



SECUREHOSPITALS.EU 

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

D6.1 Project website, social media accounts and communication channels



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

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

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

Coordinator: INTERSPREAD GmbH

Reference: 826497

Type: CSA

Program: HORIZON 2020

Theme: eHealth, Cybersecurity

Start: 01. December, 2018

Duration: 26 months

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

E-Mail: office@securehospitals.eu

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

DELIVERABLE DESCRIPTION

Number:	D6.1
Title:	Project website, social media accounts and communication channels
Lead beneficiary:	INSP
Work package:	WP6
Dissemination level:	Public (PU)
Type	Other (O)
Due date:	28.02.2019
Submission date:	28.02.2019
Authors:	Stela Shiroka, INSP
Contributors:	Dietmar Vicuinik, INSP
Reviewers:	Sigrid Panovsky, SAM

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

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

TABLE OF CONTENT

1.	Introduction.....	7
2.	Project Website	8
2.1.	Structure	8
2.2.	Outline of the content	9
2.2.1.	Section 'PROJECT INFO'	10
2.2.2.	Section 'TEAM'	14
2.2.3.	Section 'MEDIA'	15
2.2.4.	Section 'CONTACT'	16
2.3.	Search Engine Optimiser	16
2.4.	Google Analytics.....	16
3.	Social Media Channels.....	17
4.	Conclusion	19

EXECUTIVE SUMMARY

This report presents information on the main digital resources and channels that are implemented as part of the SecureHospitals.eu project. First, the structure of the project website and its content are explained. Illustrated by selected screenshots, the design, functions, and content of the website and each of its sections are highlighted. Secondly, the report includes information about social media channels which are set up as main tools for distribution and dissemination. The Twitter and Facebook accounts have already been launched. Other social media accounts (e.g. LinkedIn, YouTube) will be set up later on, depending on emerging needs for stakeholder mobilisation through different channels. The project website will be regularly updated and possibly include further sections at a later stage. The presented outline and content thus, represents only the first version of the project website.

TABLE OF FIGURES

<i>FIGURE 1: Project Website Structure</i>	8
<i>FIGURE 2: Homepage</i>	9
<i>FIGURE 3: Project Info</i>	10
<i>FIGURE 4: Project Methodology</i>	11
<i>FIGURE 5: Project Structure</i>	12
<i>FIGURE 6: Deliverables</i>	13
<i>FIGURE 7: Consortium</i>	14
<i>FIGURE 8: Experts and Advisory Board</i>	15
<i>FIGURE 9: Media</i>	15
<i>FIGURE 10: Newsletter</i>	16
<i>FIGURE 11: Twitter Channel</i>	17
<i>FIGURE 12: Facebook channel</i>	18

1. Introduction

This additional report provides information on the project website and further digital resources and channels, which were implemented for dissemination and communication activities of the SecureHospitals.eu project. The document starts by explaining the structure of the project website and highlighting its content. Some selected screenshots illustrate the design, the functions and the sections and subsections of the site. Furthermore, SEO (search engine optimiser) and Google Analytics information are briefly explained. The report also documents the social media channels, which were set up as a central distribution and dissemination tool. Finally, we would like to remark that the website will be regularly updated. Thus, it represents the first step of our communication and dissemination activities. In the future, further social media channels (e.g. Facebook, YouTube, LinkedIn) may be created, following the advance of the project results and need for reaching to large audiences of stakeholders.

2. Project Website

The project website can be accessed through <https://project.securehospitals.eu/>.

2.1. Structure

The structure of the SecureHospitals.eu website is illustrated in the graph below. In the following, each subsection will be described in more details.

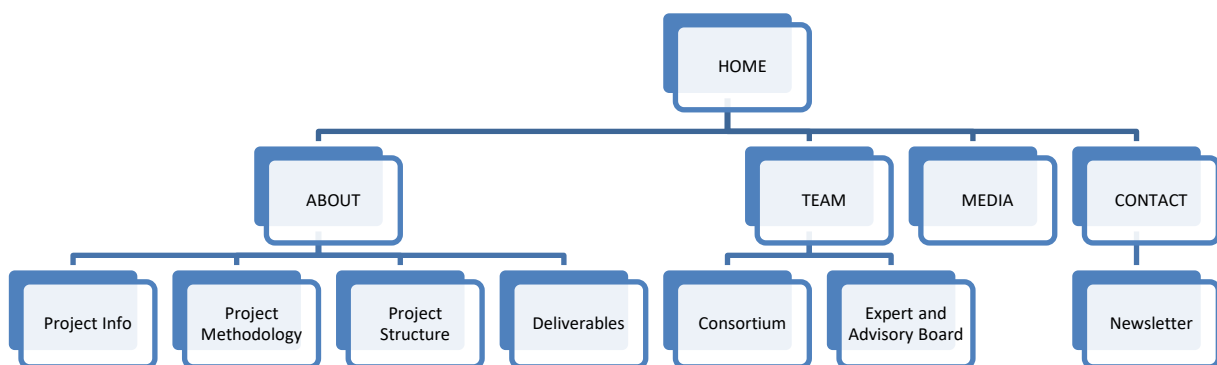


FIGURE 1: Project Website Structure

Figure 1 shows the high-level sitemap of the website. The main menu includes the most frequently required links like shortcuts to the Home page, About page with subpages such as: Project Info, Project Methodology, Work Packages and Deliverables, Team with two subpages on the consortium and the Expert and Advisory Board, Media with one subpage on the newsletter and the last Contact Page. The main menu items will be sublevelled into pages which give another context to these items.

The sitemap is also created as XML Sitemap and connected to SEO (Search Engine Optimizer) for better indexing and searching on search engines like Google, Bing, Yahoo and more.

2.2. Outline of the content

The front page (“Home”) highlights the main facts in brief and provides information on the project and its main activities. It also highlights the overall vision and the expected impacts of the action.

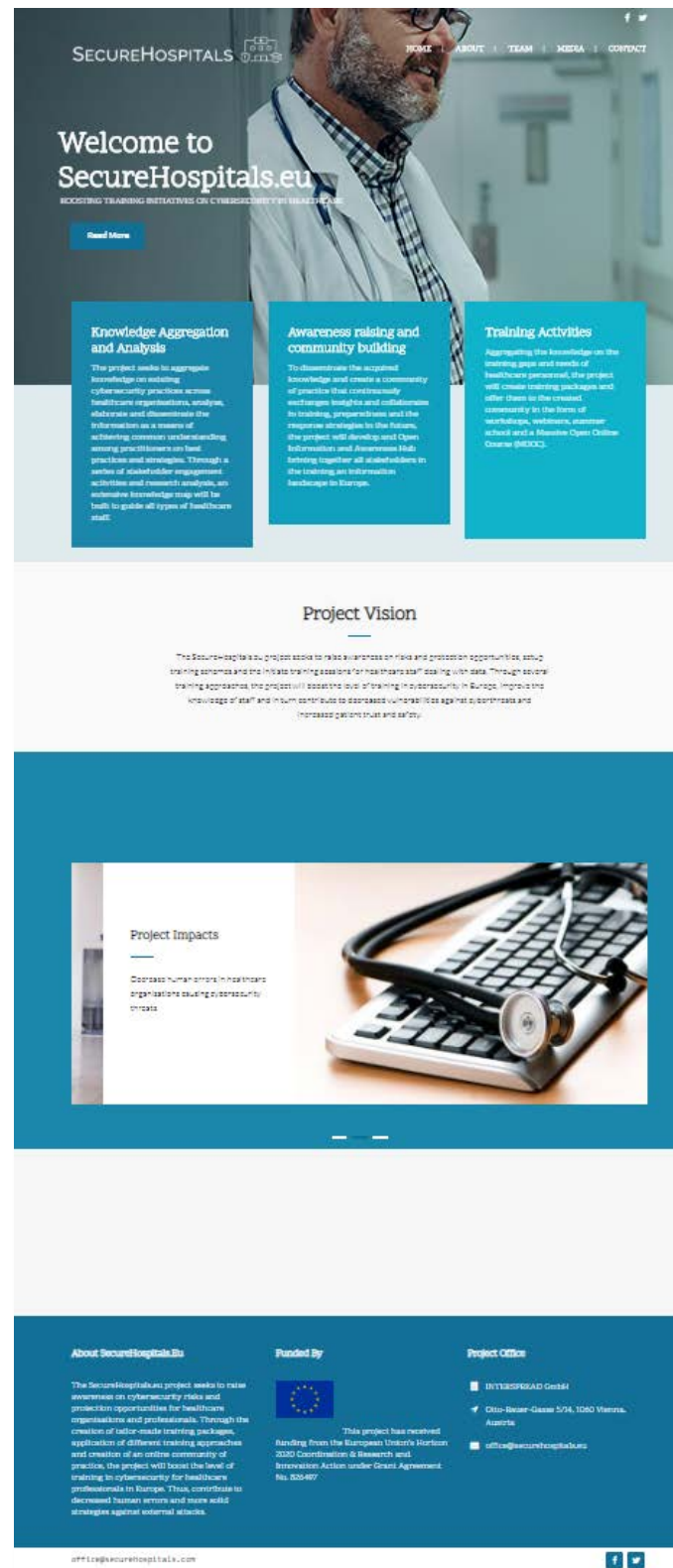


FIGURE 2: Homepage

This section describes all project detail including the call it responded to, reference to EU funding, duration, type, official title etc. It further shows the official project abstract, the objectives, the concept graph showing the overall project methodology as well as the work packages and deliverables. All public reports will be uploaded in the deliverable sections upon submission date.



[HOME](#)
[ABOUT](#)
[TEAM](#)
[MEDIA](#)
[CONTACT](#)

Project Info



Project Details

Acronym	SecuroHospitals.eu
Title	Enabling Healthcare and Cybersecurity in Hospitals across Europe and Boosting Training British and German by an Online Information Hub
Duration	30 Months
GA Number	834397
Topic ID	800000-023-EN-0175-0006-0
Call	Enabling healthcare and developing training schemes in cybersecurity in hospitals
Funding Scheme	800000
Project Type	COA, Development and Support, Audit

Project Background



Cybersecurity has recently emerged from protecting big corporations in other industries, like financial services as well as the traditional sector. Especially in the last years the need is rising, where factors are keeping sectors leads, devices that are connected to the Internet. Most cases include raising patient autonomy and managing it for remote therapy. The big problem is cybersecurity, not applicable or device. But even in the healthcare landscape a possible entry point for a cyber attack. So far most factors instead of an attack with response is a primary goal from existing patient records or releasing information. But, capabilities would also be able to handle any medical device in our system, for details. Complete cybersecurity in the health sector is unmanageable, and instead, several digital health technologies, that focus on the patient to increase the risk of cyber-attacks against healthcare facilities, around 80 percent of reported cyber-attacks would be prevented if basic protection protocols would be installed. The SecuroHospitals project seeks to build awareness in media and personnel organizations, using training schemes and the online training modules for IT staff working in hospitals. Through several training approaches, the project will boost the level of training in cybersecurity in Europe, enhance the knowledge of staff and to turn countries into more cyber-secure against cyber threats and increased patient trust and safety.

Objectives



Build awareness among decision makers and IT practitioners in hospitals and care centres across Europe in the importance of cybersecurity and continuous training of all affected staff.

Open Information And Awareness Hub



The online space created for the SecuroHospitals.eu community of practice will bring together healthcare professionals, IT and cybersecurity experts, trainers, training organisations, decision makers at different levels, researchers, and solution providers with the aim of sharing information, materials and practices and growing strategic together.

Training Activities

During the course of projects, a minimum of 10 webinars and workshops all over Europe will be carried out for raising awareness on security practices and strategies on cybersecurity. A webinar platform and a Massive Open Online Course will enable practitioners to deepen their knowledge and build on their skills through their organisations.



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

Project Methodology

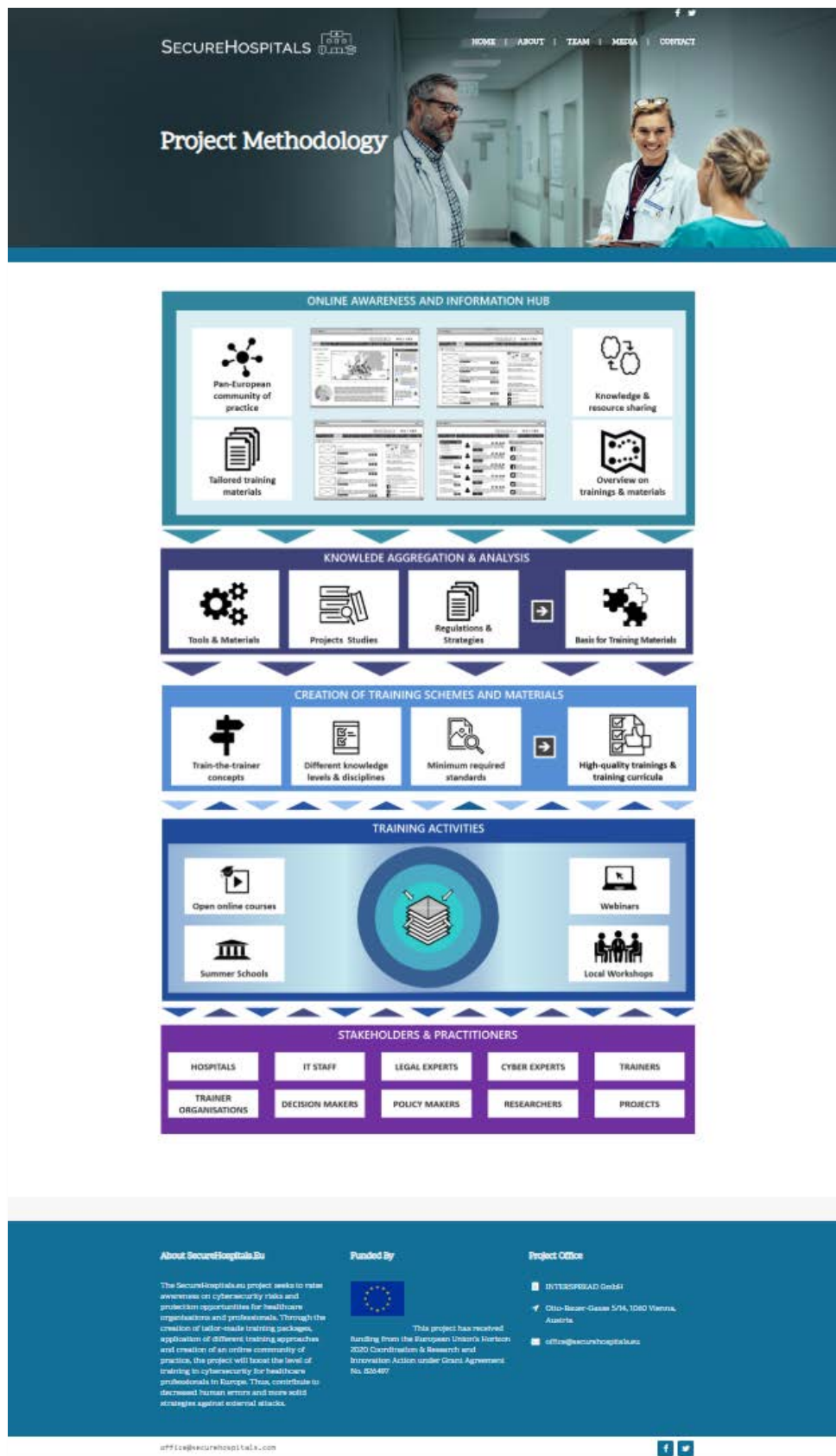



FIGURE 4: Project Methodology

Project Structure



FIGURE 5: Project Structure

Deliverables

SecureHospitals  [HOME](#) [ABOUT](#) [TEAM](#) [MEDIA](#) [CONTACT](#)


Deliverables

Number	Deliverable name	Link
D0.1	Kick-off meeting report	View Download
D0.2	Data Management Plan	View Download
D0.3	Status report	View Download
D0.4	First project documentation	View Download
D1.1	Stakeholder involvement roadmap and engagement activities	View Download
D1.2	Current participants and interests on cybersecurity in hospitals	View Download
D1.3	Online Awareness and Information Hub: www.securehospitals.eu	View Download
D1.4	Relevant cybersecurity processes and business overview	View Download
D2.1	Cybersecurity in hospitals Knowledge Map	View Download
D2.2	European, project and stakeholders on cybersecurity in hospitals report	View Download
D2.3	State-of-the-art and essentials for addressing and Approaches to Cybersecurity in hospitals training report	View Download
D2.4	Cybersecurity in hospitals Knowledge Baseline Report	View Download
D3.1	Cybersecurity in hospitals courses and programmes collection	View Download
D3.2	Trainer resources and workshops report	View Download
D3.3	New cybersecurity in hospitals curricula and materials and quality assurance report	View Download
D3.4	Top-to-ey guide for the development of new course curricula	View Download
D3.5	Training Strategy 1	View Download
D3.6	Presentational materials and registration forms	View Download
D3.7	Training Strategy 2	View Download
D3.8	SecureHospitals MOOC report	View Download
D3.9	Cybersecurity in hospitals Summer School report	View Download
D3.10	Workshops and final training report	View Download
D4.1	Project website, social media accounts and communication channels	View Download
D4.2	Dissemination materials	View Download
D4.3	Dissemination activities report	View Download
D4.4	Publications and presentations overview list	View Download
D4.5	SecureHospitals exploitation plan	View Download
D4.6	Cybersecurity in hospitals Awareness Conference summary report	View Download
D5.1	W- Requirements Eu, T	View Download
D5.2	RCMD – Requirements Eu, T	View Download




About SecureHospitals.eu

The SecureHospitals project seeks to raise awareness on cybersecurity risks and protection opportunities for healthcare organisations and professionals. Through the creation of online media content and apps, application of different training approaches and creation of an online community of practice, the project will boost the level of training in cybersecurity for healthcare professionals in Europe. This contributes to decreased human errors and more solid strategies against external attacks.

Funded By

 This project has received funding from the European Union's Horizon 2020 Coordination & Research and Innovation Action under Grant Agreement No. 1010407

Project Office

 INTERSPREAD GmbH
 Oliver Bauer-Gesetz 5/14, 1080 Vienna, Austria
 office@securehospitals.eu



office@securehospitals.eu  

FIGURE 6: Deliverables

2.2.2. Section 'TEAM' Consortium

This section provides information on the consortium partners of the project. It includes a description of the institutions and their role in the project. Additionally, a simple click on the specific link opens the webpage of the related institution in a new window.

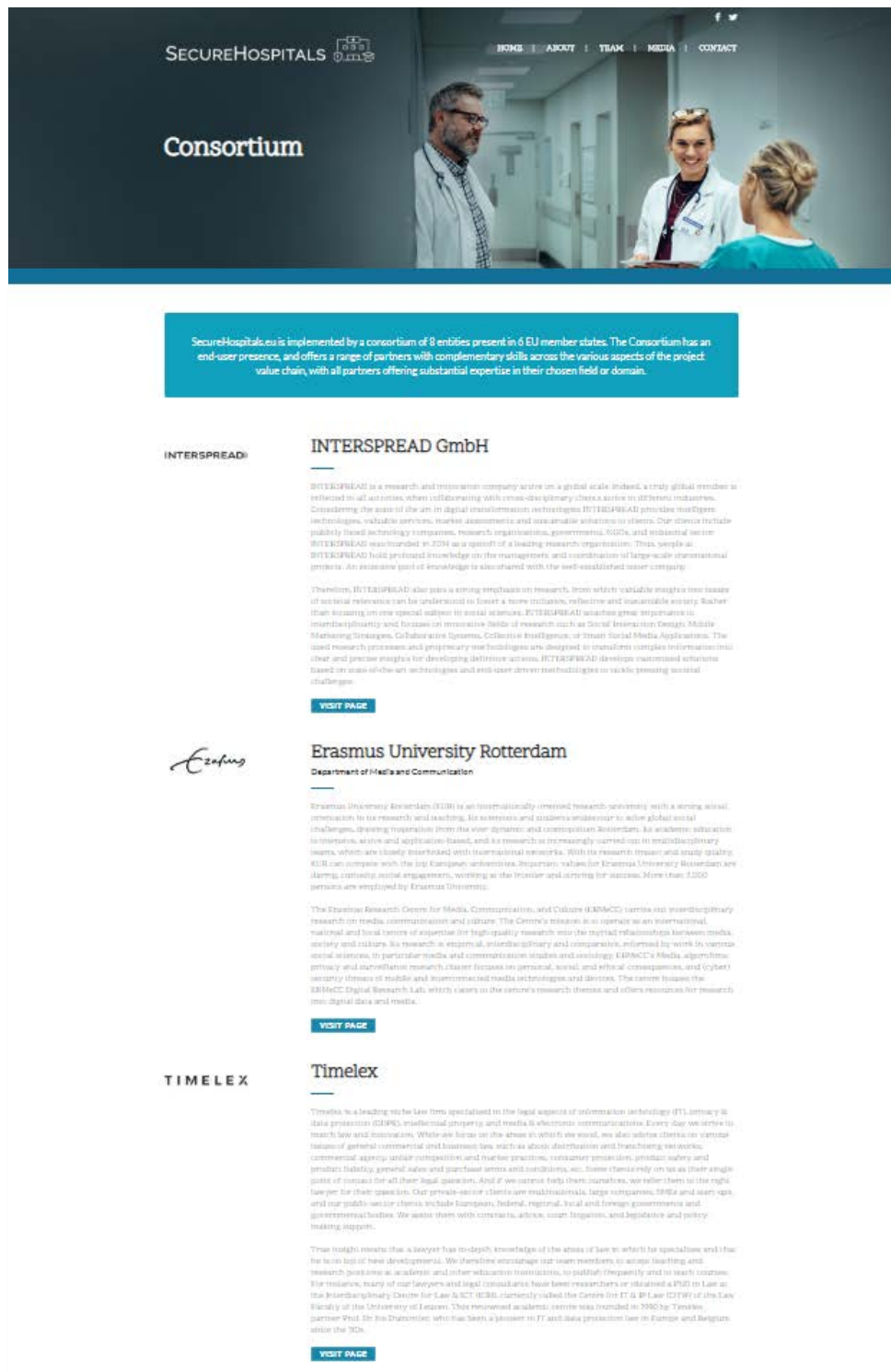


FIGURE 7: Consortium

Expert and Advisory Board

As a supporting team to the consortium, the Expert and Advisory Board is shown here with the list of the names of the experts and a short description of their profiles.

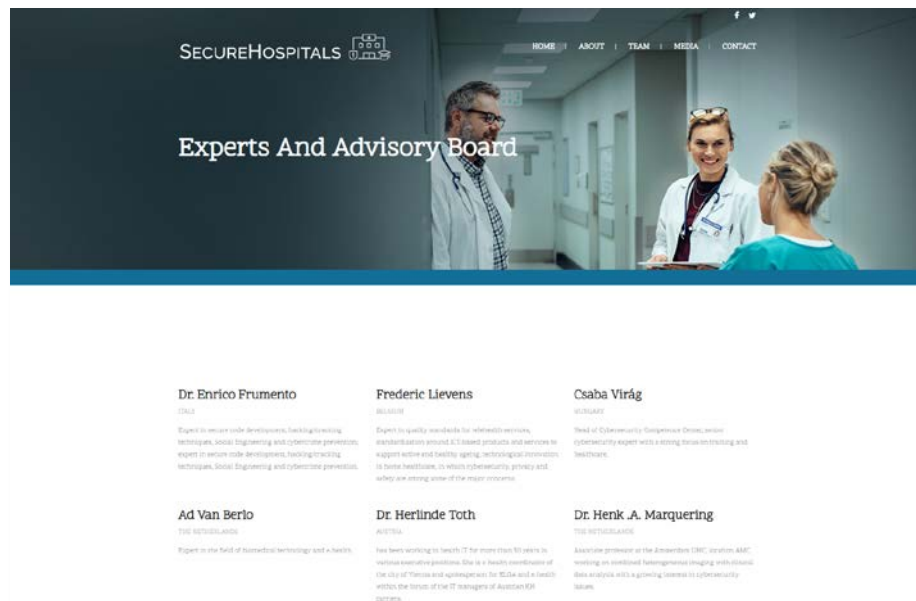


FIGURE 8: Experts and Advisory Board

2.2.3. Section 'MEDIA'

The Media section offers space for listing of dissemination materials (flyers, factsheets etc.) and other promotional materials. Additional content in this section will be added during the course of the project. Moreover, it contains downloadable versions of the project logo and integrated feeds of social media accounts.

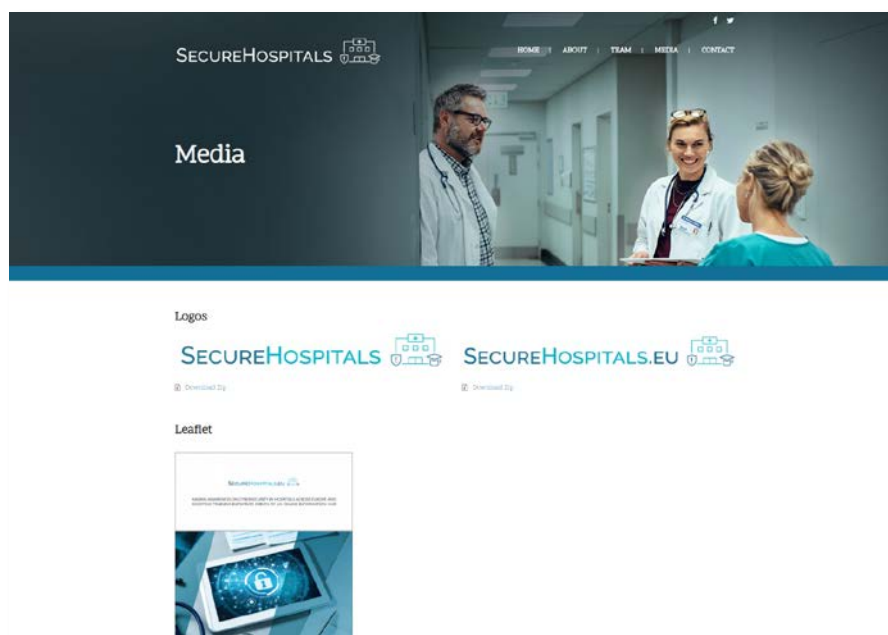


FIGURE 9: Media

2.2.4. Section 'CONTACT'

The section shows the contact details of the coordinator (INTERSPREAD GmbH) of this project. In addition to a web form for getting in touch with the project team, it includes the mailing address of the coordinator. For more information about the project or specific enquiries a single point of access email is provided (office@securehospitals.eu).

Newsletter

The Newsletter subpage provides the opportunity to subscribe and receive all project newsletters. Once circulated, the newsletter links will be published in this space, or in the media space, so that those who missed the information can still access it afterwards.

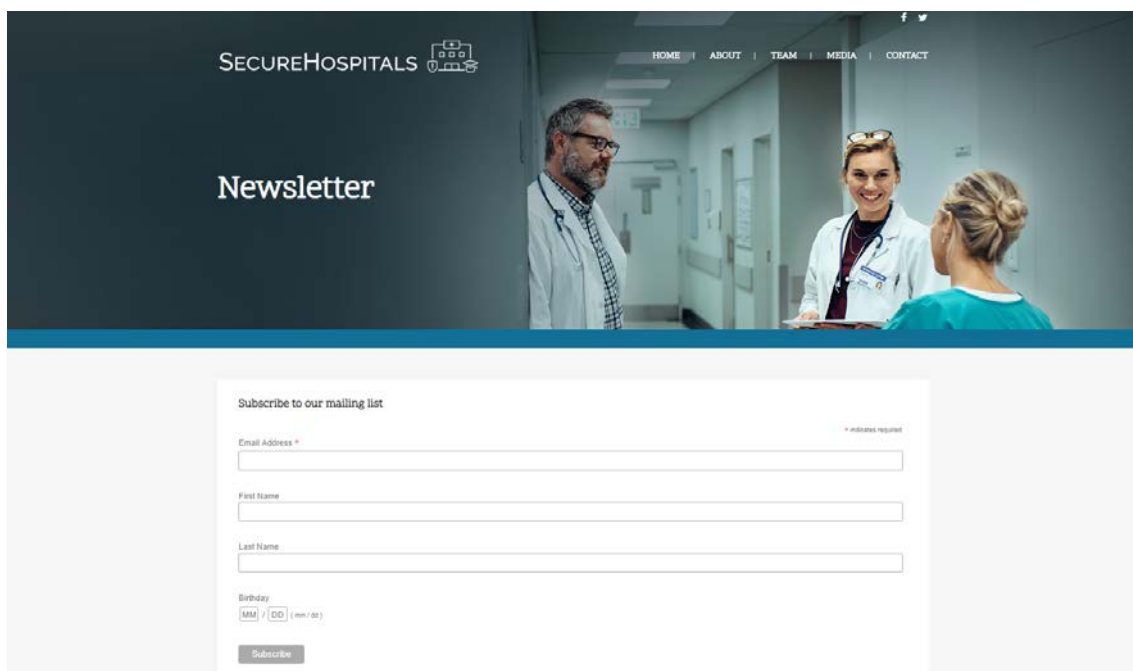
The image is a screenshot of the 'Newsletter' page on the SecureHospitals website. The header features the 'SECUREHOSPITALS' logo and a navigation menu with links for HOME, ABOUT, TEAM, MEDIA, and CONTACT. The main visual is a photograph of three healthcare professionals in a clinical setting. Below the image, the word 'Newsletter' is displayed in a large, white font. The central element is a white subscription form titled 'Subscribe to our mailing list'. It includes input fields for 'Email Address *', 'First Name', and 'Last Name', with a small red asterisk indicating required fields. There is also a 'Birthday' section with dropdown menus for 'MM' and 'DD', and a 'Subscribe' button at the bottom.

FIGURE 10: Newsletter

2.3. Search Engine Optimiser

The website has installed a Search Engine Optimization (SEO), specifically it is the Yoast SEO plugin which will increase the visibility of the site. Yoast SEO (formerly known as WordPress SEO by Yoast) is the most complete WordPress SEO plugin that exists today for WordPress.org users. In addition, the website is connected with Google Webmaster Tools to increase the project index in search engines.

2.4. Google Analytics

The project website is connected also with Google analytics which will help us survey the usage of the site from end users in different dimensions like location, language, device, technology, demographic, browser and more.

3. Social Media Channels

The first project social media channels include a Twitter and a Facebook account. LinkedIn and YouTube will be used at a later stage, when the project has increased the level of outputs delivery and open calls of participants are open.

Twitter

A Twitter account can be accessed at twitter.com/SecureHospitals or [@SecureHospitals](https://twitter.com/SecureHospitals). Considering the popularity of the platform in the professional community, it will serve as an important communication tool through the whole project duration. Project partners and external community members have already started posting and linking to the page and promoting it to their communities.



FIGURE 11: Twitter Channel

Facebook

Additionally, to the Twitter account, another one has been created on Facebook to make use of an additional channel for reaching out to project stakeholders and communication project results to the wider community. Project identity details such as the project logo, short title, description, reference to EU funding etc. have been added to both channels. Also, the content creation for Facebook has been started.



FIGURE 12: Facebook channel

4. Conclusion

This additional report sought to describe the first project communication channels created until month 3. The project website will serve as a fundamental resource and dissemination tool, where researchers, experts, stakeholders, the interested public and potential participants can find the relevant information about the project. The website is object of change as new information will be published or content adapted. In addition to the channels presented in this report, further dissemination channels and activities are planned to be rolled out in the following months.