Oblivious Data Analytics **Call: H2020 ICT-18-2016** Big data PPP: privacy-preserving big data technologies **Duration:** Jan. 2017 – Dec. 2019 **Grant agreement no.:** 731583. **Funding:** 3 Mio.	**SODA – Scalable Oblivious Data Analytics** will enable practical privacy-preserving analytics of Information from multiple data assets using multi-party computation (MPC) techniques. The project will embed this MPC techniques into a comprehensive privacy approach, demonstrated in a healthcare use case. The first objective of the project is to enable MPC for big data applications by scaling performance. The use-case driven approach will be combined with expertise from the domains of MPC and data analytics. The second objective is to combine these improvements with a multidisciplinary approach towards privacy. By enabling differential privacy in the MPC setting aggregated results will not leak individual personal data. Legal analysis performed in a feedback loop with technical development will ensure improved compliance with EU data privacy regulation. User studies performed in a feedback loop with our consent control component will make data subjects more confident to have their data processed with our techniques. The final objective is to validate our approach, by applying our results in a medical demonstrator originating from Philips practice and in a use case arising from the ICT-14.b data experimentation incubators. The techniques will be subjected to public hacking challenges. The technical innovations will be released as open-source improvements to the FRESCO MPC framework. **MAIN OUTCOMES:** State-of-the-Art analysis in secure multi-party computation (MPC), legal analysis of current privacy law in the EU, Practical privacy-preserving analytics on Big Data,
Ecossian **Call: FP7-SEC-2013-1** Pan European detection and management of incident attacks on critical infrastructures in sectors other than the ICT sector **Duration: Jun**. 2014 – May 2017 **Grant agreement no.:** 607577 **Funding:** 9,2 Mio.	**ECOSSIAN - European Control System Security Incident Analysis Network** is a project contributing to the European Programme for Critical Infrastructure Protection (EPCIP) by elaborating on a strategy and Action Plan, as well as by establishing worldwide initiatives on Cyber Security of Industrial Control Systems and Smart Grids followed by ENISA and Member States. The ECOSSIAN project's mission was to improve detection and management of highly sophisticated cyber security incidents and attacks against critical infrastructures (such as hospitals) by implementing a pan-European early warning and situational awareness framework with command and control facilities. A prototype system was developed, facilitating preventive functions like threat monitoring, early indicator and real threat detection, alerting, support of threat mitigation and disaster management. In the technical architecture with an operation centre and the interfaces to legacy systems (e.g., SCADA), advanced technologies were integrated, including fast data aggregation and fusion, visualization of the situation, planning and decision support, and flexible networks for information sharing and coordination support, and the connection of local operations centres.

	MAIN OUTCOMES: Implementation of a pan-European early warning and situational awareness framework with command and control facilities, Performance of a full-scale demonstration of the implemented ECOSSIAN framework and system
CANVAS **Call**: **DS-07-2015** Value sensitive technological innovation in Cybersecurity **Duration:** Sept. 2016 – Aug. 2019 **Grant agreement no.:** 700540 **Funding:** 1 Mio.	**CANVAS – Constructing an Alliance for Value-driven Cybersecurity** is set out to unify technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights. Within three years, CANVAS will bring together stakeholders from key areas of the European Digital Agenda – the health system, business / finance, and law enforcement / national security – for discussing challenges and solutions when aligning cybersecurity with ethics. **MAIN OUTCOMES:** Deliverables for each of the 3 target groups within the project – policy makers, industry experts/teachers, students in ICT or related fields. The outcomes contain case studies, reference curricula, a Massive Open Online Course (MOOOC) and more.
Linked2Safety **Call**: **FP7 ICT-2011.5.3** Patient Guidance Services (PGS), safety and healthcare record information reuse **Duration:** Oct. 2011 – Sept. 2014 **Grant agreement no.:** 288328 **Funding:** 3,1 Mio.	**Linked2Safety – A next generation, secure, linked data medical information space for semantically-interconnecting electronic health records and clinical trails systems advancing patients safety in clinical research** followed the vision to advance clinical practice as well as to accelerate medical research in order to improve the quality of healthcare, eventually benefitting public health and enhancing patient´s safety. The project provided pharmaceutical companies, healthcare professionals and patients with an innovative semantic interoperability framework, a sustainable business model, and a scalable technical infrastructure & platform for efficient, homogenized access to and effective, viable utilization of the increasing wealth of medical information contained the EHRs deployed and maintained at regional and/or national level across Europe. **MAIN OUTCOMES:** Developed user-friendly, sophisticated, collaborative decision-making environment
Hermeneut **Call**: DS-04-2016 – Economics of Cybersecurity **Duration:** May 2017 – April 2019 **Grant agreement no.:** 740322 **Funding:** 0,3 Mio	**HERMENEUT – enterprises intangible risks management via economic models based on simulation of modern cyber-attacks** has a strong focus on the human factor of IT security and risk management, specifically looking at psychological, behavioural, societal, organisational and economic aspects in the identification of cyber-risks. The project assesses vulnerabilities of organisations and corresponding tangible and intangible assets at risk, taking into account the business plans of the attacker, the commoditisation levels or the target organisations, exposure of the target and including human factors as well as estimating the likelihood that potential cyber-attack exploits identified vulnerabilities. **MAIN OUTCOMES:** Methodology and advanced macro- and micro-economic models.

1.3.4 Further aspects and considerations

Gender Analysis: Taking into account the differential needs and responsibilities between man and women regarding work opportunities in general and especially the low gender quota in technical fields and especially in cybersecurity, the SecureHospitals.eu project incorporates a strict gender perspective that is in line with the Treaty of the European Union which seeks to eliminate gender inequality and promote equal opportunities for man and women. The coordinator and all partners engaged in this proposal are fully committed to the philosophy and implementation of gender equality within the consortium in order to be able to promote and train for its uptake to external stakeholders.

In accordance with Articles 2 and 3 of the Treaty of Amsterdam (1997) and other EU policy directives (COM (96) 67 final) and reports (EUR 2002/2), establishing equality between men and women as a specific task of the Community, the project management is committed to incorporating the principles of gender main-streaming throughout the various elements of the entire project, ensuring equal consideration to the different life patterns, needs and interests of male and female participants. Extrapolating from these findings, it will be important to incorporate into the SecureHospitals.eu project and its actual execution a gender perspective that is sensitive to the following aspects:

- Take into account the differential needs and responsibilities between men and women regarding differential patterns of work; differential patterns of time used between paid work and responsibilities for woman and man in general.
- Track and take into account unpaid and invisible work often carried out by women. The classic type of work of course refers to reproductive work carried out by women at home. For SecureHospitals.eu, it will be important to emphasize and explicitly acknowledge the gender gap in terms of unpaid activities.

The coordinator will constantly monitor the representation of women and men within the project team. Since the share of women in technical careers overall remains below that of men, we will review our own policies and practices with regard to the career progression of young women within the project team during the course of the second project team meeting. We will support consortium members with caring responsibilities for children or others by organising meetings and conferences at family-friendly hours, and by facilitating family-friendly working arrangements within each institution involved in the project. In addition, the project will strive to incorporate a gender lens in its methodology, considering how group membership and operational procedures may limit women's participation. We will apply Time Use Analysis where appropriate in order to detect the differential necessities and effects of the SecureHospitals.eu project apply to women and men.

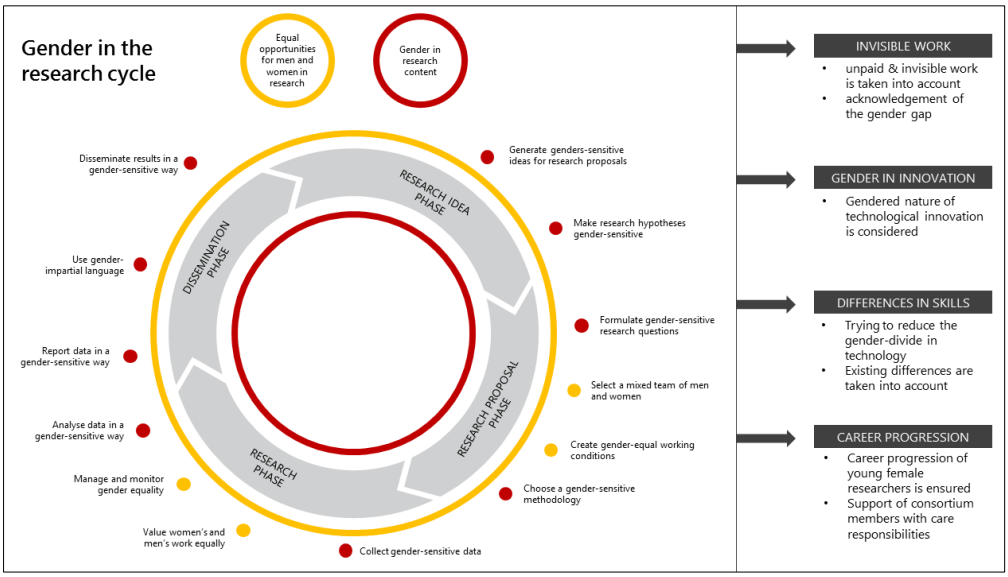


Figure 6: Gender analysis in the SecureHospitals.eu project

2. IMPACTS

2.1 Expected impacts

The SecureHospitals.eu project responds to the call SU-TDS-03-2018 which foresees awareness raising activities and the development of training schemes on cybersecurity in hospitals. The objectives and the types of actions planned in the project will provide results that meet the impacts listed in the call text and seek to go beyond them. The main impacts, the project will in overall healthcare ecosystem are grouped in the following categories:

I1	**IMPACTS on less human errors causing cybersecurity threats**

The project will collect more than 200 sources in the open online information hub. Awareness raising activities engaging the partners on the open information hub and increasing the outreach of the knowledge sources will have an impact on the abilities of the IT staff and additional employees in hospitals. In addition, the developed training materials and wide range of trainings will have increase the abilities and qualifications of the staff involved in data protection and cybersecurity in hospitals. Apart from the staff trained within the project, the open information hub will provide tools and guidelines for setting up efficient trainings in all hospitals and healthcare centres across Europe. This will have multiplier effects in the whole continent, thus increasing awareness and abilities of staff. Higher qualified staff with regards to cyberthreat and data protection can ensure that less human errors happen in the daily operations of the IT and IT-related staff that can breaches of data security and the landing of data in the dark web.

I2	**IMPACTS on less risk of data privacy breaches**

The training materials produced by the project on the basis of co-creation activities, joining together IT experts on cyber security, researchers and hospital staff that deal with such operations daily, will create solid strategies for minimising risks in breaches of data privacy. Besides the creation of strategies for risk assessment, mitigation and implementation of preparedness mechanisms, the trainings organised by the consortium will ensure that participants from at least 100 hospitals take up and implement the risk assessment and minimisation strategies. Multiplication effects caused by the rest of the communication and awareness raising activities will increase the uptake of strategies in most of the ecosystem in Europe.

I3	**IMPACT on reducing cybersecurity vulnerability of Health and Care services, data and infrastructures**

Well trained staff that is less prone to causing errors resulting in data security breaches and solid strategies for the implementation of risk assessment, risk minimisation, preparedness and the measures for rapid response against cyber attacks means less vulnerable healthcare centres. The decreased vulnerability will be measurable in all aspects covered by the trainings: bot services and data infrastructure.

I4	**IMPACT on increasing patient trust and safety**

The uptake and proper implementation of the strategies and the knowledge conveyed by the project will decrease the frequency of casualties in cyber-attacks in hospitals and healthcare centres. As a consequence, patients will have more trust in providing their data to health care settings. Increased patient trust will make those hospitals implementing the strategies more successful and competitive in the system.

2.2 Measures to maximise impact

2.2.1 Dissemination and Exploitation of Results

The project seeks to establish a two-way communication, to not only spread the word, but also receive feedback and interact with related activities. As a coordination and support action seeking to raise awareness on cybersecurity in healthcare and create an online community, achieving high visibility all over Europe is an immediate precondition for SecureHospitals.eu to fulfil its set objectives. As such, the consortium proposes an initial approach that will leverage activities and efforts from all work packages to maximise participant engagement and project results dissemination. The dissemination activities will take into account the heterogeneity of other security practitioners and the cross-sectorial interests of other stakeholders. Through the work that will be carried out during the project, we aspire to establish an impactful dissemination of SecureHospitals.eu results, allowing for its sustainability beyond the end of the project. As such, the consortium proposes an initial approach that will leverage activities and efforts from all work packages to maximise participant engagement and project results dissemination. The dissemination strategy will focus on the promotion of project results in order to **attract** the target audience, **raise their awareness** and **engage** them in the project activities. The aim of the **exploitation** will be to **ensure the optimal use** of SecureHospitals.eu results after the project's completion, and therefore speed up the potential of their **uptake in the entire cybersecurity community.**
To ensure that dissemination and exploitation of the project results align throughout the lifecycle of the project, activities will be divided into three overarching strategic areas, which, as outlined below, are designed to accord with more detailed phased-activity for both dissemination and exploitation respectively:

STRATEGIC FOCUS I: Planning and Preparation (Dissemination & Exploitation)

Researching, identifying & reviewing current status and opportunities to promote SecureHospitals.eu results and achieve & sustain practitioner usage of the project's knowledge and activities.

Analysing target audiences and their needs in order to better understand the impact of user-centric integration and decision support services, raise targeted awareness about SecureHospitals.eu benefits and support the potential for its wider sustainability.

STRATEGIC FOCUS II: Branding & Communication (Dissemination)

Systematic use of a variety of dissemination activities to 1) create an overarching 'brand' for SecureHospitals.eu and 2) reach and involve target audience groups, primarily trainers and researchers at their early career stages in order to motivate them to use SecureHospitals.eu tools and participate in its activities.

Use of social media to establish on-going communication with practitioners in order to extend the network, acquire feedback on the coordination and standardisation mechanisms and raise awareness on the common understandings generated by the project.

STRATEGIC FOCUS III: Product Refinement & Roll Out (Exploitation)

Integrating knowledge from relevant initiatives (including SecureHospitals.eu's own communication activities) and projects and establishing collaboration and synergies that can contribute to the improvement of SecureHospitals.eu features, add new services/features and develop new business cases of exploitation.

The exploitation strategy and planning will provide sustainable usage of the Gendemy.eu web platform and its community of practice in order to maximise the project impacts beyond the project duration.

2.2.2 Dissemination and Exploitation Strategy

The major focus of the SecureHospitals.eu dissemination plan is on ensuring that the project trainings, training materials and the web platform are widely disseminated to the appropriate target communities,

at appropriate timing, via appropriate methods, and that those who can contribute to development, evaluation, uptake and exploitation of the SecureHospitals.eu outcomes can be identified and encouraged to participate.

D1	**Connecting with the full potential range of trainers and researchers across Europe**

REACHING ALL PRACTITIONERS: The primary objective of the dissemination activities is the timely provision of appropriate and reliable information to all gender equality trainers and researchers across Europe as well as all additional stakeholders included in the SecureHospitals.eu scope and expected results. The consortium wants to ensure that its targeted audience is properly aware of the project motivation, methodology, the expected impacts and benefits. As a result, it is critical to utilise tailored dissemination strategies that specifically target all potential interest groups including all hospital and and healthcare centres, training providers, individual trainers, legal and cyber experts etc. SecureHospitals.eu will have an extensive reach across the whole research community in Europe to accelerate knowledge transfer, foster open dialogues, convey guiding material for the uptake of knowledge on gender equality, develop new materials and guiding materials for new course curricula tailored to the needs of various practitioners.

As another key objective of the project is the creation of an online community of practice, most of the dissemination resources and activities will also be specifically targeted to trainers across Europe. Tailored dissemination activities should establish contacts to the trainer community and the present them the benefits of utilising the SecureHospitals.eu tools (Trainer Profiles and engagement in the Community of Practice).

DYNAMICALLY EVOLVING STRATEGY: Another aspect of the SecureHospitals.eu dissemination objectives is to reach out to different fields, the circle of stakeholders needed to be approached by the project during the whole duration, will continuously expand. Hence, the mechanisms for approaching the new circles of stakeholders will also be continuously updated and tailored to the specific target groups. These continuously updated communication mechanisms will allow for effective dissemination growth and maximum awareness formation based upon the feedback obtained. The SecureHospitals.eu project has protocols in place to continuously identify additional stakeholders, especially during the early phase of the project. In addition, the partners of SecureHospitals.eu are very well connected and will leverage these connections to kick start the communities for the proposed activities.

D2	**Achieving maximum impacts of SecureHospitals.eu through effective information aggregation and dissemination materials**

The SecureHospitals.eu project as a dedicated coordination and support action has selected work packages that are focused on aggregating information, engaging stakeholders and delivering knowledge to the target groups. This process must be conducted in a timely and efficient manner to achieve maximum impact. To optimize the delivery of the anticipated data and material, the consortium will have categorized the dissemination into three stages as outlined below.

STAGE 1 | DISSEMINATION FOR AWARENESS: The general objective at this early stage of the project is to raise awareness on the risks of cyber-attacks in healthcare and the need to provide effective and high-standard training to IT staff. Practitioners will become aware of the SecureHospitals.eu project, its motivation and guiding material. The strong use of infographics and intuitive visualisations will help raise and promote overall awareness of the SecureHospitals.eu project. This initial awareness raising efforts will lay the ground work for the long-term engagement of relevant interest groups in the SecureHospitals.eu project and simultaneously ensure the success of the projects dissemination strategy.

STAGE 2 l DISSEMINATION FOR ACTION: During the second stage of dissemination, the focus shifts to delivering materials that stimulate practitioners to mobilise and take action. The types of action put forward by the project include the formation of an online community of practice for knowledge exchange on cyber risks, the engagement of a wide circles of trainers and early career-stage researcher in the SecureHospitals.eu trainings and their feedback on the creation of materials and general reflection on the project results.

The dissemination for action phase will include the creation and the promotion of video materials and infographics for the promotion of the attendance in the SecureHospitals.eu MOOC, summer school and additional trainings. Furthermore, the projects main product and dissemination channel, the web based SecureHospitals.eu online information hub will serve as a space for engaging trainers of the network to exchange practices and know-how through the community of practice and also through uploading training materials and advertising courses.

STAGE 3 l DISSEMINATION FOR RESULTS: The final stage of the SecureHospitals.eu project is dedicated to communicating the results and accomplishments and reflecting on their impact in the overall trainer and research and innovation community. The planned outcomes of the project will be disseminated not only to the network of trainers and sub-networks of practitioners, but also to a wider research and innovation community and related stakeholders.

D3	**Promoting SecureHospitals.eu through multiple dissemination channels**

According to Article 38 of the H2020 Annotated Model Grant Agreement, the SecureHospitals.eu project will exploit several channels to optimise the impactful external communication with a broad audience. The most important media channels and considerations included in the SecureHospitals.eu strategy are described in the following paragraphs.

PROJECT IDENTITY: The SecureHospitals.eu project wants to aggregate, harmonize and curate data from various providers into interlinked information repositories and provide improved, concise and coherent information that can be turned to training material for trainers and practitioners. In order to maximise the impact of the objectives it is vital to address the audience as one project and ensure the immediate recognition of disseminated materials. Together with all partners, associated partners and third parties involved, the SecureHospitals.eu project will therefore build a strong project identity. The following design and communication elements will be used to strengthen the project uniformity and identity and to deliver clear messages to our audience: SecureHospitals.eu naming, SecureHospitals.eu logo, SecureHospitals.eu presentations template, SecureHospitals.eu templates for reports and letters, SecureHospitals.eu project factsheet, SecureHospitals.eu project posters etc.

SOCIAL MEDIA: SecureHospitals.eu will have a strong social media presence and actively engage in social networking. Social Media Networks will be used to disseminate current information about the project scope, open feedback channels and establish two-way dialogues with the wider public. The various benefits of social networking on well-established social media channels like Twitter, Facebook, YouTube, Flickr, LinkedIn will be utilised to further enhance the scope and outreach of the project and specifically target and connect end-user audiences like security projects consortia, other security practitioners, industry stakeholders, researchers, policy makers, and governments.

TRADITIONAL MASS MEDIA: To address the wide audience and ensure that the project results will be taken up and embedded in the general community also the public media like newspapers, television, radio and popular science magazines will be used. These sources will be chosen based on findings during the project that point out which media optimally reaches the relevant target groups.

2.2.3 Data and Knowledge Strategy

Data Management: According to the Open Access requirements for Horizon 2020 projects, results produced will be granted open access principally using the free online access green model. In the remaining cases, the gold model will be used (considering the policies of partner think-tanks). The reason for this choice is related to the free nature and the online availability of data used for all activities. The SecureHospitals.eu project: a) is built on previous research results (improved quality of results); b) fosters collaboration and avoids duplication of effort (greater efficiency); c) involves all types of end-users of research results (improved transparency of the scientific process).

Protection of pre-existing know-how and project results: Prior to the formal project start the parties will sign a non-disclosure agreement in order to protect the intellectual property. Each consortium member has the right to exclude specific pre-existing know-how (background) from the other members' access, as far as the restrictions are announced before the signature of the funding contract or before the joining of a new party. The procedure to handle these cases will be settled in the consortium agreement. While the consortium members share software and knowledge ownership, parties in case of leaving the consortium previously to the formal project end are expected to transfer knowledge gathered and software components produced during project execution to the project coordinator immediately.

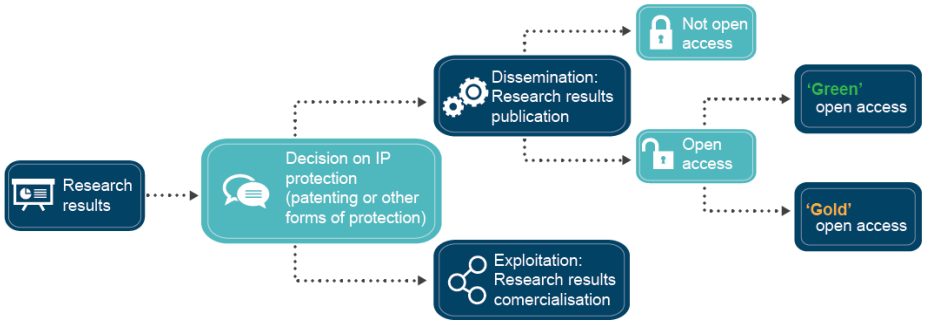


Figure 7: Flowchart of the knowledge management strategy

Ownership*:* Collected data within the project from systematic literature reviews and requirements and usability studies will be provided to all consortium members. Detailed commercialization/sales rights as well as software ownership will be defined in the consortium agreement. However, the other project participants have to be informed in advance about any publication plans. Each participant shall ensure that the foreground is disseminated to the other participants and to the coordinator. The dissemination of the foreground between the different work packages will be done during the consortium meetings, workshops or during regular conferences.

Access rights to and exploitation of pre-existing know-how and project results*:* Access rights needed for the project execution according to the agreed work plan are granted on a non-exclusive basis, expressly exclude any rights to sub-license and shall be made free of any transfer costs. The procedure will be defined in the consortium agreement. Besides these general regulations a detailed consortium agreement will be established (based on the DESCA 2020 model) and signed before the beginning of the project to guarantee that all project members are aware of their rights and responsibilities.

Intellectual Property strategy: The consortium partners will sign a consortium agreement before the beginning of the project in order to protect the intellectual property of SecureHospitals.eu. The consortium agreement will answer questions of ownership, the protection of pre-existing knowledge and project results, access rights and exploitation of pre-existing know-how and project results with regards to technical outcomes and licenses as well as social-scientific research results. Concerning IPR management, the consortium aspires to an agreement from which all consortium partners can benefit regarding their portfolio and expertise.

SEARCH ENGINE OPTIMISATION: The visibility of SecureHospitals.eu open information hub will be optimized via effective Search Engine Optimization (SEO) to both increase the web-portals relevance to specific keywords and to remove barriers to the indexing activities of search engines. As an effective

knowledge awareness strategy, SEO considers how search engines work, what people search for, the actual search terms or keywords typed into search engines and which search engines are preferred by their targeted audience. In general, via SEO the Gendemy.eu will appear more frequently in the search results list, and more visitors it will receive from the search engine's users. SEO may also target different kinds of search, including image search, local search, video search, news search and theme-specific vertical search engines.

2.2.4 Communication activities

SecureHospitals.eu will use a multi-level approach including tailor-made dissemination tools and activities depending on the respective target audiences and their needs. The project has identified target groups on three different levels: European level, national level and project level. For all these three levels, a full set of traditional dissemination tools accompanied by innovative dissemination activities will be carried out. The following tables describe some of the communication means to be used for addressing the various stakeholders and the key performance indicators of the overall engagement and dissemination activities.

Table 2: Means of Communication

LEVEL	MEANS OF COMMUNICATION
International & European	• Folders, flyers, press releases • Articles in scientific journals and other specific publications • Academic and non-academic conferences and meetings • Videoscribe/thunderclap, Slideshare • Social Media (FB, Twitter, Linkedin, Youtube) • Project Website and Platform
National	• Personal contacts and email marketing • Folders and Flyers • Talks at academic and non-academic conferences, meetings and events • Dedicated press conferences and public presentations • Project website and platform • Press releases, Articles, Radio Interviews
Project	• Email list and conference calls • Collaborative online space and forum • Workshops and meetings • Project coordination manuals • Cooperation agreement

Table 3: Key Performance Indicators

PERFORMANCE INDICATOR	SUCCESS MEASURES	TARGET
Knowledge Mapping	Number of mapped projects	>150
	Number of collected stakeholders and related experts	>300
	Collaborations with existing European and International initiatives	>50
Training and Collaboration	Number of sources in the online knowledge library	>100
	Number of training courses listed in the online training directory	>100
	Yearly visits on the Gendemy.eu platform and all SecureHospitals.eu web instances in the last project year	>50,000
	Minimum number of trainers registered with profiles and joining the 'Community of Practice'	>100
	Number of the participants in SecureHospitals.eu MOOC	>200
	Number of participants in the SecureHospitals.eu summer school	>25
	Minimum number of overall local trainings	> 10
	Minimum number of participants in one training	>10
Additional Dissemination	Mentions and presence in external media during the project timeline	>20
	Subscribers to the SecureHospitals.eu Newsletter	>200
	Followers on Twitter at the end of the project	>500

Table 4: Key Performance Indicators

CONFERENCE OR EVENT NAME	TENTATIVE LOCATION	DATE
Global Cyber Security in Healthcare & Pharma Summit	UK, Heathrow	2019 2020
IT-Sicherheit im Gesundheitswesen	Germany, Leipzig	June, 2019 2020 & 2021
Big Data in Healthcare Conference	UK, London	2019 2020
EAHM Congress	Portugal, Cascais	September, 2019 September, 2020
conhIT – Connecting Healthcare IT	Germany, Berlin	April, 2019 April, 2020
European Hospital Conference	France, UK, or Germany	Q1 2019 Q1 2020
UK e-Health Week	UK, London	May, 2019 May, 2020
HIMSS Europe	Spain, Barcelona	May, 2019 May, 2020
Swiss eHealth Summit	Switzerland, Berne	11 - 12 September 2018
Digital Healthcare Show	UK, London	June, 2019

3. IMPLEMENTATION

3.1 Work plan, Work packages, Deliverables and Milestones

To reach all described aims and objectives of the SecureHospitals.eu project, with a total duration of 26 months, an integrated project plan and overall work plan strategy consisting of structured work packages and strategic positioned milestones will be applied as described below and in the next section.

As the project is designed as a coordination and support action, it has been divided into 6 different work packages. The analysis part will provide the timely conception to take place followed by technical research and development activities. The sublevels of each WP are linked to one or more deliverables. It is this substructure that facilitates the calculation of the person months needed to complete the WP as a whole. This emphasizes the importance of flexible partners that have competencies in several areas. A flexible consortium can react better to problems arising from the interconnection of WPs and can, in the worst-case scenario of a partner leaving, redistribute their work tasks among the other partners.

The work plan strategy is a structured programme defining how the project objectives and aims will be fulfilled. The objectives described in section 1.1 represent the theoretical groundwork from which the 6 work packages (WP) have been articulated. The work plan will follow a model which ensures that the output of the earlier work packages is taken up by the following ones and also allowing on-going iterations. The WPs structure the diverse tasks and group them under certain main topics as for example manage (WP1), involve (WP2) or aggregate (WP3). Each WP is designed to treat an important aspect of the project and has a lead partner that has the best set of skills for the overview of the WP.

Table 5: Work package leaders and total person months estimated

NO.	WORK PACKAGE TITLE	LEAD NO.	LEAD NAME	PERSON MONTHS	START MONTH	END MONTH
WP1	**MANAGE:** PROJECT MANAGEMENT AND COORDINATION	**1**	**INSP**	14,5	1	26
WP2	**INVOLVE**: HOSPITALS AND PRACTITIONERS VIA AN ONLINE AWARENESS AND INFORMATION HUB	**5**	**COOSS**	18	1	10
WP3	**AGGREGATE:** EXISTING KNOWLEDGE AND APPROACHES ON CYBERSECURITY IN HOSPITALS	**2**	**EUR**	19,5	1	9
WP4	**CREATE:** STRUCTURED TRAINING SCHEMES AND CURRICULA FOR HOSPITAL STAFF & TRAINERS	**4**	**FPHAG**	16	2	13
WP5	**BOOST:** TRAINING INITIATIVES IN HOSPITALS AND INTEGRATION OF PROVIDERS AND COURSES	**7**	**JOIN**	21	1	23
WP6	**COMMUNICATE**: AWARNESS RAISING ON PROJECT ACTIVITIES AND PROMOTION OF THE HUB	**8**	**EDE**	17	1	26
	Total PM	**106**				

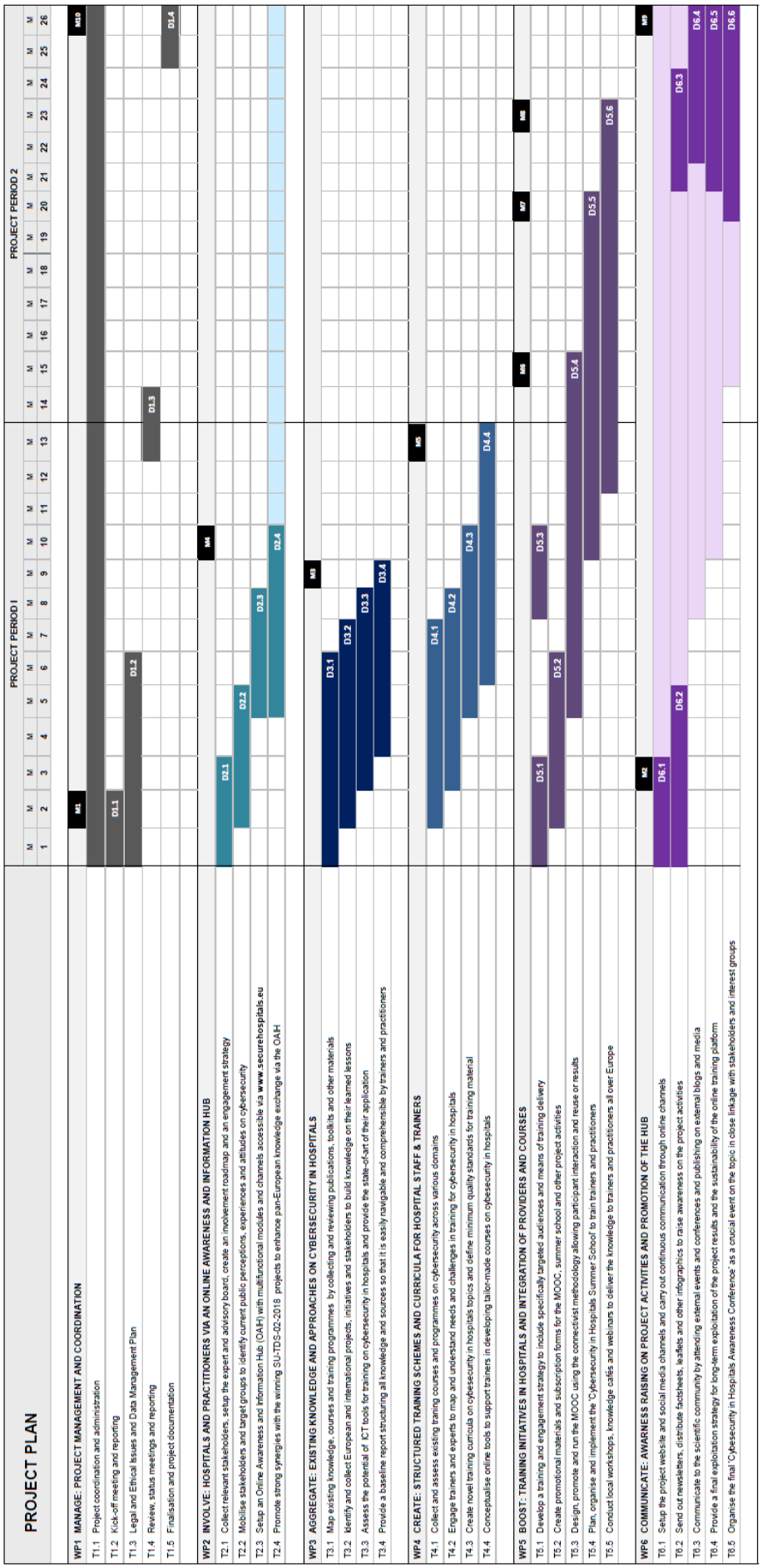


Figure 8: SecureHospitals.eu work plan

WP1 MANAGE: PROJECT MANAGEMENT AND COORDINATION (Start Month 1)								
Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	11	0,5	0,5	0,5	0,5	0,5	0,5	0,5

OBJECTIVES

The main objective of this WP is the **coordination of the project and reporting** during the project. The scientific work will be assisted and monitored while the administrative tasks will be performed in order to pursue an effective and most productive project performance. A **kick off meeting** will be organised at the beginning of the project in Vienna, Austria. This meeting will allow to put the project on the right track and to assure that all partners share the same idea of the tasks assigned to them. It will provide the basis for ensuring dialogue, communication and exchange within the consortium. There will be a summarised overview of the meeting for interested external experts/other third parties provided by the coordinator. Also, an overview of the work progress and the next steps will partly be put on the project website to serve the consortium partners, the EU and the wider public. More detailed technical and management information will be delivered in the form of reports to the EU, including final project documentation and publication at the end of the project.

Work package 1 will ensure that the skills, capacities and efforts of all involved partners are fully integrated and all put to the benefit of the project. Therefore, a specific task in this first WP will be to oversee and assist the advancement and ongoing improvement of the project. The final main characteristic of the first WP will be the monitoring of the achievements in the other work packages, whereby the first work package will oversee the in-time and regular achievement of deliverables and milestones, foreseen in each of the WPs throughout the entire project. The monitoring of these achievements will require an ongoing and consequent focus on results, targets and the agreed upon plans. WP1 will oversee achievement of deliverables and milestones, foreseen in each of the WPs, in a timely manner and on a regular basis. Accomplishments in this WP are marked by **M1** and **M10**.

DESCRIPTION OF WORK

T1.1 Project coordination and administration (Lead: INSP)

This task is designed to supervise the objectives of the work packages, which can be seen as the general project coordination and administrative management. As such, this task includes effective communicative exchange among the consortium, assisting and monitoring the scientific work, overseeing the whole project, collecting and delivering reports on time. It will function as a red line throughout the whole project in order to keep focussed and to act as effective and efficient as possible. This task will be managed by the coordinator INSP and an intense cooperation between the consortium partners is established.

T1.2 Kick-off meeting and reporting (Lead: INSP, Participants: ALL)

The WP1 leader is responsible for organising a kick-off meeting and for reporting on this meeting at the beginning of the project. The kick-off meeting shall establish initial information exchange and task delegation among the consortium, which is the basis for successful collaboration and project outcomes. An important part of this kick-off meeting is to meet each other in person, which also contributes to a better understanding and a feeling of trust within the consortium from one partner to another.

T1.3 Legal and Ethical Issues and Data Management Plan (Lead: TLX, Participants: ALL)

In order to ensure the alignment of the project with the legal requirement and the ethical standards in research and development – especially with regard to the development of the MOOC, a legal and ethical issues report will be produced during the first half year. Such report will particularly focus on the privacy and security aspects in relation to the project data. Furthermore, a data management plan will be developed, which will provide information on which data that will be made openly accessible, their interoperability and re-usability. It will also highlight the costs of the data storage as well as security, legal and ethical issues related to it.

T1.4 Review, status meetings and reporting (Lead: INSP, Participants: ALL)

The project will include project status meetings in different partner countries and a mid-term status report. In these meetings progress will be discussed and feedback or updates can be given so that the work is constantly improved for ensuring the success of the SecureHospitals.eu project.

T1.5 Finalisation and project documentation (Lead: INSP)

The last task within WP1 will be the completion of the final project documentation, which will summarise the methodology, achievements and lessons learned from all WPs in the SecureHospitals.eu project. The documentation plays an important role to determine the lessons learned for the partners and for the next projects they might be involved in. It can serve as a basis for follow up research projects.

DELIVERABLES

D1.1 Kick-off meeting report (project month 2)

A kick-off meeting report will be provided within the first two months of the project. This will contain the meeting agenda, participant list and all relevant information on important consortium decisions. The report will contribute to a good shared understanding so the consortium can start with level playing field in order to pursue effective communication.

D1.2 Data management plan (project month 6)

This report will deliver the data management issues, which are relevant for the SecureHospitals.eu project and will additionally, ensure continuous monitoring. The data management plan will be updated throughout the project.

D1.3 Status report and financial overview (project month 14)

After the first a status report will be delivered, which will not only showcase all project accomplishments, but also identify all obstacles up to this date. According to the project plan these reports will contain primarily information on the research and development progress as well as societal impacts. Within this summary report special attention will be given also to the reflection on the communication within the consortium.

D1.4 Final project documentation (project month 26)

The final project documentation will describe how objectives were achieved, which challenges complicated the project process and which further perspectives arise from the final project state.

WP2 INVOLVE: HOSPITALS AND PRACTITIONERS VIA AN ONLINE AWARENESS AND INFORMATION HUB (Start Month 1)								
Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	5	2	1	2	4	1	1	2

OBJECTIVES

The objective of this WP is to initiate a strong involvement and integration of key stakeholders throughout the duration of the SecureHospitals.eu project.

The WP will identify the main stakeholders in cybersecurity in hospitals (researchers, cybersecurity experts, hospital managers, developers, etc.) and will organise different activities for outreach and engagement. The emphasis will be on bringing together research experts, content providers, technology infrastructure specialists, legal experts, practitioner groups from various sectors of cybersecurity within Europe.

The focal point of this WP will be to launch the **Online Awareness and Information Hub – OAIH** as the hub will greatly support the consortium in raising awareness and promoting the results of all projects related to cybersecurity in hospitals.

All its outputs will directly feed in the following work packages 3, 4 and 5. Achievement in this work package are oriented towards the achievement of the Objective 1: "**RAISE** awareness among decision makers and ICT practitioners in hospitals and care centres across Europe on the importance cybersecurity and continuous training of all affected staff."

Its achievement is marked with milestone **M4** in the project workplan.

DESCRIPTION OF WORK

T2.1 Collect relevant stakeholders, setup the expert and advisory board, create an involvement roadmap and an engagement (Lead: COOSS, Participants: INSP, EUR, TLX, FPHAG, SAM, JOIN, EDE)

This task will serve to identify and categorise groups of actors and stakeholders involved in the European cybersecurity in hospitals landscape. Once stakeholders have been identified and categorised, a roadmap for the mobilisation of stakeholders will be drawn up outlining potential areas of engagement and strategies for cross-stakeholder fertilisation. The stakeholder engagement strategy will inform the design and evaluation of the Online Awareness and Information Hub - OAIH.

T2.2 Mobilise stakeholders and target groups to identify current public perceptions, experiences and attitudes on cybersecurity (Lead: EDE, Participants: COOSS, JOIN, SAM FPHAG)

Within this task the consortium with cast a wide net in the form of public consultations in order to obtain first hand information on the current status and attitudes on cybersecurity in hospital and care centers. This task represents the building blocks for the next steps in providing lessons learned (WP3), surveys related to training curricula (WP4) and organisation of local workshops, knowledge cafés and webinars to deliver the knowledge to trainers and practitioners all over Europe (WP5).

T2.3 Setup an Online Awareness and Information Hub (OAIH) with multifunctional modules and channels accessible via www.securehospitals.eu (Lead: INSP)

Based on the initial feedback INSP will launch the OAIH in order to provide a meaningful collaboration and discussion space on the topic of cybersecurity in hospitals. The modules will be designed and adapted within the project lifetime in order to ensure the perfect spot for constructive discussions and training delivery.

T2.4 Promote strong synergies with the winning SU-TDS-02-2018 projects to enhance pan-European knowledge exchange via the OAIH (Lead: INSP, Participants: COOS, EDE, EUR)

This task is critical to the success of the project and it focuses on establishing strong communication and knowledge transfer links between the SecureHospitals.eu, and the winning SU-TDS-02-2018 projects. The assessments and analysis of cybersecurity in hospitals will be shared with the other consortiums to make sure that such issues are considered while developing assessment toolkits to protect privacy/data/infrastructures. Two iterative time periods of round table discussions (both via on-line and in-person modes) will foster an insightful knowledge exchange between the teams. Opportunities for joint workshops and events will also be explored and rendering the OAIH as the main point of exchange.

DELIVERABLES

D2.1 Stakeholder involvement roadmap and engagement strategy (project month 6)

The deliverable holds structured information on all identified key stakeholders, networks, initiatives and other end-users of relevance across Europe along with an engagement strategy.

D2.2 Current perceptions and trends on cybersecurity in hospitals (project month 7)

The results of the public consultations of stakeholders will be summarised in this deliverable.

D2.3 Online Awareness and Information Hub www.securehospitals.eu (project month 8)

The OAIH is launched and promoted within the consortium network and relevant stakeholders.

D2.4 Relevant cybersecurity projects list and liaisons overview (project month 9)

This deliverable will provide an extensive overview of all relevant past and present actions related to cybersecurity in hospitals, while remaining subject to consequent updates if need it.

WP3 AGGREGATE: EXISTING KNOWLEDGE AND APPROACHES ON CYBERSECURITY IN HOSPITALS (Start Month 1)

Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	4	5	1		1	1,5	3	1

OBJECTIVES

The objective of this work package is to map all the knowledge and activities on cybersecurity in hospitals in Europe. One of the primary foci of observation will be the knowledge produced by EU projects and initiatives and mainly the knowledge, activities and tools developed so far. Mapping the most relevant and recent knowledge sources on cybersecurity in hospitals serves as the basis for the creation of high quality training materials and training activities. The libraries that will be developed in this work package will be fed directly into the online hub, in a categorised an easily navigable manner so that trainers and practitioners can easily find sources for developing new training curricula. Another focus of this work package will be the observation of the implementation of ICT tools on training for cybersecurity in hospitals in Europe and internationally.

All its outputs will directly feed in the following work packages 4 and 5. Achievement in this work package are oriented towards the achievement of the Objective 2: "**AGGREGATE** all existing knowledge on cybersecurity in hospitals filtering the most relevant for the development of high quality trainings supported by innovative e-approaches."

It achievement is marked with milestone **M3** in the project workplan.

DESCRIPTION OF WORK

T3.1 Map existing knowledge by collecting and reviewing publications, toolkits and other materials (Lead: FPHAG, Participants: INSP, EUR, FPHAG, COSS, SAM, JOIN, EDE)

This task will start by an extensive collection of knowledge sources, reviewing and mapping them in order to make sure the whole ecosystem has been observed in detail and important knowledge does not miss out. The aim of the task is not only to map the knowledge for internal use in the creation of training materials in the following work packages, but also to create a library of mapped sources that can be integrate on the online hub and support network trainers to create new training materials.

T3.2 Identify and collect European and international projects, initiatives and stakeholders to build knowledge on their learned lessons (Lead: JOIN, Participants: INSP, COOS, EDE, EUR)

This work package will collect existing European projects and other initiatives funded by the EU but also other major institutions and. Once a list of the most relevant projects and initiatives has been created, the aim will be to observe their experiences and build on their lessons learned. This will enable the SecureHospitals.eu project to exchange information with other actors and build synergies with their work. A list and description of relevant projects and initiatives related to training for the uptake of cybersecurity in hospitals considerations also be integrated in the online hub to increase the outreach of their outputs in the trainer community.

T3.3 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)

Training on cybersecurity in hospitals is one of the areas that suffers from the lack of novelty in both the delivery of training, training methods and inclusion of new materials and concepts. The aim of this task is thus to overcome this barrier in the future and introduce eLearning and e-approaches to training with relevance the field of gender studies and enable trainers build more successful course curricula. The task will thus start by mapping the ICT tools with a relevance to training, the potential that specific technologies entail for the delivery of training in a higher quality and reaching out to larger audiences. The second part of the task will thus be to make recommendations on the inclusion of specific technologies and eLearning methods as complementary to on-site trainings or for the development of fully online courses for the uptake of cybersecurity in hospitals measures.

T3.4 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)

This task involves the re-digestion of the information collected and delivered in the previous tasks and the development of a baseline report in the form of a handbook that sorts the information in a concise for its inclusion on the online hub. The baseline report will also constitute another iteration of the collection and review of relevant sources.

DELIVERABLES

D3.1 Cybersecurity in hospitals Knowledge Map (project month 6)

The Stakeholder map will present the collection of the sources, list the important materials and their relevance for the further developments in the project and an infographic of the ecosystem of cybersecurity in hospitals in Europe.

D3.2 European project and stakeholders on cybersecurity in hospitals report (project month 7)

This deliverable will present the collection of the related projects and initiatives, describe briefly each of the projects, why they are relevant for SecureHospitals.eu and the which concrete aspects from them allow for synergies and cooperation with the SecureHospitals.eu.

D3.3 State-of-the art and potentials for eLearning and Approaches in Cybersecurity in hospitals training report (project month 8)

The report will describe the state of the art of eLearning and e-approaches to training on cybersecurity in hospitals, analyse of the potential for increased usage of existing approaches (MOOCs, Webinars, Game-based learning, m-Learning, communities of practices and other online communities etc.), and also the implementation of additional ones in newly developed training courses on cybersecurity in hospitals.

D3.4 Cybersecurity in hospitals Knowledge Baseline Report (project month 9)

The baseline report will be delivered in the form of a handbook including a detailed library of sub-sources ready to be implemented on the online hub and transfer the relevant knowledge to trainers.

WP4 CREATE: STRUCTURED TRAINING SCHEMES AND CURRICULA FOR HOSPITAL STAFF & TRAINERS (Start Month 2)

Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	2	2	2	5	1	2	1	1

OBJECTIVES

Based on the outcomes and the knowledge acquired in Work package 2 and 3, this work package encompasses the main outputs of the project in its initial stage: the creation of new training materials and definition of certain quality standards that all trainings on cybersecurity in hospitals should feature. The training materials created will serve for carrying out trainings of trainers and practitioners in the second project period. The rest of the material created in this work package will support the future of training on cybersecurity in hospitals in two ways: first by defining minimum requirements required for training courses on cybersecurity in hospitals and second by creating guiding materials that support trainers develop tailor-made training courses. The needs for new course curricula and the quality standards will be developed on the basis of feedback from trainers and other cybersecurity experts.

The tasks defined in this work package are designed towards the achievement of Objective 3: '**CREATE** tailor-made training materials for trainers and IT practitioners to ensure the effective uptake of knowledge on data protection and privacy and cybersecurity measures.'

Achievements in this work package are marked with milestone **M5**.

DESCRIPTION OF WORK

T4.1 Collect and assess existing training courses and programmes on cybersecurity in hospitals across various domains (Lead: FPHAG, Participants: SAM, EUR, JOIN)

This task includes and extensive collection of course curricula, online training offers, training programmes as of academic training or outside of the academic field. An extensive collection of all major training offers throughout Europe will enable to get the bigger picture on the ecosystem and understand very clear gaps, inconsistencies or discrepancies across regions, territories and types of organisation. The collection of courses will furthermore be implemented on the online hub to allow practitioners search for trainings fit to their needs or trainers to advertise their trainings. Having an overview of the types of existing training offers will also allow to come to conclusions on quality standards in the following tasks and created materials.

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)

In order to support the creation of solid materials for training, the views from the field should also be measured. Along the analysis of existing courses by the project team, additional inputs will be sought from trainers and other experts involved in designing, evaluating and carrying out training courses and programmes on cybersecurity in hospitals. Feedback from the external experts is sought to address issues related to quality standards, needs assessment, barriers and opportunities for the implementation of novelty in training content and training delivery etc. The expert engagement will be decided by the tasks lead and it will feature a mix-method approach including stakeholder interviews, small workshops or focus groups.

T4.3 Create novel training curricula on cybesecurity in hospitals topics and define minimum quality standards for training material (Lead: INSP, Participants: EUR, FPHAG, SAM, JOIN)

Based on the feedback received by the trainers and related cybesecurity experts, this task includes the creation on one of the main outputs of the projects: the course curricula that will be implemented in the multiple trainings. New training materials will be created to respond to the needs of the field but also certain quality standards for the training curricula and the trainer profiles (require qualifications of trainers) will be defined. All materials will be designed in the form of infographics and be disseminated widely across all available channels but primarily through the online hub.

T4.4 Conceptualise online tools to support trainers in developing tailor-made courses on cybersecurity in hospitals (Lead: EUR, Participants: TLX, FPHAG, SAM, JOIN)

This task includes building a roadmap that leads trainers to the development of new curricula tailored to the needs for the training seekers. Based on the quality standards set out in the previous tasks, this task will build a step-by-step guide that helps in developing courses that meet required training standards on knowledge equality. The guide will be implemented as an online tool in the OAIH to support all trainers that visit the online network.

DELIVERABLES

D4.1 Cybersecurity in hospitals courses and programmes collection (project month 7)

This deliverable will present the collection of existing courses and programmes across Europe and beyond, describe and describe the offers briefly.

D3.2 Trainer interviews and workshops report (project month 8)

This report will present the feedback of the stakeholder engagement in the form of interviews and small workshops analysing the training need and the standard require for training on cybersecurity in hospitals in the European context. The trainer and relevant experts' feedback enables the creation of powerful materials for trainings as well as the definition of quality criteria that will be deal with in the upcoming reports.

D3.3 New cybersecurity in hospitals curricula and materials and quality assurance report (project month 10)

This major output will present some new course curricula developed by the project based on the expert feedback. The second stage of the report will define the quality standards of future courses.

D3.4 Step-by-step guide for the development of new course curricula (project month 13)

The guide will be delivered in a step-by-steam roadmap that can be useful in a pdf form but also as an online tool leading to tailored recommendations for the development of new course curricula.

WP5 BOOST: TRAINING INITIATIVES IN HOSPITALS AND INTEGRATION OF PROVIDERS AND COURSES (Start Month 1)

Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	4	3	0	2	3	2	5	2

OBJECTIVES

This work package constitutes the second major Contribution offered by the project to the field. The aim of the work package is to exploit the existing knowledge acquired by the European projects, institutions and other actors on cybersecurity in hospitals, and the training materials developed in the first stage. As the name of the work package conveys (BOOST) a long round of trainings including multiple formats will be carried out targeting trainers but also practitioners all over Europe. At the European level, a MOOC, a summer school and several webinars will be organised.

At the local level each of the partners will carry out at least four trainings in the form of workshops and knowledge cafes. These tasks contribute to the achievement of Objective 4: '**TRAIN** the trainers and practitioners all over Europe using different online and on-site training methods targeting stakeholders at the European and the local level'. Its major achievements broken down in the completion of the MOOC, the summer school and the local training rounds are marked with **M6, M7** and **M8** in the project workplan.

DESCRIPTION OF WORK

T5.1 Develop a training and engagement strategy to include specifically targeted audiences and means of training delivery (Lead: JOIN: Participants: SAM, FPHAG, EDE)

At the start of the training activities a master plan for the overall training and stakeholder engagement will be developed. The overall plan will define more specific audiences targeted for the training at European and local level and the means for reaching out to them. Tentative dates for the trainings and

training types will be defined and agreed by all consortium partners. This task involves two iterations: Primarily defining the stakeholders to be addressed and the strategy for contacting and engaging them; and secondly setting the timeline and agendas for all the other trainings.

T5.2 Create promotional materials and subscription forms for the MOOC, summer school and other project activities (Lead: EUR, Participants: INSP, COOS, EDE)

In order to the achieve wide attendance of trainers and practitioners in the MOOC and the summer school but then also in the local trainings, the release of promotional materials and subscription/registration forms at an early stage will be important. This task thus involved the creation of the promotional videos and additional materials for the MOOC and summer school. The video will feature experts from the consortium who will each of them. The aim of the video will be to describe the contents of the courses, methods used, the methods of assessment, the learning outcomes, and the targeted participants. Along with the video online registration forms for both the MOOC and summer school will be delivered and promoted extensively within the tasks of Work package 6.

T5.3 Design, promote and run the MOOC using the connectivist methodology allowing participant interaction and reuse or results (Lead: EUR, Participants: INSP, COOS, EDE)

This task includes the overall design and implementation of the MOOC. Initially the task leads will develop its curriculum (based on WP3), design assessments and online collaboration forms using the connectivist pedagogy model that allow reuse, remix and re-purposing of the content and active participation of the course participants. The whole course will be run within this task, the assignments evaluated and certificates to successful participants assigned.

T5.4 Plan, organise and implement the 'Cybersecurity in Hospitals Summer School' to train trainers and practitioners (Lead: JOIN, Participants: COOSS, SAM, FPHAG)

This task includes the planning, implementation and organisation of the summer school which will take place in a commonly agreed location. The task lead will be supported by other consortium members in designing the curriculum and the materials for the courses, designing other social activities, targeted audience etc.

T5.5 Conduct local workshops, knowledge cafes and webinars to deliver the knowledge to trainers and practitioners all over Europe (Lead: COOSS, Participants: JOIN, EDE)

All webinars in targeting trainers and practitioners at the European level and local training activities will be carried out within this task. A detailed plan and tentative agendas for the training will be set out in the second iteration of T5.1. The training will be partly conducted in local languages and fulfil comply with the key performance indicators.

DELIVERABLES

D5.1 Training Strategy 1 (project month 3)

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.

D5.2 Promotional materials and registration forms (project month 6)

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

D5.3 Training Strategy 2 (project month 11)

The second iteration of the training strategy will provide the timelines and agendas of local trainings and the webinars.

D5.4 SecureHospitals.eu MOOC report (project month 15)

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 SecureHospitals.eu summer school report (project month 20)

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

D5.6 Webinars and local trainings report (project month 23)

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.

WP6 COMMUNICATE: AWARNESS RAISING ON PROJECT ACTIVITIES AND PROMOTION OF THE HUB (Start Month 1)

Number	1	2	3	4	5	6	7	8
Partner	INSP	EUR	TLX	FPHAG	COOSS	SAM	JOIN	EDE
Person Months	4	2,5	1	1	1	1	1	5,5

OBJECTIVES

This work package will run throughout the whole project duration with the aim to communicate and broadly raise awareness on all project activities to the targeted audiences. This includes continuous communication activities primarily online through a strong web and social media presence. Besides continuous communication through newsletters, distribution of factsheets, news articles, blog posts on external channels and attendance the external events for the promotion of the project, this workpackage also includes the organisation of final conference at the project end.

The tasks in the work package correspond to the achievement of Objective 5**: 'COMMUNICATE** training needs, developments of the training schemes, project training initiatives and further awareness raising on the online awareness and information hub'. Two major achievement in the workpackage, the creation of the project website and the social media channels, and the full completion of the final conference marking the completion of all dissemination activities, are marked with milestones **M2** and **M9** in the project workplan.

DESCRIPTION OF WORK

T6.1 Setup the project website and social media channels and carry out continuous communication through online channels (Lead: EDE, Participants: ALL)

The project website will contain detailed information on the project aims, objectives, consortium, work packages and describe the progress towards their fulfilment. It provides information for all interested parties and the general public. The website will offer the opportunity to register for a periodical newsletter that provides updates on the project state and further information related to the project. The strong potential of social media for exposure of the project will be realised by setting up the most relevant channels (e.g. Twitter, Facebook, LinkedIn) and distributing content. Profiles will also be created

on third-party hubs to increase presence and visibility. This task includes creating the website, social media accounts and newsletter template and updating them continuously until the project end.

T6.2 Send out newsletters, distribute factsheets, leaflets and other infographics to raise awareness on the project activities (Lead: EDE, 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.

T6.3 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, EDE)

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.

T6.4 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)

This task aims at preparing a future exploitation plan for the project outputs, which will ensure the sustainability of the outcomes of the project and future use of the knowledge by all the partners involved.

T6.5 Organise the final 'Cybersecurity in Hospitals Awareness Conference' as a crucial event on the topic in close linkage with stakeholders and interest groups (Lead: EDE, 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.

DELIVERABLES

D6.1 Project website, social media accounts and communication channels (project month 3)

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.

D6.2 Dissemination materials (project month 5)

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)

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.

D6.4 Publication and presentation overview list (project month 26)

This deliverable will present the external contributions on blogs, news outlets, science magazines, external newsletters etc.

D6.5 Securehospitals.eu exploitation plan (project month 26)

The exploitation plan presents all exploitable project results and the partners' individual exploitation plans

D6.6 Cybersecurity in Hospitals Awareness Conference summary report (project month 26)

The conference report defines the scope, agenda, participants and outcomes of the conference. The focus here will also be on reflections on impacts, sustainability of results and future needs.

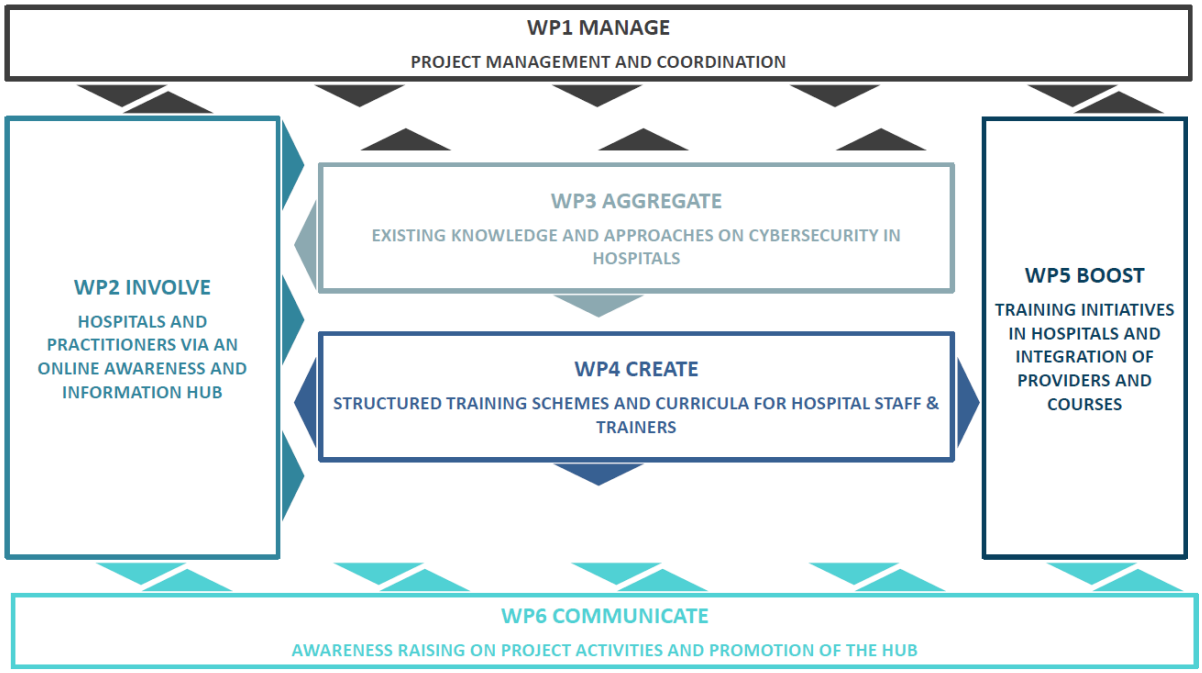


Figure 9: Work Packages Interdependencies

Table 6: List of Deliverables

No.	DELIVERABLE NAME	WP	LEAD	TYPE	DISS: LEVEL	DELIVERY MONTH
D1.1	Kick-off-meeting report	1	INSP	R	CO	2
D1.2	Data Management Plan	1	INSP	R	RE	6
D1.3	Status report and financial overview	1	INSP	R	RE	14
D1.4	Final project documentation and financial reporting	1	INSP	R	CO	26
D2.1	Stakeholder involvement roadmap and engagement strategy	2	COOS	R	PU	3
D2.2	Current perceptions and trends on cybersecurity in hospitals	2	EDE	O	PU	5
D2.3	Online Awareness and Information Hub www.securehospitals.eu	2	INSP	O	PU	8
D2.4	Relevant cybersecurity projects list and liaisons overview	2	INSP	O	PU	10
D3.1	Cybersecurity in hospitals Knowledge Map	3	FPHAG	O	RE	6
D3.2	European project and stakeholders on cybersecurity in hospitals report	3	JOIN	R	RE	7

D3.3	State-of-the art and potentials for eLearning and Approaches in Cybersecurity in hospitals training report	3	INSP	R	RE	8
D3.4	Cybersecurity in hospitals Knowledge Baseline Report	3	EUR	R	RE	9
D4.1	Cybersecurity in hospitals courses and programmes collection	4	FPHAG	R	PU	7
D4.2	Trainer interviews and workshops report	4	TLX	R	PU	8
D4.3	New cybersecurity in hospitals curricula and materials and quality assurance report	4	FPHAG	R	PU	10
D4.4	Step-by-step guide for the development of new course curricula	4	EUR	R	PU	13
D5.1/D5.3	Training Strategy 1 / Training Strategy 2	5	JOIN	R/O	PU	3/10
D5.2	Promotional materials and registration forms	5	EUR	O	PU	6
D5.3	MOOC report	5	EUR	R	PU	15
D5.4	Cybersecurity in Hospitals Summer School report	5	JOIN	R	PU	20
D5.5	Workshops, knowledge cafes and webinars overview and conclusions	5	COOSS	R	PU	23
D6.1	Project website, social media channels and communication activities	6	INSP	O	PU	3
D6.2	Dissemination materials	6	EDE	O	PU	5
D6.3	Dissemination activities report	6	EDE	R	PU	24
D6.4	Publication and presentation overview list	6	EUR	O	PU	26
D6.5	Securehospitals.eu exploitation plan	6	INSP	R	RE	26
D6.5	Cybersecurity in Hospitals Awareness Conference summary report	6	EDE	R	PU	26

3.2 Management structure and procedures

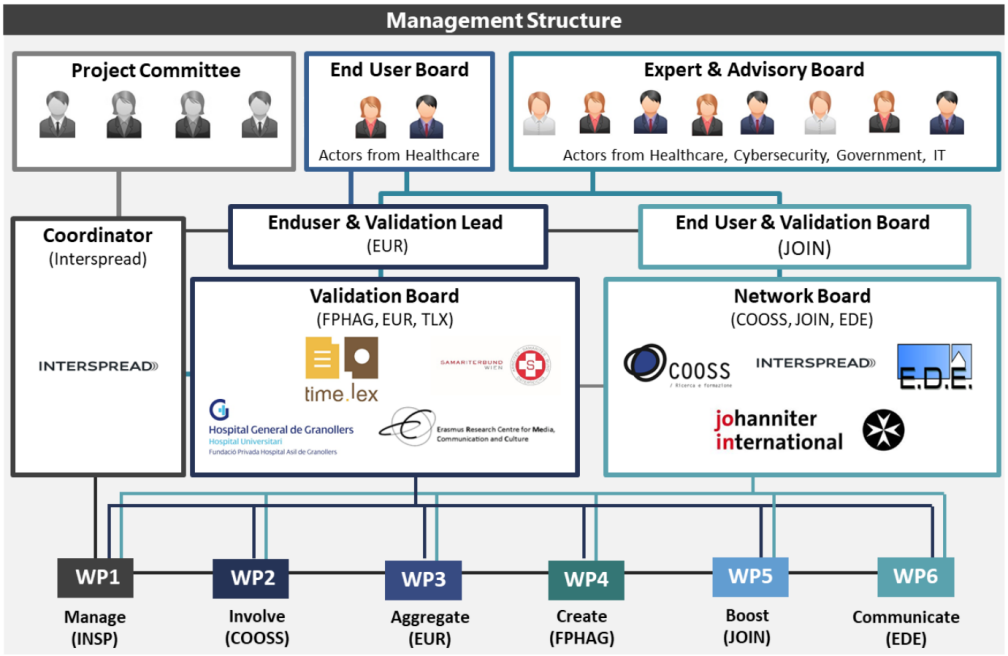


Figure 10: Organisational Management Structure

In this chapter, the organisational management structure will be described together with the management procedures. The organisational management structure includes the bodies involved in the project, the roles and responsibilities and its interdependencies, as well as the operational project management and the management procedures. These procedures include decision making mechanisms, meetings that will take place, knowledge and document management procedures as well as communication and collaboration procedures and tools. The project management will deal with the organisational, administrative, financial and operational issues of the project and the decision making.

3.2.1 Project Committee

The Project Committee (PC) consists of 2 representatives of each partner and is responsible for the general supervision of the project. One representative of INSP (coordinator) will be the chairman of the PC. The PC will meet initially for the kick-off. Of each meeting, a report (kick-off report and status meeting report) will be made available to the various participants and the EU, providing them with an overview and details on the progress of the project. The PC will decide on general principles and property rights, such as budget-related matters, financial planning, alterations of the Consortium Agreement and the acceptance or exclusion of new and existing parties. Every Partner shall have one vote in the Project Committee meetings. The quorum and rules of voting shall be further defined in the consortium agreement.

3.2.2 Coordinator

The Coordinator (INSP) will be in charge of all the coordination and management activities. The tasks that will be performed by the Coordinator are among others to Chair the Project and manage the overall legal, contractual, financial and administrative of the consortium. The coordinator will furthermore supervise various work packages (WP), the objectives of the project including the quality and timelines of the various findings and reports to the EU and ensure that the tasks regarding accession to the contract are carried out in a timely manner.

Concerning the communication between contractors and the Commission, the Coordinator will act as the intermediary and will therefore also prepare meetings and minutes of the project related meetings. Finally, the coordinator will manage a database with relevant contacts, project documents and a file with administrative notes and will inform the Commission of the sharing of the funds and the date of transfers to contractors. This is partly because the Coordinator will also receive all payments made by the Commission to the consortium and manage the Community contribution regarding its allocation between contractors and activities in accordance with this contract and the decisions taken by the consortium. The coordinator shall ensure that all the payments are made to contractors without unfounded delay.

3.2.3 Expert & Advisory Board (EAB)

An external Expert & Advisory Board (EAB) will be established within the Training Strategy developed in the WP 5 which is able to deliver valuable inputs and feedback at different stages of the project. It will provide a space for other external and associated stakeholders to participate in the project and it will contain representatives with different areas of relevance to the project. Through this board it will be able to build up direct linkages for networking activities (e.g. for stakeholder involvement and engagement) and further dissemination activities. When deemed necessary, EAB meetings will be connected with PC meetings (kick-off, status meeting) to build up strong interconnections between all members of the project. The use of such an instrument provides additional quality assurance in the form of high-level reflections and guidance for the SecureHospitals.eu action.

3.2.4 Decision making mechanism

The PC will decide about the distribution of the funding, about scientific and organisational steps that have to be taken and will approve financial and technical project reports to the European Commission. In case a partner is unable to fulfil its tasks, the PC has to decide on the removal of this partner from the project consortium. In case this partner is dismissed, or in case a partner should decide to drop out of the project

itself, the PC also decides democratically on the admission of a new partner taking over the tasks from the former partner.

In any case the new partner should be able to replace the old one in terms of expertise and origin. In case of other unforeseeable events affecting the further development and success of the project, the PC will decide democratically on alternative strategies to overcome the problems and to ensure the full success of the project.

The Kick-off will also be used to bring together the relevant persons of the Project Committee. The meeting will be used to solve all upcoming and foreseeable issues. If there is urgent need for action, the PC will make use of telephone conferences, email or other forms of electronic communication. If a physical meeting of the PC is necessary, the PC and the Coordinator can setup an additional meeting.

3.2.5 Conflict resolution

The coordinator INSP will endeavour to resolve any conflicts at the lowest possible level. Every work package leader is responsible to solve minor issues within his/her work package. Only if this fails the conflict will be discussed within the PC. An extraordinary meeting may be convened to resolve extremely urgent and/or serious cases.

3.2.6 Risk & Innovation Management

The SecureHospitals.eu consortium has built up a stringent work programme and allocated tasks and responsibilities precisely. Nevertheless, within a project runtime of 60 months some expected and unexpected situations may occur, that may have major influence on the successful outcome of the project. To reduce the overall risk to the project the coordinator INSP will fulfil also this role. Furthermore, the coordinator monitors, with support of other consortium partners, continuously the projects progress, achievements of milestones and task efforts to identify possible upcoming risks and problems immediately. This will enable to undertake counter measures at an early stage. Risks concerning intellectual property right will be dealt with in a separate way. In case of project funding by the European Commission, the consortium partners will sign a non-disclosure agreement and a consortium agreement before the beginning of the project in order to protect the intellectual property of SecureHospitals.eu. The consortium agreement will answer questions of ownership, the protection of pre-existing knowledge and project results, and access rights to and exploitation of pre-existing know-how and project results with regards to technical outcomes and licenses as well as social-scientific research results. Concerning IPR management, the consortium aspires to an agreement from which all consortium partners can benefit regarding their portfolio and expertise.

3.2.7 Milestones and Critical Risks

The following table contains a list of 10 strategically placed milestones, each of which documents a major achievement of the SecureHospitals.eu project.

Table 5: List of Milestones

NO.	MILESTONE NAME	RELATED WP(S)	MONTH	MEANS OF VERIFICATION
M1	Kick-off meeting	1	2	Kick-off meeting report submitted
M2	Project website and social media channels created	6	3	Deliverable 6.1 submitted
M3	Knowledge aggregation completed	2	9	Deliverable 3.4 submitted
M4	Creation of the open online information hub completed	3	11	Deliverable 2.4 submitted

M5	Creation of training schemes and materials completed	4	15	Deliverable 4.4 submitted
M6	MOOC completed	5	15	Deliverable 5.4 submitted
M7	Summer school completed	5	20	Deliverable 5.5 submitted
M8	All training activities completed	5	22	Deliverable 5.6 submitted
M9	SecureHospitals.eu conference completed	6	26	Deliverable 6.6 submitted
M10	Project finalised and documented	1	26	Deliverable 1.3 submitted

The following table gives an overview of possible risks from the administrative and technical sides, involved work packages and proposes mitigation measures to address these possibilities.

Table 6: Critical risks for implementation

DESCRIPTION OF RISK	WP(S) INVOLVED	PROPOSED RISK-MITIGATION MEASURES
Defaulting partner	1 – 6	Alternative distribution of missing partners' tasks
Communication problems in the consortium	1 – 6	Good communication rules in the communication strategy and support by modern communication technologies (Skype, etc.)
Disputes and conflicts among consortium partners	1 – 6	Effective and professional conflict management involving all conflict parties equally
Lack of internal work capacity	1 – 6	Outsourcing workload or coordinating workloads with partners
Possible deliverable or milestone delays during the project	1 – 6	Efficient project management will keep this risk to minimum by formulating internal timeframes. This risk will diminish with the on-going collaboration of partners
Poor engagement of other think-tanks and stakeholders	1-6	Engagement of all partners in the research in several project phases will keep this risk to a minimum through awareness raising channels and dissemination activities
Events fail to involve a large number of stakeholders or not the right ones	4	The vast network of experts from the think-tanks of the consortium, their affiliated fellows, board members and the SecureHospitals.eu Expert and Advisory Board will ensure that the project is well connected and disseminated in the community
Copyright issues regarding third party content and personalised data	3	Results will be published under Creative Common License
MOOC and summer school fail to have a lot of participants	5	Promotional materials and registration forms will be created at an earlier stage to ensure target audiences can be informed of the opportunities in advance

3.3 Consortium as a whole

The Consortium of SecureHospitals.eu was setup having in mind the fact that extensive data is expected to be delivered and complementary insights analysed and interpreted against the background of the projects' objectives. Furthermore, it is expected that the partners of the consortium fully contribute to communicating and disseminating the results, in particular the networking partners, and the solutions of the project among the main stakeholders. In general, the SecureHospitals.eu consortium provides the necessary expertise to run this project in the best possible way, while covering major geographical axes of the EU.

The consortium shows a **high complementarity and balance** concerning nationality, type of partner, expertise, role in the project and gender balance. In order to bring together the optimal consortium for this project, the coordinator was well aware of the fact that the project consortium needs to be focussed on the expertise that is essential for the success of the project. With this in mind, the coordinator set up a consortium for the SecureHospitals.eu project that unites the leading expertise in the relevant fields while at the same time providing practical or "on-the-ground" experience as well as relevant networks for dissemination.

The 8 consortium partners are located in the following EU member states and associated countries: **Austria, Netherlands, Belgium, Spain, Italy** and **Czech Republic**. External support is provided (through LoS) by associations with background from the healthcare sector, NGOs and research centres working in the fields as well as from cybersecurity companies.

Tackling the challenges related to the issues of the project requires integrating concepts, methods, and principles from different academic disciplines. To this end, SecureHospitals.eu will have **an interdisciplinary consortium** consisting of partners with expertise from a variety of disciplines such as cybersecurity, legal and ethical issues, health care and hospitals, computer science / technical expertise, training expertise / education and communication science. Especially the **hospital** and **enduser organisation** partners (FPHAG, COOSS, JOIN and SAM) will contribute with their hands-on experience and network competence to work on the project. Their involvement ensures that the solutions are tailored to the requirements and needs of European hospitals and healthcare organisations and that the solutions are further taken up and used – based on an elaborate SecureHospitals.eu exploitation planning. Complementary to the end user partners, the consortium also integrates **legal competence** (TLX) as well as experienced partners in **training development** (EUR).

Finally, the most well-connected **networking partners** in the field of healthcare (EDE, COOSS, JOIN) will ensure the communication of the project through relevant channels and a wide distribution of the project results among the wider community of EU citizens.

The project consortium will be coordinated by **INTERSPREAD** (Coordinator and Lead Development Partner, Leader WP1 and WP4) from Austria. As a matter of risk management, there are of course some overlapping expertise areas for certain partners. This will increase the reliability and significance of the outcomes of the project and guarantee its success. The following table shows the distribution of the expertise, experiences and skillsets of the partners along six main dimensions. The table highlights the fact that the competencies required for a successful work on this particular project are all fully covered.

Table 11. Matrix of core competencies of the consortium

CORE COMPETENCIES	TECHNICAL PARTNER	EXPERTISE ON CYBERCRIME AND	END USER-ORGANISATION / HOSPITAL	TRAINING DEVELOPMENT	LEGAL ISSUES, ETHICS & DATA	NETWORKING, COMMUNICATION
SYNYO	X	X				X
EUR				X		X
TLX		X				X
FPHAG			X	X		
COOSS			X		X	
ASM			X			
JOIN			X		X	X
EDE				X	X	X
EUR		X	X			

3.4 Resources to be committed

The overall financial plan consists of the personnel costs (person months x monthly salary), travel costs (for kick-off meetings, review and work meetings, conferences, policy dialogues and workshops), other costs (composed of equipment costs, costs for other goods and services, events organisation and dissemination materials). For a project duration of 26 months, a total of € 998.063 are requested for funding in order to cover the 106-person-months estimated according to the efforts requested by the participants to project activities. The distribution of resources effort is shown in Figure 11.

Part.No. PARTICIPANT Reimbursement Rate (RIA)	1 INSP 100%	2 EUR 100%	3 TLX 100%	4 FPHAG 100%	5 COOSS 100%	6 SAM 100%	7 JOIN 100%	8 EDE 100%	TOTAL
PERSONNEL COSTS	180.000	97.500	52.800	83.700	45.150	48.000	71.300	66.000	644.450
Average personnel costs for 1 PM	6.100	6.500	9.600	6.200	4.300	6.000	6.200	5.500	
TOTAL PERSON MONTH	30	15	5,5	13,5	10,5	8	11,5	12	106
PM WP1	10	0,5	0,5	0,5	0,5	0,5	0,5	0,5	13,5
PM WP2	5	2	1	2	4	1	1	2	18
PM WP3	4	5	1	3	1	1,5	3	1	19,5
PM WP4	2	2	2	5	1	2	1	1	16
PM WP5	4	3	0	2	3	2	5	2	21
PM WP6	4	2,5	1	1	1	1	1	5,5	17
OTHER COSTS	28.000	17.000	15.000	16.000	20.000	16.000	20.000	22.000	154.000
Travel Costs	15.000	12.000	12.000	12.000	12.000	12.000	12.000	12.000	99.000
Equipment Costs	3.000	0	0	0	0	0	0	0	3.000
Other Goods and Services Costs	10.000	5.000	3.000	4.000	8.000	4.000	8.000	10.000	52.000
SUBCONTRACTING COSTS	0	0	0	0	0	0	0	0	0
Subcontracting Third Parties	0	0	0	0	0	0	0	0	0
DIRECT COSTS	208.000	114.500	67.800	99.700	65.150	64.000	91.300	88.000	798.450
INDIRECT COSTS (25%)	52.000	28.625	16.950	24.925	16.288	16.000	22.825	22.000	199.613
TOTAL COSTS	260.000	143.125	84.750	124.625	81.438	80.000	114.125	110.000	998.063
REQUESTED GRANT (EC)	260.000	143.125	84.750	124.625	81.438	80.000	114.125	110.000	998.063

Figure 11: SecureHospitals.eu budget overview

3.4.1 Summary of staff effort and resource distribution

Figure 11 shows the individual contributions of partners in terms of PM in all of the six work packages. The largest share is held by INSP, as project coordinator (leader of WP1), followed by a relative even share between the rest of the partners. Regarding gender aspects the team aimed at equally distributing PM between female and male project team members. The consortium ensures a wide regional outreach and thus greatly facilitates the dissemination of the projects outputs and results. As the consortium aims at achieving maximum visibility, around 18% of the total effort is allocated to dissemination activities and materials. Another 14% is allocated to the development and maintenance of the online tools and strategies for training delivery which serve also as the project's main communication and dissemination channel. This makes a total of 32% of the overall efforts allocated to involving the cybersecurity and healthcare community, raising awareness on the project activities and findings while ensuring a long-lasting effect on the future generations of gender specialists by making available the relevant facts and trainings in one place. Furthermore, the consortium made great efforts to minimise the costs of management activities.

3.4.2 Other costs

The amount of the budget allocated to other costs includes the travels costs, equipment costs and costs for other goods and services.

Travel Costs - The overall budget for travel expenses is € 99.000 and is based on an estimation of the cost for the kick-off-meeting, reviews and work meetings and other events (Conferences/Summer School/Trainings etc.) per Beneficiary's employees of € 1.000. These costs are calculated to include transportation, accommodation and subsistence expenses.

Equipment cost - The budget for equipment includes costs spent for the web-based collaboration platform and a collaboration & document sharing system and necessary hardware/software for the MOOC development. The total amount of the equipment costs is 3.000.

Other Goods and Services - Additional resources were allocated for the SecureHospitals.eu Events including trainings, summer school and conference. The trainings will be organised by each of the partners locally. This comprises therefore the organisation of the trainings, comprised of venue rental fees for meetings, translation cost as per the multilingual character of the project and pan-European outreach strategy, expenses related to dissemination materials expected to be developed as a part of strengthening and broadening the European ecosystem. Therefore, trainings are allocated all over Europe targeting at local stakeholders in different regions. Furthermore, the coordinator, INSP holds budget for organization of the kick off meeting. The total amount of the other goods and services is 52.000.

Participant 1 **INSP**	**Cost (€)**	**Justification**
Travel	15.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	3000	

Participant 2 **EUR**	**Cost (€)**	**Justification**
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 3	**Cost (€)**	**Justification**

TLX		
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 4 FPHAG	Cost (€)	Justification
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 5 COOSS	Cost (€)	Justification
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 6 UNIBO	Cost (€)	Justification
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 7 SAM	Cost (€)	Justification
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

Participant 8 JOIN	Cost (€)	Justification
Travel	12.000	This includes the base travel costs for the participation to the kick-off meeting, work and review meetings, workshops as well as to the final Networking event.
Equipment	0	

SecureHospitals.eu

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

Topic: Raising awareness and developing training schemes on cybersecurity in hospitals

Coordinator Contact: Dr. Florian Huber, INTERSPREAD GmbH, florian.huber@interspread.com

Table of Contents

4. Members of the consortium 53

4.1. Participants (applicants) 53

4.2. Third parties involved in the project (including use of third party resources) 69

5. LETTERS OF SUPPORT 70

6. ETHICS AND SECURITY 74

6.1 Ethics 74

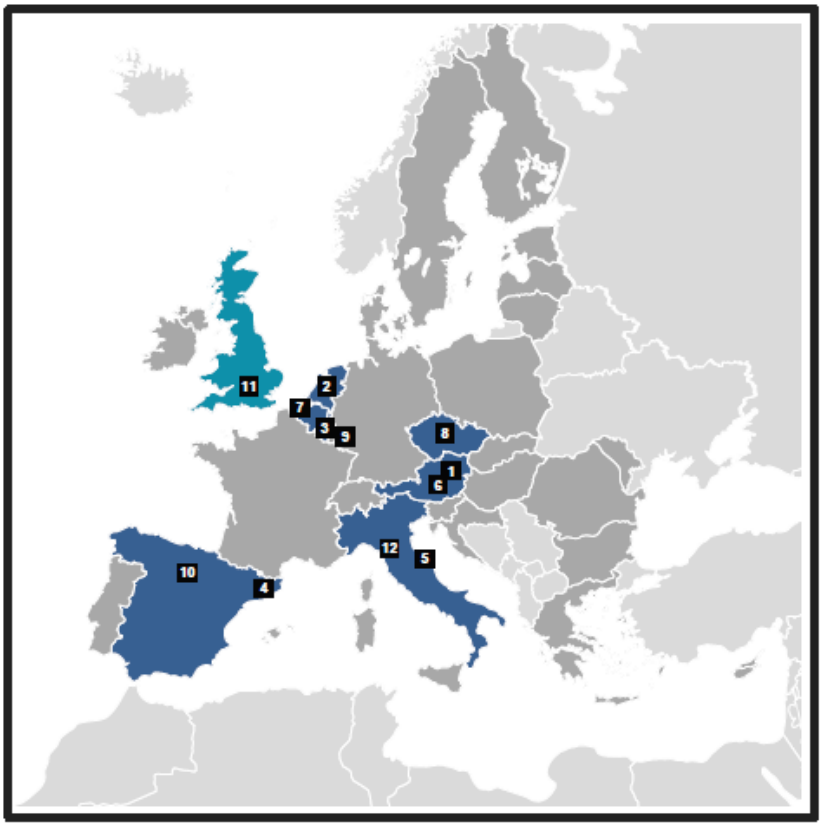
6.2 Security 76

SecureHospitals.eu Consortium Map

Interspread 1
Research & Development Department
Vienna
AUSTRIA

Erasmus University 2
Department of Media and Communication
Rotterdam
THE NETHERLANDS

Time.lex CVBA 3
Brussels
BELGIUM



Fundació Privada Hospital Asil De Granollers 4
Research and Innovation Unit
Granollers
SPAIN

COOSS Marche Onlus 5
Research & Training Department
Ancona
ITALY

Arbeitersamariterbund 6
Research & Training Department
Vienna
Austria

Johanniter International 7
Brussels
BELGIUM

European Association for Directors and Providers of Long-Term Care Services for the Elderly (E.D.E.) absl. 8
Prague
CZECH REPUBLIC

European Association for Directors and Providers of Long-Term Care Services for the Elderly 9
Luxemburg
LUXEMBURG

Erle Robotics S.L. 10
Vitoria
SPAIN

Cyber London Ltd 11
London
UK

Legend
Main Project Partners
Supporters of the Project

Dedalus 12
Bologna
ITALY

4. Members of the consortium

4.1. Participants (applicants)

INTERSPREAD GMBH RESEARCH AND DEVELOPMENT DEPARTMENT		Number	1
SHORT NAME	INSP	INTERSPREAD	
TYPE	SME		
COUNTRY	Austria		

DESCRIPTION OF THE ORGANISATION

INTERSPREAD GmbH (INSP) is a research and innovation company active on a global scale. Indeed, a truly global mindset is reflected in all activities when collaborating with cross-disciplinary clients active in different industries. Considering the state of the art in digital transformation technologies INTERSPREAD provides intelligent technologies, valuable services, market assessments and sustainable solutions to clients. Clients include publicly listed technology companies, research organizations, governments, NGOs, and industrial sector. INTERSPREAD was founded in 2014 as a spinoff of a leading research organization. Thus, people at INTERSPREAD hold profound knowledge on the management and coordination of large-scale transnational projects. An extensive pool of knowledge is also shared with the well-established sister company.

MAIN TASKS IN THE PROJECT

INSP will coordinate the project thus lead WP 1. It will also contribute to all WPs by steering the work of other partners. Its expertise will mainly be dedicated to dissemination activities in WP6, T6.1 and 6.4 and the involvement activities in WP2. Moreover, INSP contributes to WP3, leading T3.3 the assessment of ICT tools.

PREVIOUS EXPERIENCE

INTERSPREAD has already developed and implemented a number of concepts to national and international companies in selected industries (consumer goods, telecommunications, and retail) and political organizations such as the Ministry of the Interior and the City of Vienna. Additionally, INTERSPREAD is a member of various innovator networks and well-connected within the scientific community to keep up to date on new technologies, features and methodologies in the field of web applications, monitoring tools and interface design.

Relevant publications:

Open Data Topologies, Catalogues and Metadata Harmonization. From the OpenDataMonitor Project http://project.opendatamonitor.eu/images/deliverables/OpenDataMonitor_611988_D2.1-Open-data-topologies-catalogues-and-metadata-harmonisation.pdf

Best Practice Visualisation, Dashboards and Key Figures. From the OpenDataMonitor Project http://project.opendatamonitor.eu/images/deliverables/OpenDataMonitor_611988_D2.3-Best-practice-visualisation,-dashboard-and-key-figures-report.pdf

Neuschmid, Julia/Gajevic, Ljubica/Schrenk, Manfred/Wasserburger, Wolfgang (2014): *The Blind's Critical Space and the Role of Modern ICT*, in: Critical Spaces. Contemporary perspectives in urban, spatial and landscape studies.

Jäger, Bernhard/Leitner, Peter (2013): *Design Considerations for the Development of Intuitive Social Media Analytics Tools*, in: Proceedings of the IADIS International Conference Interface and Human Computer Interaction 2013, Prague, Czech Republic, 22.-26.7.2013, IADIS Press, pp. 311-316.

Relevant Projects:

INTERSPREAD is actively involved in 3 ongoing collaborative FP7 projects, acting as technical coordinator in one (UniteEurope) and as overall coordinator in two others (OpenDataMonitor and Graffolution). In addition, INTERSPREAD just started a new Urban Europe (Joint Programming Initiative) project entitled UrbanData2Decide. All of these projects deal with the development of web-based platform with novel services and collaboration spaces:

OpenDataMonitor: Monitoring, Analysis and Visualisation of Open Data Catalogues, Hubs and Repositories (Number: 611988)

Graffolution: Awareness and Prevention Solutions against Graffiti Vandalism in Public Areas and Transport (Number: 608152)

UrbanData2Decide: Integrated Data Visualisation and Decision Making Solutions to Forecast and Manage Complex Urban Challenges

UniteEurope: Social Media Analytics and Decision Support Tools Enabling Sustainable Integration Policies and Measures (Number: 288308)

SHORT PROFILES OF STAFF MEMBERS

Peter Leitner (M) is Head of Research and Development at INTERSPREAD. He holds two masters and received his Ph.D. from the Vienna University of Technology. Dr. Leitner has extensive experience in the field of software engineering, complex web platforms, innovative applications and analytical solutions. As well he is architect for large IT systems and has a broad know how on innovative frameworks and information visualisation engines. He has extensive project and risk management skills combined with 13 years of practical experience. Beside his activities at INTERSPREAD Dr. Leitner is a lecturer for project management and software engineering at the Vienna University of Technology.

Mag. Diotima Bertel (female) is a Research Manager at SYNYO GmbH. She holds a master's degree in Communication Science and bachelor's degrees in Communication Science and Comparative Literature. She has broad experience in the field of Active and Assisted Living and has worked for a range of AAL projects, both at AIT – Austrian Institute of Technology and the national Austrian work group AAL Austria; with a focus on user experience and stakeholder requirements. Additionally, she teaches at the University of Vienna.

Adela Nacu (female) is a Research Manager at SYNYO GmbH. She holds a Master of Science Degree in European Spatial Planning and has four years' experience in international projects related to urban development issues, among which are strategic planning, urban regeneration, end-user engagement in the processes related to ICT and smart cities. Steered by the sustainable development values her background is supported by skills such as empirical research and capacity development. Complementary to her skills she has extensive experience in international dissemination activities and conference facilitation.

Ermia Anvari (male) is a Software Engineer at SYNYO. He holds a Bachelor degree in Software Engineering from Technical university of Hungary. He moved to Vienna to continue studying for master degree from Technical university of Vienna and he is doing his master besides work. He has nearly 3 years of work experience in E-Commerce Platform in MackTak Mart Corp from 2012 to 2015 and also his Diploma project was in E-Commerce and Search Engine Optimization. He has the variety of

knowledge and skills in two main programming language PHP and JAVA and some technology and frameworks from these programming languages. Ermia is the leading developer of the PeaceTraining.eu web platform.

Iulia Luca, BSc (female) is a Graphic Designer at SYNYO GmbH. She holds a Bachelor of Science in Landscape Architecture. After her studies she has worked with different graphic design agencies from which she gained practical experience by developing artwork and creating graphic design solutions from concept through to completion. At SYNYO, she is involved in creating dissemination materials for different projects, corporate identity and media design. She is responsible for creating visual concepts, layout development, branding and advertising in both print and digital media. Combining her visual skills with her professional background, she delivers efficient graphic output with a strong focus on marketing design, by using a wide range of design software.

ERASMUS UNIVERSITY DEPARTMENT OF MEDIA AND COMMUNICATION		**Number**	**2**
SHORT NAME	**EUR**	Erasmus Research Centre for Media, Communication and Culture	
TYPE	**UNIVERSITY**		
COUNTRY	**THE NETHERLANDS**		

DESCRIPTION OF THE ORGANISATION

Erasmus University Rotterdam (EUR) is an internationally oriented research university with a strong social orientation in its research and teaching. Its scientists and students endeavour to solve global social challenges, drawing inspiration from the ever dynamic and cosmopolitan Rotterdam. Its academic education is intensive, active and application-based, and its research is increasingly carried out in multidisciplinary teams, which are closely interlinked with international networks. With its research impact and study quality, EUR can compete with the top European universities. Important values for Erasmus University Rotterdam are daring, curiosity, social engagement, working at the frontier and striving for success. More than 3.000 persons are employed by Erasmus University.

The **Erasmus Research Centre for Media, Communication, and Culture (ERMeCC)** carries out interdisciplinary research on media, communication and culture. The Centre's mission is to operate as an international, national and local centre of expertise for high-quality research into the myriad relationships between media, society and culture. Its research is empirical, interdisciplinary and comparative, informed by work in various social sciences, in particular media and communication studies and sociology. ERMeCC's Media, algorithms, privacy and surveillance research cluster focuses on personal, social, and ethical consequences, and (cyber) security threats of mobile and interconnected media technologies and devices. The centre houses the ERMeCC Digital Research Lab, which caters to the centre's research themes and offers resources for research into digital data and media.

MAIN TASKS IN THE PROJECT

EUR will lead WP3 about the aggregation of existing knowledge, in particular T3.4. More than that, EUR leads T4.4 about the conceptualization of online tools and is strongly involved in WP5. Here, EUR is leading two tasks T5.3 and T5.4 and will contribute to WP6 by leading T6.3 for the scientific community by attending external events and conferences.

PREVIOUS EXPERIENCE

Publications

Pridmore, J. (2017). The Consumer-Citizen Nexus: Surveillance and Concerns for an Emerging Citizenship. In: Jürgen Mackert & Bryan S. Turner (Eds), The Transformation of Citizenship. New York: Routledge.

Van der Ploeg, Irma and Jason Pridmore (eds.) (2016) Digitising Identities: Doing Identity in a Networked World. New York: Routledge.

Bouman, M.P.A., Lubjuhn, S. & Singhal, A. (2016): The Positive Deviance approach in action. In: Parvanta, C., Nelson, D.E., Parvanta, S.A., Harner, R.N. (Eds.) Essentials of Public Health Communication, Jones and Bartlett Learning

Bouman, M.P.A. (2014): Entertainment-Education in Western Countries, SAGE Encyclopedia of Health Communication (Teresa L. Thompson), SAGE Publications.

Bouman, M.P.A., Drossaert, C.H.C., Pieterse, M.E. (2012) Mark My Words: The Design of an Innovative Methodology to Track Down and Analyze Interpersonal Health Conversations in Web and Social Media, Journal of Technology in Human Science, 30:3-4, 312-326.

Relevant Actions

The Erasmus University houses the ERMeCC Digital Research Lab, which caters to the centre's research themes and offers resources for research into digital data and media.

Previous projects

Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems: This project focuses on how users determine privacy and security concerns within the contextual choices they make with mobile devices. More specifically, the project maps how Dutch and American users of mobile neighbourhood watch groups, intelligent personal assistants, and fitness apps and wearables consider and make decisions about their personal data and privacy. (https://www.eshcc.eur.nl/english/ermecc/projects/mobile_privacy/)

The BOLD Cities 'Big Data for Youth Policy' Project concentrates on the identification of NEET youth (Young people Not Employed, in Education or Training) that often slip through a municipalities normal registration practices. This project will develop policies on privacy sensitive means to discover and integrate vulnerable NEET youth in the City of Rotterdam.

Digital Vigilantism: Visibility as a tool for social change and social harm explores Digital Vigilantism in the Netherlands, the United Kingdom, China and Russia. Its theoretical and empirical findings will inform a conceptually rigorous and nuanced understanding of the motivations and practices that surround digital vigilantism, alongside recommendations for key stakeholders. (https://www.eshcc.eur.nl/english/ermecc/projects/digital_vigilantism/)

RESPECT (Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies) seeks to investigate whether the current and foreseeable implementation of ICTs in surveillance is indeed "in balance" and, where a lack of balance may exist or is perceived by citizens not to exist, the project explores options for redressing the balance through a combination of Privacy- Enhancing Technologies and operational approaches. (http://respectproject.eu/)

Mark My Words project focused on young people as they make intensive use of social and interactive media to talk about their lifestyle, hobbies, experiences and insights. There is a great need for contemporary methods to be able to measure the effects of health communication interventions in

which social media play a major role. The project developed a new method for monitoring conversations about healthy lifestyle among young people via social media

SHORT PROFILES OF STAFF MEMBERS

Jason Pridmore (male) is an Assistant Professor in the Department of Media and Communication. His work focuses on practices of digital identification, mobile devices, security issues, social media, and consumer data. Jason participated in an advisory/managing capacity for a range of EU and Dutch projects, including PRISMS, the MOSAIC project, and the Privacy in the 21st century project. Currently, Jason leads the NWO-funded project Mapping Privacy and Surveillance Dynamics in Emerging Mobile Ecosystems. He is co-editor of Digitising Identities with Routledge, associate editor of Surveillance & Society and has published on surveillance, security, and consumer marketing. Jason worked as senior researcher on the Digideas Project on the social and ethical issues that arise in relation to digital identification. He completed his PhD at Queen's University in Kingston, Canada.

Martine Bouman (female) is Scientific Director and founder of the Center for Media & Health in Gouda and a professor occupying an endowed chair in Entertainment Media and Social Change at Erasmus University (at the Erasmus Research Centre for Media, Communication and Culture, ERMeCC). She obtained her doctorate at Wageningen University in 1999 and published her ground-breaking dissertation 'The Turtle and the Peacock: the entertainment-education strategy on television'. Her current research focuses on media use, popular culture, storytelling, health-related communication, functional illiteracy, and socioeconomic disparities in health. She is an international award winner and an expert in the field of Entertainment Education for Social Change (EE). She has many years of experience in designing, implementing and researching healthy lifestyle projects and campaigns. She works with and has worked with creative professionals on various media projects such as Medisch Centrum West, Costa, Je Echte Leeftijd and Nederland in Beweging.

Roel Lutkenhaus (male) is a PhD candidate at the Erasmus Research Center for Media, Communication and Culture and the Centre for Media & Health in Gouda. As a PhD candidate, he researches the effects of interactive storytelling in Entertainment-Education (EE) strategies on a health related behavior. His PhD-project focuses on storytelling, media planning, and collaboration strategies, as well as on methods to study the target audiences' behaviors and preferences (formative research) and measuring the reach and impact of EE interventions (process and summative research).

TIME.LEX CVBA		**Number**	**3**
SHORT NAME	**TLX**		
TYPE	**SME**		
COUNTRY	**Belgium**		

DESCRIPTION OF THE ORGANISATION

time.lex is a *niche* law firm of about 20 lawyers based in Brussels, specialised in information technology and electronic communications law in the broadest sense, including privacy protection, data and information management, e-business, intellectual property and telecommunications. Its activities cover all legal issues encountered in the creation, management and exploitation of information and technology, in all of its diverse forms.

time.lex as an independent firm was founded in 2007, but all its lawyers started their career in international law firms and multinational companies. The team is internationally recognised, being both

a ***Legal 500 Top Tier*** firm in Information Technology, and a ***Chambers Europe Recommended*** Firm for TMT - Information Technology, Intellectual Property, Data Protection and Entertainment.
The time.lex team is specifically known for its European policy studies in a variety of subjects, including electronic communications, data protection, electronic signatures, electronic identity management, e-business and e-government, in which they can rely on an extensive network of IT law experts covering all European countries

Most of the time.lex partners and associates are former researchers of KU Leuven and acquired a strong experience in ***legal research*** during their academic career in the Interdisciplinary Centre for Law and ICT (www.icri.be) and iMinds (www.imec.be). Today time.lex is involved in a series of research and innovation actions and participates as a legal partner in a series of ongoing Horizon 2020 Actions.

From a ***business perspective***, time.lex frequently assists companies in establishing suitable policies and legal frameworks in their data management activities, including about the cross-border transfer and processing of personal data, data security and liability management issues. Its clients include private companies and public sector bodies in the IT sector, financial services, e-health, marketing and e-commerce.
Being specialized in inter alia cyber law, data protection law and health law, as well as the interaction between those fields of law, time.lex presents a good fit to deal with the legal aspects of this action.

MAIN TASKS IN THE PROJECT

In this project, TLX will play an expert role and contribute to raised legal issues and questions. As such, TLX is going to contribute to WP3, T3.3 and lead T4.2.

PREVIOUS EXPERIENCE

Relevant Publications:

DUMORTIER, J., Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation) (July 1, 2016). Available at SSRN: https://ssrn.com/abstract=2855484

DUMORTIER, Jos and VERHENNEMAN, Griet (2012) "Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US" in Carlisle George, Diane Whitehouse and Penny Duquenoy, eHealth: Legal, Ethical and Governance Challenges, Springer-Verlag, 398

WUYTS K., VERHENNEMAN G., SCANDARIATO R., JOOSEN W., DUMORTIER J.(2012). What electronic health records don't know just yet. A privacy analysis for patient communities and health records interaction. Health and Technology. Springer nr.2 , pp. 159-183 , ISSN 2190-7188

DUMORTIER, Jos, Study on a Legal Framework for Interoperable eHealth in Europe, European Commission, 2009, http://ec.europa.eu/information_society/activities/health/docs/studies/legal-fw-interop/ehealth-legal-fmwk-final-report.pdf

Relevant Projects:

European Commission – Horizon 2020 - Legal assistance of the Horizon 2020 KONFIDO project: The 36-month KONFIDO project aims to advance the state of the art of eHealth technology targeting all architectural layers of an IT infrastructure, namely: storage, dissemination, processing, and presentation – to address challenges of secure storage and exchange of eHealth data, protection and control over personal data, and security of health related data gathered by mobile devices. KONFIDO will build on and extend the results of a best of breed selection of successful projects (namely: epSOS, STORK, DECIPHER, EXPAND and ANTILOPE). time.lex provides extensive legal advice & support in KONFIDO.

European Commission – Horizon 2020 - AEGLE – An analytics framework for integrated and personalized healthcare services in Europe: Horizon 2020 project building a European scale big data eHealth cloud. AEGLE will process health data in relation to live patients from four Member States on cases covering diabetes, leukemia and intensive care, in order to provide better analysis and clinical therapeutic support. time.lex leads the legal work package of EAGLE.
European Commission – Horizon 2020 -OACTIVE - Advanced personalised, multi-scale computer models preventing OsteoArthritis: The OActive project aims to transform and accelerate the diagnosis and prediction of osteoarthritis. With the use of data and augmented reality, the experts will achieve a more comprehensive and holistic understanding of disease pathophysiology, dynamics, and patient outcomes. time.lex is in charge of ensuring compliance with data protection law, IP law & licensing and ethics.
European Commission – DG CONNECT - Development Leader – Project Editor for European EC Code of Conduct on Mobile Health Apps: time.lex is assisting a team of mobile health industry experts in Europe in drafting a Code of Conduct for cloud service providers, as a tool to facilitate high quality data protection compliance. The assignment includes liaising with the various representatives, drafting/editing the Code of Conduct itself, and seeking its endorsement by the Article 29 Working Party.
European Commission – DG Health - Overview of the national laws on electronic health records in the EU Member States: Study performed by time.lex aiming to provide an overview of the national laws on electronic health records within the EU Member States, and assessing the interaction of these national laws with the provision of cross-border eHealth services mentioned in Directive on patients' rights in cross-border healthcare (2011/24/EU).

SHORT PROFILES OF STAFF MEMBERS

Hans Graux (male) graduated in Law in 2002, and obtained a complementary degree in IT in 2003 (both at K.U.Leuven, Cum Laude). He then joined the Interdisciplinary Centre for Law and Information Technology, where he did fundamental research on a number of IT law related issues, with a specific focus on electronic identity management. In May 2005 he became a lawyer at the bar of Brussels, and participated in a number of international ICT policy studies, primarily for the European Commission. In July 2007, he co-founded the IT law firm time.lex. His expertise lies in the collection of legal and administrative information in cross border studies, in the analysis of legal frameworks and policy choices, and in formulating policy recommendations to eliminate barriers to the correct functioning of the internal market. His recent work for the European Commission has focused on the European Cloud Strategy, eSignatures, electronic identity management, data protection, e-business and the implementation of the Services Directive.

Prof. Dr. **Jos Dumortier** (male) is an honorary professor in Information Technology Law and Electronic Communications Law at the Faculty of Law, KU Leuven since 1989 and the founder of the Interdisciplinary Centre for Law and Information Technology (ICRI). With this research group he has been in charge of the legal guidance of a large number of IT law and IT policy related research and development projects in Belgium. As a regular expert working for the Belgian government he has been intensively involved in the development of the Belgian federal and regional legal frameworks with regard to ICT and electronic communications. Prof. Dumortier frequently works as an expert for the European Commission, foreign governments and for private organisations. He is a member of several boards and committees in Belgium and abroad. Professor Dumortier published numerous books and articles on various issues related to information technology law. He is the editor of the International

Encyclopaedia of Cyber Law. Since 2014 Jos Dumortier left his functions at the University of Leuven and works on a full-time basis as a time.lex lawyer in Brussels.

Pieter Gryffoy (male) has a Master of Laws degree (Cum Laude) from KU Leuven (2014) and a degree of Master of Laws in International and European Law (Summa Cum Laude) from Saarland University (2015). Before joining time.lex in October 2016 Pieter was employed as an academic researcher at the Jean Monnet Chair for European Law and European Integration at Saarland University. In that capacity Pieter mainly researched the current challenges facing data protection in the European Union. He also published several articles on data protection related topics. Pieter specializes in privacy and data protection, ICT law and intellectual property law. He also has a special interest in questions of private international law related to those fields.

Zenzi De Graeve (female) joined time.lex in September 2017. Zenzi obtained a Master of Laws degree in 2016 and a complementary Master in Intellectual Property Rights and ICT Law in 2017 (both at the Faculty of Law of the Catholic University of Leuven, Cum Laude). During the Master of Laws, Zenzi participated in the ELSA WTO Moot Court Competition as representative for the Faculty of Law of the Catholic University of Leuven. Her team won the Regional Eound in Czech Republic and qualified for the semi-finals at the International Round in Switzerland. Zenzi specializes in privacy and data protection, intellectual property law and ICT law.

ACIÓ PRIVADA HOSPITAL ASIL DE GRANOLLERS		**Number**	**4**
SHORT NAME	**FPHAG**	Hospital General de Granollers Hospital Universitari Fundació Privada Hospital Asil de Granollers	
TYPE	**Non for profit**		
COUNTRY	**Spain**		

DESCRIPTION OF THE ORGANISATION

The **Fundació Privada Hospital Asil de Granollers (FPHAG)** is a healthcare, socio-sanitary and social care center, integrated into the comprehensive healthcare system of Catalonia. FPHAG comprises the Geriatric Center Adolfo Montañá and the General Hospital of Granollers, which provides health care assistance both for acute and non- acute patients and it is the reference hospital of the territories comprising the area known as Vallès Oriental, covering a population of around 400000 people and with a total number of beds of 340. Another important role is played by the Sant Jordi Day Care Centre, a centre for the treatment of patients with dementia and cognitive disorders (Alzheimer's and other types of dementia), with the capacity for 40 people. Teaching is an important activity developed in the Hospital, accredited for postgraduate teaching by the National Council of Medical Specialties. At FPHAG works 1956 people.

Research and innovation at **FPHAG** is growing and expanding: the **institution** aims at increasing the number of research activities and collaborative research projects both at a local, national and European level that involve its health workers. The constant motivation has led the hospital to incorporate into the networks, platforms and regional and national clusters, managers and promoters of research and innovation in health and medical technologies such as REGIC (Network of Managing Entities of Clinic Innovation), XISCAT (Catalan Health Innovation Network), ITEMAS (Platform for Innovation in Medical and Health Technologies) and the Health-Tech Cluster (of the Generalitat of Catalonia). From 2012, the

hospital participates in European projects of technological innovation of the European Programme H2020 and in regional PO FEDER Grants.

FPHAG wants to be a referent in health care, and social health care. Being recognized for its sensitivity to the needs of its patients, the commitment and competence of its professionals and the excellence of its services in an environment of innovation and efficiency all are goals of its principle mission.

FPHAG general Expertise

Pilot Operations and Demonstrations Support and Evaluation:

- Expertise in working in cooperation with end users (elderly users, users associations).
- Recruitment of patients and experience in user profile definition
- Validate solutions generated in a real scenario (home care services and Adolfo Montañá Elder Care)
- Smart Room for research projects and new healthcare services
- Expertise as a pilot in multicentre studies. Demonstrated expertise in participation in clinical trials.
- Experience in designing operational models for Decision-Making and data interoperability.
- Expertise in evaluation data from multidimensional assessment, clinical and technical parameters

MAIN TASKS IN THE PROJECT

FPHAG is lead of WP4 and leads T4.1 and T4.3. More than that that, FPHAG contributes to the other WP as expert hospital partner and is involved in all other WPs.

PREVIOUS EXPERIENCE

- I-DONT-FALL Integrated prevention and detection solutions tailored to the population and risk factors associated with falls. CIP-ICT-PSP-2011-5 *(Policy Support Programme for health, ageing well and inclusion)*

- RADIO :Robots in assisted living environments: Unobtrusive, efficient, reliable and modular solutions for independent ageing H2020-PHC-19-2014 *(Personalising Health and Care)*

Regional Projects: Comunitats Ris3Cat PO EU FEDER grants comunitats-ris3cat

- DIALCAT: Diabetes as an accelerator of cognitive impairment and Alzheimer's disease: comprehensive approach and adherence to treatment (TEC-SALUT: Community for a technology applied to health)
- NEXTCARE (Nextcare) Personalized assistance of chronic patients in a digital health market (HEALTHCARE: Community of multidisciplinary solutions for the next health challenges)

SHORT PROFILES OF STAFF MEMBERS

Anna Benavent holds a Master of Science in Telecom engineering. She has worked as a chief in the health and care industry for 18 years. She is currently the Chief Information and organization Officer at fundació Privada Hospital Asil de Granollers (FPHAG). She is responsible for preparation and execution of the Information Systems Plan. She plans budgets for programs and IT projects, purchases and equipment upgrades. She is the chairman of IT related comittees. ***Person in charge of the technological issues. Female.***

Ramon Romeu holds a technical degree in management informatics from Universitat Politècnica de Catalunya. He has worked as a IT programmer for 15 years. He is currently de Head of System Administration of Granollers General Hospital, one of the center's that integrate Fundació Privada Hospital Asil de Granllers (FPHAG). ***Technical profile to develop, follow and control research project solutions and pilot studies. Male.***

Diana Navarro-Llobet holds a Ph. D. in Chemistry from Indiana University, and a Graduate Degree in Chemistry from Universitat de Barcelona. She has worked as a postdoctoral fellow at Imperial College. She has worked as an R&D chemist before turning into research and innovation management. She is

currently the Head of Research and Innovation of Granollers General Hospital, one of the center's that integrate Fundació Privada Hospital Asil de Granollers (FPHAG), the vice-chair of the Clinical Research Ethics Committee and the Chair of the Scientific Committee at FPHAG. She is an evaluator for several Spanish and European research agencies, both for research and innovation and for ethics. She has been acting as Chair of the Ethics Advisory Committee for the H2020 project RADIO (http://radio-project.eu/). ***Person in charge for the proposal (Main organization contact). Female***

Mercè Ratera holds a Ph. D. in Biomedicine from Universitat de Barcelona, a Master Degree in Innovation and Project Management from Universitat La Salle BES, and a Master Degree in Molecular and Cellular Biology from Joseph Fourier University and Institute de Biologie Structurale, France. She worked as team leader and project manager in an SME. Currently, she works in the Research and Innovation Area at FPHAG, as innovation and collaborative research manager. ***Person in charge for technical innovation and project management issues. Female.***

COOSS MARCHE ONLUS RESEARCH & TRAINING DEPARTMENT		**Number**	**5**
SHORT NAME	**COOSS**		
TYPE	**NGO**		
COUNTRY	**ITALY**		

DESCRIPTION OF THE ORGANISATION

COOSS is a no-profit organization providing social services to disadvantaged people all over the Marche Region. Born in 1979, it counts nowadays more than 2700 employees. COOSS manages a great number of structures: residential settings, daily centres, family-like communities, protected homes mainly for elderly and disabled people. Some of them are managed on behalf of the Local bodies, while others are COOSS property. COOSS also provides territorial and home services, as home assistance to elderly and disabled people, educational support to problematic children, both at home and within the schools, labour insertion initiatives for disadvantaged groups of users, first acceptance services for asylum seekers and refugees. Since 1993, COOSS has created its own Department of Research and Training, which was officially recorded as Research Institute by the Italian Ministry of University and Research in 2012. Its main activities consist in the proposal of/participation to EU and National research projects dealing with social issues. COOSS has wide experience in the user needs analysis and in the management of pilots in assistive technologies projects (5th, 6th and 7th FP, AAL, CIP-ICT-PSP), but also in the management of project in more social-based programs (Daphne, LLP..) The Department is also accredited as VET body and specialized in the design and management of training courses to qualify, upgrade and/or specialize social operators. Given the large number of users who experience speech problems, together with the wide experience in European research, COOSS will mainly contribute to the needs analysis, the deployment of pilots and the usability, accessibility and impact assessment.

MAIN TASKS IN THE PROJECT

COOSS is leading WP2, and here T2.1. Also, COOSS is involved in WP5 and leads T5.5. More than that, COOSS is involved in WP6 and contributes to dissemination activities as well as other activities in WP4 and WP5.

PREVIOUS EXPERIENCE

Publications

1. Nursing homes and daily centres for older people
2. Protected homes and daily centres for disabled people
3. Individual home and school services to seriously disabled persons

Projects

CAREGIVERSPRO-MMD (H2020-PHC-25-2015-690211): development of a platform for people with dementia or mild cognitive impairment and their caregivers, incorporating a combination of ICT interventions and services. The platform is aimed to improve the quality of life for people with dementia, to reduce the caregivers' stress and to improve the user-caregiver's relation quality.

ZocAALo (AAL-2014-1-073) – development of a platform for widespread uptake of certified, accessible and easy-to-use AAL mobile apps in Europe, aimed to tackle the challenge of an ageing society.

SHORT PROFILES OF STAFF MEMBERS

Francesca Cesaroni (F): BSc Human Sciences, University of Macerata, post degree qualification for teaching. Since 1994 employed in COOSS Marche, Department of Research and Training, with tasks related to EU projects management and training courses design and coordination. She took part to many EU projects under V/VI/VIIFP, AAL and CIP-ICT-PSP programmes, as responsible for user oriented activities as user needs analysis, pilots management, trials evaluation and ICT usability and accessibility assessment. She has managed many social-oriented projects under Daphne and LLP programmes.
She is author of publications dealing with care and social issues, ageing phenomenon and ICT related solutions, barriers to social inclusion. She acted as Advisory Board Member in two AAL projects (PALETTE-2016; ActiveAdvice-2017)
Loredana Dottori (F): degree in psychiatric and psychosocial rehabilitation, she is highly specialized in socio-educational problems of disabled and autistic users. She is expert in the field of the communication rehabilitation, facilitated communication and Augmentative Alternative Communication. She is responsible for the rehabilitative community "il Cigno" in Ancona, a structure for severe disabled people, and has a long experience as trainer.

ARBEITER-SAMARITER-BUND WIEN GESUNDHEITS- UND SOZIALE DIENSTE GEMEINNÜTZIGE GMBH DEPARTMENT OF HOME CARE SERVICES		**Number**	**6**
SHORT NAME	**SAM**		
TYPE	**SME**		
COUNTRY	**Austria**		

DESCRIPTION OF THE ORGANISATION

Our main business is providing home care to currently about 900 older adults in living on their own in the city of Vienna. In order to maintain and enhance the quality of our services, we keep in touch with scientific and technological research and innovation and participate in regional, national and international research and best practice projects.

We foster the professional development of our staff by the means of basic and continuous education in those areas. We provide education in thematic fields related to nursing, health care, home care and first aid. Number of persons working at the SAM: 267.

MAIN TASKS IN THE PROJECT

SAM is an expert partner and contributes mainly to dissemination activities in WP6 and to WP5 which is about the toolkits development and training initiatives.

PREVIOUS EXPERIENCE

Relevant previous projects or activities:

1) In the EU-project "FEARLESS" (Fear Elimination as a Resolution for Loosing Elderlys' Substantial Sorrows), an automatic fall alarm system was designed. This system was developed on basis of a user requirement analysis and of following test pilots for the first and second prototype of the system. We contributed to this process by the means of recruiting and assisting the interviewees and test persons among our clients, as well as of taking part in the evaluation, the dissemination and in the creation of a business plan.
2) In the EU-project "FEARLESS" (Fear Elimination as a Resolution for Loosing Elderlys' Substantial Sorrows), an automatic fall alarm system was designed. This system was developed on basis of a user requirement analysis and of following test pilots for the first and second prototype of the system. We contributed to this process by the means of recruiting and assisting the interviewees and test persons among our clients, as well as of taking part in the evaluation, the dissemination and in the creation of a business plan.
3) In the still ongoing EU-project "Enter Train" (Entertainment by Training on a Personalized Exergame Platform), we acted as workpackage leader in WP 1, the user needs analysis, and will support the test pilots and further tasks of the project.

SHORT PROFILES OF STAFF MEMBERS

Mag.[a] **Petra Hellmich** (female) MA is head of department at Samaritan Vienna's department of home care. Her professional experience comprises, amongst others, project management, quality and risk management. Her academic career includes studies of nursing sciences and gerontology (Master's degree), continuous education to various topics of medical and social sciences, and activities as academic lecturer.

Hermine Freitag (female) is head of home care and visiting services, and sheltered housing at Samaritan Vienna's department of home care. After graduating and working as medical nurse at hospitals and at a laboratory, she assumed manifold responsibilities at Samaritan Vienna's, including management, educational and project activities.

Dr.[in] **Sigrid Panovsky** (female) works as secretary and project management assistant at Samaritan Vienna's department of home care. Graduated in sports sciences, the focus of her theoretical and practical experiences lies in health promotion in various settings.

JOHANNITER EUROPE		Number	7
SHORT NAME	JOIN		
TYPE	Non-Profit Organisation		
COUNTRY	Belgium		

DESCRIPTION OF THE ORGANISATION

Johanniter International is an umbrella organisation for 14 countries that follow the mission of supporting people. By this, JOHANNITER INTERNATIONAL (JOIN) is working with experts from the field to find solutions and exchanges on larger scale. JOIN work closely with the European Comission and other international organizations as well. The main purpose of JOIN is to exchange informations and strategies of large health care providers in Europe and to support each other with lessons learned and expertise for new fields.

MAIN TASKS IN THE PROJECT

JOIN is leading WP5 about the training initiatives in hospitals and also T5.1 and T5.4. In WP3, JOIN is leading T3.2 about the stakeholder identification. Moreover, JOIN is contributing to WP6 and all ongoing dissemination activities.

PREVIOUS EXPERIENCE

Publications

Aumayr, Georg (2016): From Ambient Assisted Living to Active and Assisted Living: A practical perspective on experiences and approaches. ITIB-2016: Information Technologies and Biomedicine (in print). Kamien Slaska, Poland:
Aumayr, G. (2015). Health Data Processing - System Theory Based Meaning and Potential for Future Health. IDIMT-2015: Information Technology and Society Interaction and Interdependence (pp. 423-430). Podebrady, Czech Republic: Trauner Verlag.
Aumayr, G. (2014). Fallprevention as Social business Model. Presentation at: iStoppFalls Symposium, 24.10.2014-25.10.2014, Köln
Aumayr, G., & Hofer, K. (2011): Behavior Pattern Recognition – Daten für die Pflege. Österreichische Pflegezeitschrift, 64(11), 12-14.

Projects

International Mission for medical support in Africa

St. John Eye Hospital in Jerusalem

SOCIAL CARE Project (AAL JP)

SHORT PROFILES OF STAFF MEMBERS

Joachim Berney (male) is General Manager and holds a Master Degree in political science. He was responsible for the administrative issues and dissemination activities of the SOCIAL CARE Project and has profound business experience from agricultural entrepreneurship in Nicaragua. Joachim Berney speaks multiple languages fluently and is rooted in many networks across Europe.

Georg Aumayr (male) is research officer and holds a Master Degree in Communication science. He was responsible for the scientific parts and dissemination activities of the SOCIAL CARE project. Furthermore he is head of R&D for Johanniter in Austria and worked on several national and European projects. He has strong ties to the health care services and hospital providers across Europe.

EUROPEAN ASSOCIATION FOR DIRECTORS AND PROVIDERS OF LONG-TERM CARE SERVICES FOR THE ELDERLY (E.D.E.) ABSL.		Number	8
SHORT NAME	EDE		
TYPE	Non-Profit Organisation		
COUNTRY	CZECH REPUBLIC		

DESCRIPTION OF THE ORGANISATION

European Connected Health Alliance (ECHAlliance) is the trusted connector, facilitating multi-stakeholder connections around ecosystems, driving sustainable change and disruption in the delivery of health and social care. Our community gathers 350+ member organisations and 16,500+ experts: governments, health & social care providers, leading companies and start-ups, researchers, insurances, patients and citizens, investors... through ecosystems meetings (100+ per year), international events (such as Mobile World Congress) and our online platform "Connector".

The Alliance is active in 25+ regions/countries (Europe, USA, Canada, China), the ECHAlliance members develop innovative solutions around mobile Health, chronic diseases, active & healthy ageing, Internet of Things, wearables, personalised medicine, genomics, Big Data, etc.

ECHAlliance has for over 6 years a large community of 16500+ people across the Europe, North America (USA,Canada) and China. It owns am associated qualified contact database that allow large communication and dissemination of innovative ideas, projects and solutions. This community is supported by an online platform "Connector" bringing together functionalities for professional social networking (each member has a profile and profiles can communicate together, exchange documents...) publications and share files, emailing and newsletters, collaborative work tools in secured project areas, calendar and alerts, business intelligence tool, built-in communication tools (in-mail and video conference).

ECHAlliance has a long experience of event organisation, with regional events (ecosystems) and international ones (Digital Health & Wellness Summit @ Mobile World Congress Barcelona & Shanghai, eHealth week with the European Commission, EU-US eHealth marketplace...). Events propose, additionally to conferences and keynote addresses, some B2B matchmaking sessions allowing direct contacts and discussions between participants and facilitated by our Connector web platform.

MAIN TASKS IN THE PROJECT

ECH is leading WP2, T2.2 and mainly involved in WP6. ECHAlliance will be the lead on Dissemination and reflecting their experience and credibility as the Global Connector. ECHAlliance will lead all the efforts within the Dissemination and Communication Work Package with their experience of hosting similar events in the targeted countries as well as lead the Exploitation Work Packages

PREVIOUS EXPERIENCE

Publications:

ECHAlliance Methodology: Creating a Connected Health Ecosystem (last version 2015)

The ECHAlliance International Network of Permanent Connected Health Ecosystems is expanding very quickly due to the high demand from those wishing to b break the silos and develop lasting collaborations to create better patient care, at lower costs and creating economic growth. Recognising the challenges that establishing an Ecosystem can pose, we have responded by developing an ECHAlliance methodology for creating a Connected Health Ecosystem (internal tool for Ecosystems in the ECHAlliance network only).

Connected Health White Paper (2014) Many people are using a range of terms to describe Connected Health products and services. Recognising the challenges this can pose, we have worked with one of our Foundation Partners, Wragge & Co, to produce a White Paper summarising the various definitions. We hope this will be a helpful reference point for those businesses and organisations working in digital health, eHealth, mHealth, telecare, telehealth and telemedicine. Published February 2014 http://www.echalliance.com/wp-content/uploads/2014/01/Connected-Health-White-Paper.pdf

The Economy & Jobs Initiative Task and Finish Group – Group Recommendations (2013)

The Task and Finish Group, led by ECHAlliance Chair Brian O'Connor, was appointed by Northern Ireland Ministers, Edwin Poots (DHSSPS) and Arlene Foster (DETI), to provide an assessment of the potential opportunities for employment and business development from Health and Social Care through greater innovation and export-led growth.

The group had 90 days to complete its task. It concluded that Health and Social Care should be recognised as having the potential to be a major driver for innovation and economic growth. The recommendations provide a basis for strengthening the important links between Health and the Economy. Published May 2013 http://www.dhsspsni.gov.uk/t_f_final_report.pdf

B2B matchmaking session / "Meet the buyers"

We organise different events including direct B2B meetings between the different stakeholders of the eHealth sector (see above the description of ecosystems). Those matchmaking sessions are short meetings (15 min) allowing the participant to know each other quickly and decide if they can have collaborations. We organised it in Barcelona (Mobile World Congress), Boston (Connected Health Summit), Dublin and Athens (eHealth week/Forum with the EU commission and EU Presidency), in our ecosystems (see the list above).

Previous projects and activities:

- Readi for Health - Regional Digital Agendas for Healthcare (WP Lead): ECHAlliance is responsible for the dissemination work package (funded by European FP7-REGIONS programme). http://www.readiforhealth.eu/
- GET – Global e-Health Transforming Services (WP Lead): ECHAlliance is responsible for the 'GET Global' service, aimed at providing support for mature SMEs who have had success in their initial markets and are ready to access international markets (funded by the European Commission under the 7th Framework Programme). http://www.get-ehealth.eu/
- PULSE - Participatory Urban Living for Sustainable Environments: PULSE will leverage diverse data sources and big data analytics to transform public health from a reactive to a predictive system, and from a system focused on surveillance to an inclusive and collaborative system supporting health equity. Working within five global cities, PULSE will harvest open city data, and data from health systems, urban and remote sensors, personal devices and social media to enable evidence-driven and timely management of public health events and processes. Started Nov 2016
- SEED - Supporting the recognition of the Silver Economy in Europe in the Digital Era: Main objective is to establish a widely recognised European Annual Award Scheme for innovative digital solutions which demonstrate significant impact improving the quality of life of the ageing population. Started Nov 2016.
- Trillium-II: EU/US Cooperation for Global Interoperability in Digital Health / Responding to the EU-US interoperability roadmap call (SCI-HCO-14-2016), to further advance global Electronic Health Record (EHR) interoperability. Trillium-II aims to bridge, harmonize, evaluate and guide existing and emerging patient summary initiatives, leading the way toward one international patient summary standard. Started Dec 2016.

SHORT PROFILES OF STAFF MEMBERS

Mr **Brian O'Connor** (male), Chair. Brian has developed his career as a consultant, manager and/or investor in both private and public companies. He has worked in the UK, the US and lived in Hong Kong for eleven years. He has gained vast experience as a company director in a variety of industries and professions, and has raised significant sums for companies through both private equity structures and stock exchange listings. Through his long established consultancy company, Corporate Direction Ltd, he is currently providing strategic advice to Governments, International organizations and companies on the challenges facing healthcare in general and specifically on the Connected Health opportunity. Brian has founded a number of companies in the healthcare services area in the UK, Ireland and Hong Kong. He therefore has experience of the public and private health care systems in a number of countries and also an understanding of the often difficult balance between delivering care and making profit. He believes that overcoming the cultural and other barriers within healthcare is an interesting if sometimes frustrating challenge, but worthwhile if it leads to better patient care.

Brian is Chair of the European Connected Health Alliance organization, the rapidly expanding not for profit membership organisation. It is creating an International Network of Permanent Connected Health Ecosystems throughout Europe and beyond, to provide sustainable and structured opportunities for industry, academia and health and care providers and payers to meet and provide solutions to specific problems. Brian is a member of the European Commission's eHealth Stakeholder Group and a member of the European Innovation Partnership B3 Action Group on Integrated Care. He also sits on the board of the Scottish Digital Health Institute and the Connected Health and Prosperity Board in Northern Ireland. He is a director and shareholder in Connected Health Ltd, a start-up in Northern Ireland and makes investments in health and non-health companies from time to time

Mr **Andy Bleaden** (male) currently works for the ECHAlliance after a long career at Stockport Council based in the UK and since 2002 has led on securing funding and managing EU programmes with a specialism in Regeneration, Low Carbon and Adult Social Care. The latter is particularly focussed around the development of Telehealth and Telemedicine solutions. His background is within Social Care working in Psychiatric settings with offenders as well as employment work with homeless young people. He has a wealth of experience in developing successful long term European Co-operation Partnerships and has been involved with delivering many NWE Interreg Projects. In addition he is involved in Ambient Assistive Living Programmes, 7th Framework Programmes and ICT PSP programmes. More recently Andy has been working directly with the Commission both as an evaluator for Horizon 2020 and FP7/CIP Programmes as well as the EIT Health KIC and Urban Innovation Actions and an assessor for existing projects as an external expert. He has a wealth of experience in Active and Healthy Ageing and built many successful projects and partnerships across Europe using his skills around funding and networking. Andy will manage the project for ECHAlliance and lead on all project management and links with the EIP-AHA, Coral, Agile Ageing Alliance and the Covenant for Demographic Change

Mr **Julien Venne** (male), Strategic Advisor. Julien is the Strategic Advisor of the European Connected Health Alliance (ECHAlliance). His role is to support companies in their business development in Europe, and policy-makers and public authorities in several European Countries. His expertise covers innovation development, business models design and ecosystem creation within the Connected Health sector.

He has a multi-disciplinary academic background, with economics, sociology, political sciences and complex systemic. He worked by the past for different health and social care providers and drove several projects and eHealth clinical trials about chronic diseases management and active & healthy ageing. He has as well a good experience in the support to start-ups and SMEs in their development, as he managed 2 incubators and created 2 companies. He's fluent French (native language), English and Spanish.

4.2. Third parties involved in the project (including use of third party resources)

SYNYO

Does the participant plan to subcontract certain tasks (please note that core tasks of the project should not be sub-contracted)	N
If yes, please describe and justify the tasks to be subcontracted	
Does the participant envisage that part of its work is performed by linked third parties[1]	N
Does the participant envisage the use of contributions in kind provided by third parties (Articles 11 and 12 of the General Model Grant Agreement)	N

[1] A third party that is an affiliated entity or has a legal link to a participant implying a collaboration not limited to the action. (Article 14 of the Model Grant Agreement).

5. LETTERS OF SUPPORT

LETTER OF SUPPORT

To whom it may concern

Project on Cybersecurity in Healthcare Organisations

On behalf of **European Association for Directors and Providers of Long-Term Care Services for the Elderly (E.D.E.) absl** I confirm that we consider your mentioned project in context of cybersecurity in healthcare organisations as very important contribution to improve the vulnerable situation of critical infrastructures like hospitals and care centres by strengthening the capabilities as highly important. We agree that the outlined project approach of improving the cybersecurity in the whole lifecycle as well as the definition of innovative cybersecurity measures in order to tackle cybersecurity challenges such as for privacy/data/infrastructures of utmost importance to operationalise a safe and highly efficient innovative healthcare ecosystem.

In case your Horizon 2020 project is getting funded, we will be pleased to offer our expertise during the project by joining surveys, providing feedback, and validating results. We will receive continuous information on the project outcomes and expert and advisory activities. In context of addressing cybersecurity challenges in healthcare organisations we are especially interested on the following measures and instruments :

- ☒ Awareness Raising & Empowerment
- ☒ Handbooks & Guidelines
- ☒ Trainings & Workshops
- ☒ Best Practices & Case Studies
- ☒ Risk Assessment & Checklists
- ☒ Smart Advice & Decision Support
- ☒ Technical Approaches & Solutions

Dipl.ing. Jiri Horecky, Ph.D., MBA
President of E.D.E.

Jiří Horecký - EDE president
E.D.E. asbl
c/o Résidence Grande Duchesse Joséphine Charlotte
11, avenue Marie-Thérèse
L-2132 Luxembourg
president@ede-eu.org

Dedalus
HEALTHCARE SYSTEMS GROUP

LETTER OF SUPPORT

To whom it may concern

Project on Cybersecurity in Healthcare Organisations

On behalf of Dedalus S.p.A., I confirm that we consider your mentioned project in context of cybersecurity in healthcare organisations as very important contribution to improve the vulnerable situation of critical infrastructures like hospitals and care centres by strengthening the capabilities as highly important. We agree that the outlined project approach of improving the cybersecurity in the whole lifecycle as well as the definition of innovative cybersecurity measures in order to tackle cybersecurity challenges such as for privacy/data/infrastructures of utmost importance to operationalise a safe and highly efficient innovative healthcare ecosystem.

In case your Horizon 2020 project is getting funded, we will be pleased to offer our expertise during the project by joining surveys, and providing feedback. We will receive continuous information on the project outcomes and expert and advisory activities. In context of addressing cybersecurity challenges in healthcare organisations we are especially interested on the following measures and instruments [please select, also multiple if relevant]:

- ☒ Awareness Raising & Empowerment
- ☒ Handbooks & Guidelines
- ☒ Trainings & Workshops
- ☒ Best Practices & Case Studies
- ☒ Risk Assessment & Checklists
- ☐ Smart Advice & Decision Support
- ☐ Technical Approaches & Solutions

23/04/2018

Name of contact Person: Camilli Gianpiero
Organisation/Institution: Dedalus S.p.A.
Address: via Gobetti n 52
City, Country: Bologna, Italy
E-Mail: Gianpiero.camilli@dedalus.eu
Phone: +390514193911

CYLON

LETTER OF SUPPORT

To whom it may concern

Project on Cybersecurity in Healthcare Organisations

On behalf of Cyber London Ltd (CyLon), I confirm that we consider your mentioned project in context of cyber security in healthcare organisations as very important contribution to improve the vulnerable situation of critical infrastructures like hospitals and care centres by strengthening the capabilities as highly important. We agree that the outlined project approach of improving cyber security in the whole lifecycle as well as the definition of innovative cyber security measures in order to tackle the security challenges such as privacy/data/infrastructures of utmost importance to operationalise a safe and highly efficient innovative healthcare ecosystem.

If your Horizon 2020 project receives funding, we will be pleased to offer our expertise during the project by joining surveys and providing feedback. We will receive continuous information on the project outcomes and expert and advisory activities. In context of addressing cyber security challenges in healthcare organisations we are especially interested on the following measures and instruments:

- ☐ Awareness Raising & Empowerment
- ☐ Handbooks & Guidelines
- ☐ Trainings & Workshops
- ☐ Best Practices & Case Studies
- ☐ Risk Assessment & Checklists
- ☐ Smart Advice & Decision Support
- ☐ Technical Approaches & Solutions

Kirsten Connell
Managing Director
Cyber London Ltd
27 Hammersmith Grove
London
kirsten@cylonlab.com
07765999473

Erle Robotics

LETTER OF SUPPORT

To whom it may concern

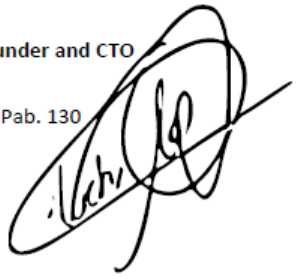
Project on Cybersecurity in Healthcare Organisations

On behalf of Erle Robotics S.L. I confirm that we consider your mentioned project in context of cybersecurity in healthcare organisations as very important contribution to improve the vulnerable situation of critical infrastructures like hospitals and care centres by strengthening the capabilities as highly important. We agree that the outlined project approach of improving the cybersecurity in the whole lifecycle as well as the definition of innovative cybersecurity measures for robots in order to tackle cybersecurity challenges such as for privacy/data/infrastructures of utmost importance to operationalise a safe and highly efficient innovative healthcare ecosystem.

In case your Horizon 2020 project is getting funded, we will be pleased to offer our expertise during the project by joining surveys, providing feedback, and validating results. We will receive continuous information on the project outcomes and expert and advisory activities. In context of addressing cybersecurity challenges in healthcare organisations we are especially interested on the following measures and instruments:

- ☐ Awareness Raising & Empowerment
- ☐ Handbooks & Guidelines
- ☐ Trainings & Workshops
- x Best Practices & Case Studies
- ☐ Risk Assessment & Checklists
- ☐ Smart Advice & Decision Support
- x Technical Approaches & Solutions

Víctor Mayoral Vilches - **Founder and CTO**
Erle Robotics S.L.
Calle Venta de la Estrella 6, Pab. 130
Vitoria, Spain
victor@erlerobotics.com
0034 616151561



6. ETHICS AND SECURITY

6.1 Ethics

The SecureHospitals.eu consortium confirms that the relevant EU legislation, international and national texts will be taken into consideration in WP2 where the team is planning to engage the relevant parties in providing their views on gender in research. As the solution to be developed are stakeholders specific the project team will hold in high regards the contributions of all participants in the consequent surveys and activities connected to data gathering. In this particular case data will be mostly textual and contextual, while ultimately also aggregated data will be used to improve certain features of the platform. An initial survey has identified the following.

The Charter of Fundamental Rights of the EU

The Charter of Fundamental Rights in the course of the respective legal trend dedicates a separate article to the protection of personal data. Article 8 sets out the right to the protection of personal data of an individual and thus the protection of personal data has now its own legal basis apart from the right to respect an individual's private life and the protection of human dignity. Article 8 of the Charter sets out the rules for the legitimate processing of personal data, notably that the processing shall be fair and for pre-specified purposes based on the consent of the data subject or other legitimate basis laid down by law. Reference is furthermore made to two rights of the data subject: the right of access to the data and the right to have it rectified. Finally, Article 8 sets out the need for an independent authority, which shall control the compliance with the data protection rules.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data lays down a series of rights of the data subject. These are:

• The right of access to own personal data.

• The rights of erasure, blocking or rectification of the data, which do not comply with the provisions of the Directive, are incomplete or inaccurate.

• The right to be informed of all relevant details relating to the data processing and the rights granted to self.

• The right to a judicial remedy for any breach of the above-mentioned rights.

All these are applicable to SecureHospitals.eu. The first three aforementioned rights may be restricted if this is necessary for reasons relating to the protection of the data subject or the rights and freedoms of others or to prevent a criminal offence or for reasons relating to public security.

Informed Consent

Informed consent is the process by which a participant will be fully informed about the research in which they are going to participate. It originates from the legal and ethical right the participant has to direct what happens to their personal data and from the ethical duty of the investigator to involve the participant in research. Seeking the consent of an individual to participate in research reflects the right of an individual to self-determination and also their fundamental right to be free from bodily interference whether physical or psychological and to protect their personal data.

The written information as well as the sought informed consent corresponds to information gathered from the revised version of the Helsinki Declaration of 1964, as lastly amended in Tokyo, 2004, and the Convention of the Council of Europe on Human Rights and Biomedicine (1997).

Basic elements of informed consent

• In order to involve a human being as a participant in research, the investigator will obtain the legally effective informed consent of the participant or the participant's legally authorized representative.

• All investigators within SecureHospitals.eu will seek such consent only under circumstances that provide the prospective participant or the representative sufficient opportunity to consider whether or not to participate and that minimize the possibility of coercion or undue influence.

• The information given to the participant or the representative will be in language understandable to the participant or the representative.

• No informed consent, whether oral or written, may include any exculpatory language through which the participant or the representative is made to waive or appear to waive any of the participant's legal rights, or releases or appears to release the investigator, the sponsor, the institution or its agents from liability for negligence.

Procedures for protecting the confidentiality of personal data

The protection of the privacy of participants is a responsibility of all people involved in research with human participants. Privacy means that the participant can control the access to personal information; they decide who has access to the collected data in the future. Due to the principle of autonomy the participants have to be asked for their agreement (informed consent) before private information can be collected.

It should be also ensured that all the persons involved in research work understand and respect the requirement for confidentiality. The participants should be informed about the confidentiality policy that is used in the research.

The privacy plays a role at different levels:

• Hints to or specific personal information of any participant in publications.

• It should be prevented to reveal the identity of participants in research deliberately or inadvertently, without the expressed permission of the participants.

• Dissemination of data among partners.

• Access to data, method of access, data formats, method of archiving (electronic and paper), including data handling, data analyses, and research communications. Offer restricted access to privacy sensitive information within the organization of the partner.

• Protection of the privacy within the organization of volunteers (employers, etc.) throughout the whole process in various aspects, such as communications, data exchange, presentation of findings, etc.

Adequate security measures for storage and handling of such data

SecureHospitals.eu will use state-of-the-art technologies for secure storage, delivery and access of personal information, as well as managing the rights of the users. In this way, there is complete guarantee that the accessed, delivered, stored and transmitted content will be managed by the right persons, with well-defined rights, at the right time.

Security enforcement within the project

In this section we will describe the data protection measures for information used by researchers during research. Data will be collected at different research sites with surveys and experiments. The collected data will be stored in a secure server, only visible to the research site network, in a locked room at each of the research locations. Anonymous and identity data will be stored separately, and only the project leader

will have access to all the users' identities. Anonymity will be granted by separating identifiable data from anonymous data. Each user will be granted a unique identifier that will link one to the other, but only anonymous data will be available to researchers. If any identifiable data is required, access to it will be granted only after explicit user permission and after agreement of the Executive Board.

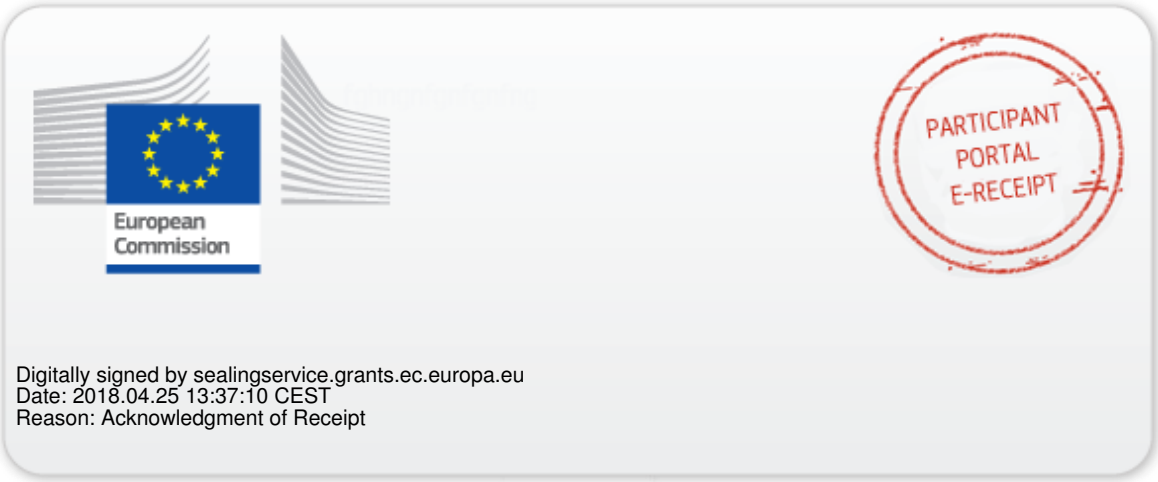
6.2 Security[2]

Please indicate if your project will involve:

- activities or results raising security issues: (NO)
- 'EU-classified information' as background or results: (NO)

The project does not involve any activities or results raising security issues. Therefore, the naming of special security staff, a project security officer, and a security advisory board are not needed.

[2] Article 37.1 of the Model Grant Agreement: *Before disclosing results of activities raising security issues to a third party (including affiliated entities), a beneficiary must inform the coordinator — which must request written approval from the Commission/Agency.* Article 37.2: *Activities related to 'classified deliverables' must comply with the 'security requirements' until they are declassified. Action tasks related to classified deliverables may not be subcontracted without prior explicit written approval from the Commission/Agency. The beneficiaries must inform the coordinator — which must immediately inform the Commission/Agency — of any changes in the security context and — if necessary —request for Annex 1 to be amended (see Article 55*



This electronic receipt is a digitally signed version of the document submitted by your organisation. Both the content of the document and a set of metadata have been digitally sealed.

This digital signature mechanism, using a public-private key pair mechanism, uniquely binds this eReceipt to the modules of the Participant Portal of the European Commission, to the transaction for which it was generated and ensures its full integrity. Therefore a complete digitally signed trail of the transaction is available both for your organisation and for the issuer of the eReceipt.

Any attempt to modify the content will lead to a break of the integrity of the electronic signature, which can be verified at any time by clicking on the eReceipt validation symbol.

More info about eReceipts can be found in the FAQ page of the Participant Portal. (http://ec.europa.eu/research/participants/portal/page/faq)