SECUREHOSPITALS.EU

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

D2.3 Online Awareness and Information Hub www.securehospitals.eu

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

PROJECT DESCRIPTION

Acronym: **SecureHospitals.eu**

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

Coordinator: INTERSPREAD GmbH
Reference: 826497
Type: CSA
Program: HORIZON 2020
Theme: eHealth, Cybersecurity
Start: 01. December, 2018
Duration: 26 months
Website: https://project.securehospitals.eu/
E-Mail: office@securehospitals.eu

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

DELIVERABLE DESCRIPTION

Number:	**D2.3**
Title:	**Online Awareness and Information Hub www.securehospitals.eu**
Lead beneficiary:	**INSP**
Work package:	WP2
Dissemination level:	PU
Type	Other
Due date:	31.07.2019
Submission date:	31.07.2019
Authors:	**Stela Shiroka,** INSP
Contributors:	**Peter Leitner,** INSP **All partners**
Reviewers:	**Peter Leitner**, INSP

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

TABLE OF CONTENT

TABLE OF FIGURES

EXECUTIVE SUMMARY

This deliverable describes the structure and functionalities of the SecureHospitals.eu Open Information and Awareness Hub, detailing the current stage of development the upcoming releases' timeline. Each of the modules has been created in compliance with the Description of Action, while also integrating the feedback acquired and lessons learned during the first project months. The first version of the online hub will be launched in September 2019 for the public. Upcoming versions will enrich it with additional materials and functionalities.

1 Introduction

The initial version of the SecureHospitals.eu online hub goes online for the public via www.securehospitals.eu on 1st September 2019. This first-release is a pre-launch of the platform, mainly containing the structure of the upcoming modules and brief information on the upcoming content.

The development of the online hub will follow these three stages until the full launch:

1. **September 2019**: Alpha release
2. **November 2019**: Beta release
3. **January 2020**: Full launch

This report includes information on the overall platform structure as it can be seen on the alpha version, illustrates the design of existing and upcoming modules and describes their functionality.

The SecureHospitals.eu online platform consists of five main modules:

- Interactive Knowledge Directory
- Directory of Solutions Providers
- Training Directory
- Community of Practice

Figure 1 illustrates the overall structure that is currently being implemented. New modules, renaming or modifications of existing ones might be subject to the upcoming iterations.

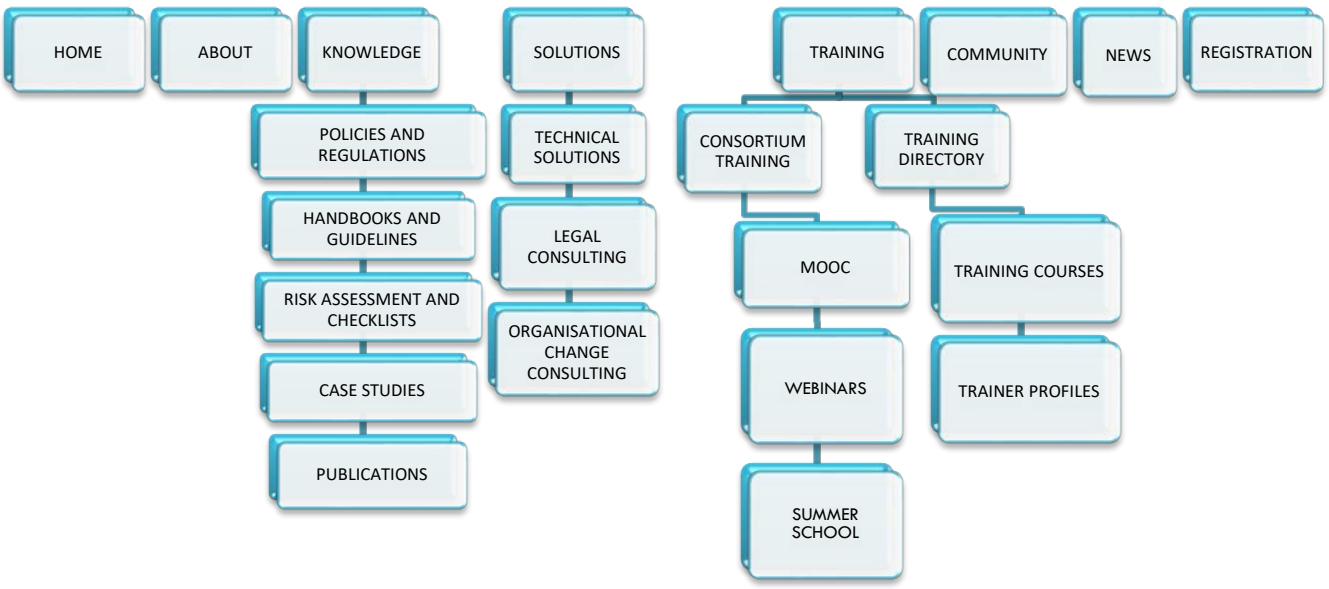

FIGURE 1: Structure Map of the SecureHospitals.eu Open Awareness and Information Hub

2 Homepage

The home page of the SecureHopsitals.eu online hub serves as an entry point, from which the activity of the whole platform can be seen in one view. The home page consists of the project's main information (about the project), describes the main modules and how the knowledge, training and solutions seekers can find what they need for increased cybersecurity within healthcare organisations; a development timeline mentioning what will come up next (temporary); as well as the latest news and materials listed on the platform. (See Figure 2).

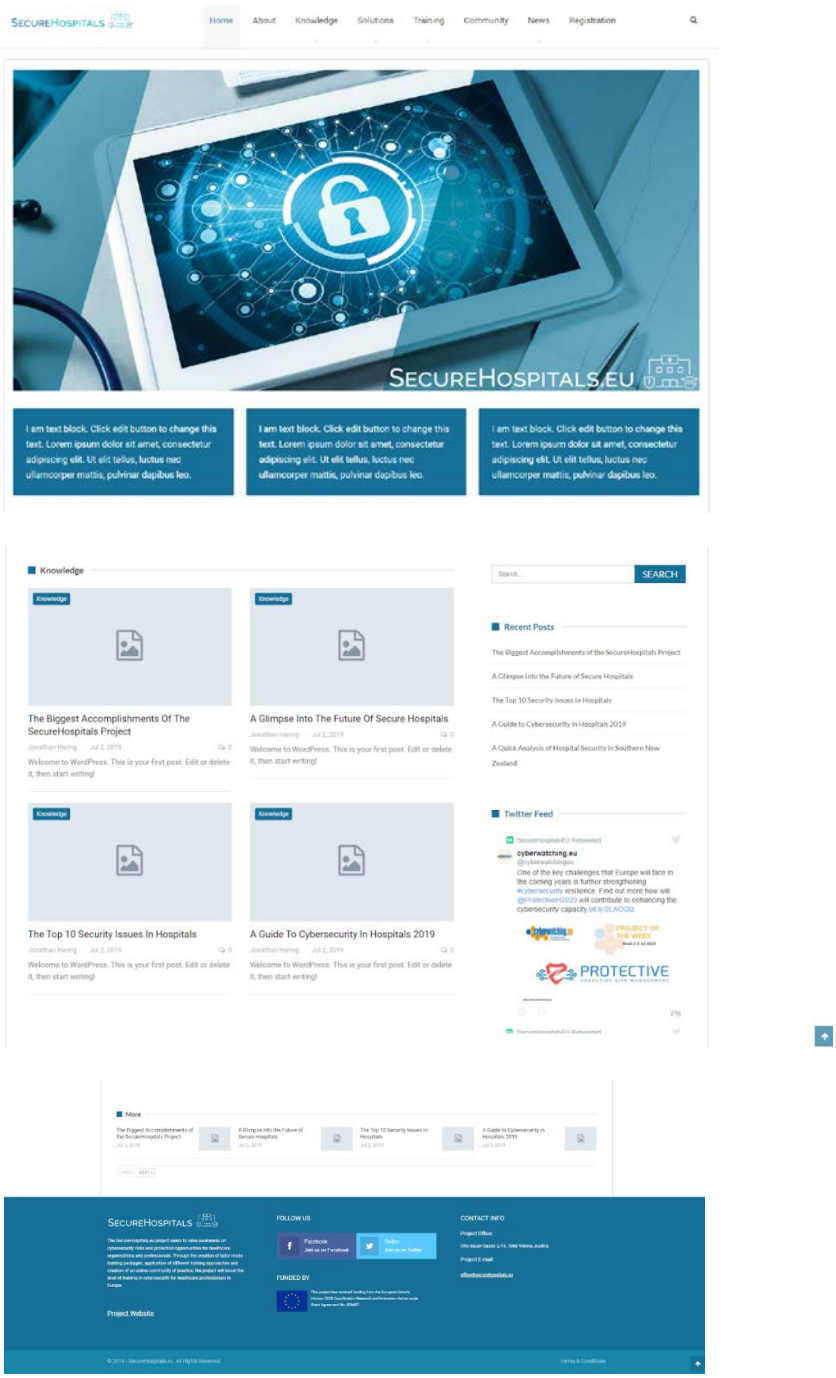

FIGURE 2: Homepage

3 Knowledge Directory

This module includes the outcomes of the knowledge aggregation activities conducted as part of all work packages. The knowledge materials collected during the initial project stage have been categorised and the most relevant information for project stakeholders has been filtered out, categorised and summarised to provide concise and comprehensible knowledge. According to the discussions among the consortium that took place primarily during a consortium meeting in Ancona, Italy, the knowledge materials should be categorised as shown in Figure 3.

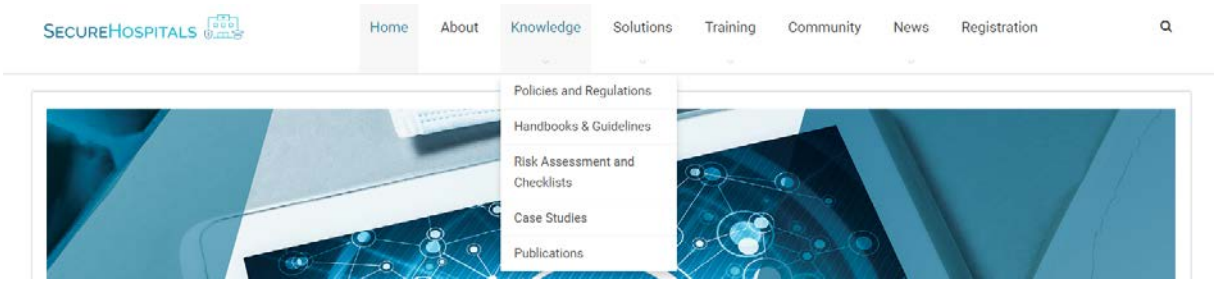

FIGURE 3: Knowledge Categories

3.1 Policies and Regulations

This section provides information on the main pieces of legislation regulating cybersecurity issues in Europe such as the NIS Directive, the Cybersecurity Act, etc., and describes their relevance and applicability for healthcare organisations. The summaries of each of these pieces of legislations seek to provide a common understanding for non-legal audiences, in an easily understandable terminology illustrated with concrete examples from healthcare contexts, while also providing links to the legislations and relevant authorities.

3.2 Handbooks & Guidelines

As part of other work packages, the different types of cybersecurity threats facing healthcare organisations, and the types of professionals within an organisation being affected by each of the threats have been identified. For each of the main threats, we provide lists of guidelines including structured rules and policies e.g. on data handling, threat identification, risk minimisation, etc. Besides concise tips in the form of guidelines addressing all types of healthcare professionals, this section will also include the latest handbooks released by main knowledge providers in the field of the field of cybersecurity, such as ENISA (the European Union Agency for Cybersecurity).

3.3 Risk Assessment & Checklists

Once different types of healthcare professionals become aware of the cybersecurity risks, a summary of all guidelines in the form of checklists for multiple types of professionals is essential for monitoring risks and making sure that all lessons learned are kept in mind. This section of the online hub thus provides cybersecurity checklists for healthcare professionals, as well as for IT staff to ensure continuous assessments of all cybersecurity strategies, measures and systems. The risk assessment checklists will help IT and cybersecurity staff to monitor human behaviour and technical systems on a regular basis.

3.4 Case Studies

In order to illustrate the risks, common threats and especially the consequences of major attacks or data breaches for healthcare organisations to their staff members, this section includes a collection of past incidents in Europe and globally. Each of the major cases describes the type of attack and the full scenario, highlighting the consequences for the organisation or potentially for the staff members involved, and lists the lessons learned.

3.5 Publications

At the beginning of project, a library of different knowledge sources, including primarily scientific articles, has been created using the Zotero tool. The library is a lively document which is being extended throughout the project lifetime with the most recent contributions to the field. This section of the platforms integrates the whole list collected in Zotero as a repository of knowledge sources for further reading.

4 Solutions

FIGURE 4: Solution Categories

The 'Solutions' module of the platform lists different types of the providers that offer solutions to those 'having the problem' (healthcare organisations). The directory showcases organisations offering different types of solutions required by healthcare organisations.

4.1 Technical Solutions

The technical solution providers include all types of providers of IT security solutions such as software, hardware, physical security etc. By creating a profile and listing their solutions, cybersecurity organisations have the chance to showcase their expertise and bring the solutions closer to the potential clients.

4.2 Legal Consulting

This section lists organisations providing legal expertise on healthcare organisations' compliance with different pieces of European and national legislations regulating cybersecurity issues. Considering that most of the cybersecurity incidents in the healthcare domain include data breaches, and that data protection procedures are strictly regulated by the EU Regulation 2016/679 (GDPR), legal expertise to advise on, and assess compliance with GDPR requirements, is an essential requirement for healthcare organisations.

4.3 Organisational Change Consulting

Besides providers of technical solutions and legal advice, a third type of solution providers in the context of cybersecurity are consulting companies offering advice on cybersecurity strategies for management level professionals. These types of consultants can advise directors of hospitals and care centres on changing the cybersecurity culture within their organisation by expanding the cybersecurity budget, changing the organigramme by adding new cybersecurity roles (e.g., Risk Manager etc.), implementing an enhanced training strategy for all types of staff, renewing the technical infrastructure by purchasing innovative products, purchasing security by design devices, etc.

4.4 R&D Projects

Finally, an important part of the solutions providers are consortia of European projects on cybersecurity with a focus on healthcare. A directory of projects and initiatives related to SecureHospitals.eu has been collected as part of D3.2 and is integrated into the Solutions directory, as showcases of innovation endeavours in the field, to promote the uptake of R&D outcomes.

5 Training

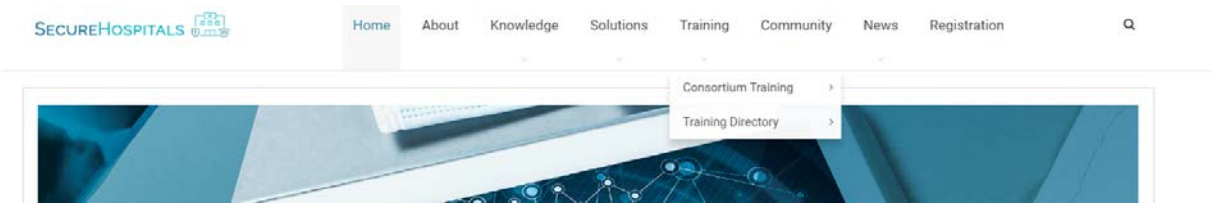

FIGURE 5: Training Module

5.1 Consortium Training

This part of the Training module will include information on the trainings to be organised by the consortium, namely the MOOC, Webinars, Workshops, and the Summer School.

MOOC

This page will rely information on the upcoming MOOC and provide the link to register. After the creation of the online course and the matching it's launch, the page will also be used to host the MOOC. After the end of the live course, all the materials will remain available on the page, for everyone to complete the course at any time.

Workshops & Webinars

This page will feature information on the workshops and webinars organised by the consortium in the second half of the project. During the workshops, platform visitors will have opportunity to register for each of the events and download the materials following the completion.

Summer School

The summer school page will provide registration and attendance information for the target audiences. After the completion, it will showcase all the materials and outcomes.

Conference

The conference page will be created in the second half of the project matching with the initiation of the organisation. It will also contain information on the agenda, audience, include the registration link etc.

5.2 Training Directory

The training directory provides an overview on existing cybersecurity courses, especially on those with a focus on healthcare, by different provides around Europe. The overall repository includes a directory of training providers which have the opportunity to list one or more available courses, a directory of available courses, as well as a directory of individual trainers who can showcase their expertise and and/or affiliate to any of the training provider organisations.

Training Providers

Training providing organisations have the opportunity to create an organisation page showcasing their profile and advertising their training courses. Organisations can also list their trainers, by

selecting one of the trainer profiles registered on the platform, or by inviting their trainers to register as affiliated. Training provider organisations can also register as providers of other solutions included in the Solutions directories.

Courses

The course catalogue is one of the most important directories of the SecureHospitals.eu online hub, enabling training seekers to find a one-stop-shop covering all possible training needs. The registration and showcasing of available courses are currently under development in the platform's backend. The course catalogue contains filters and sorting tools to enable fast navigation and matchmaking for training seekers.

Trainers

Individual trainers also have the opportunity to register on the platform and showcase their expertise by creating a trainer profile. Registration and profile setup utilities will be available in the second release of the SecureHospitals.eu online hub. Trainers can demonstrate their affiliations with registered organisations, list references, skill and types of expertise. Registered training organisations can send an initation to an external trainer to create a profile on the online hub and affiliate with the trianing provider organisation.

6 Community

This section of the online hub implements the 'Community of Practice' module as described in the Description of Action. The module is meant to be a virtual space for interaction and knowledge exchange for professionals to keep the cooperation ongoing on different topics. Registered users on the online hub can create a group on a specific topic to which they can invite other registered or non-registered users, and/or join exiting groups. Within a group, users can share documents and start discussions. The groups can also be open or closed. The following figures show mock-ups of community functionalities at the current stage of development.

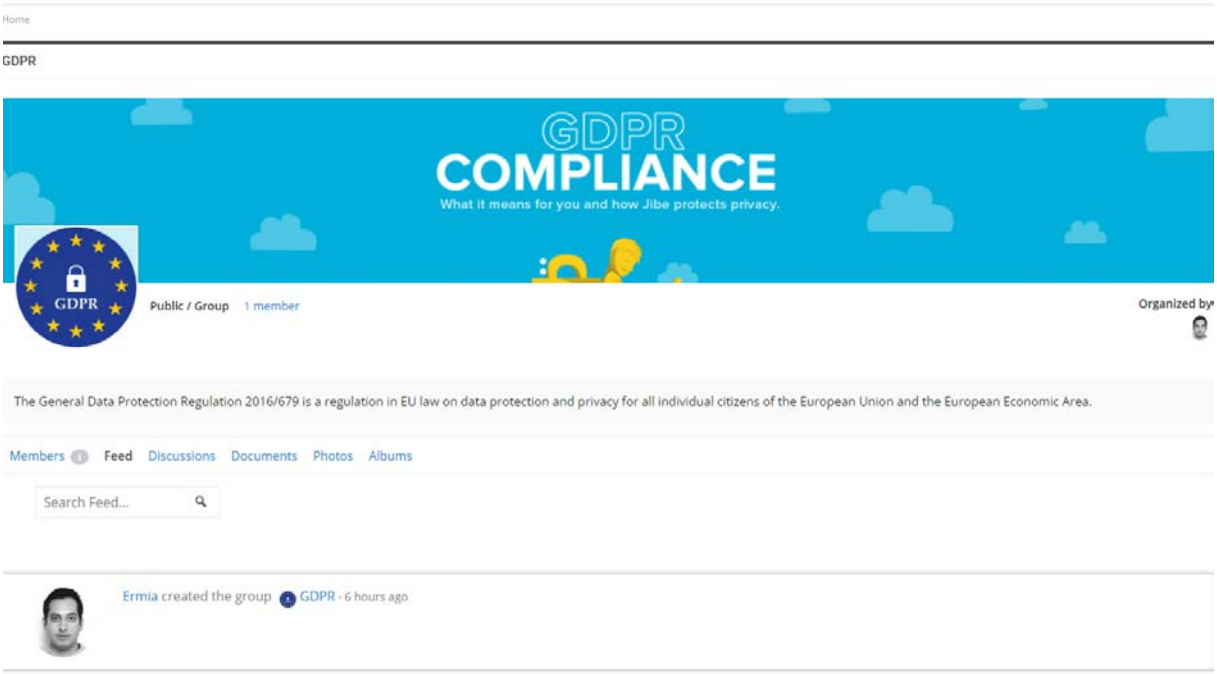

FIGURE 6: Community: Group View

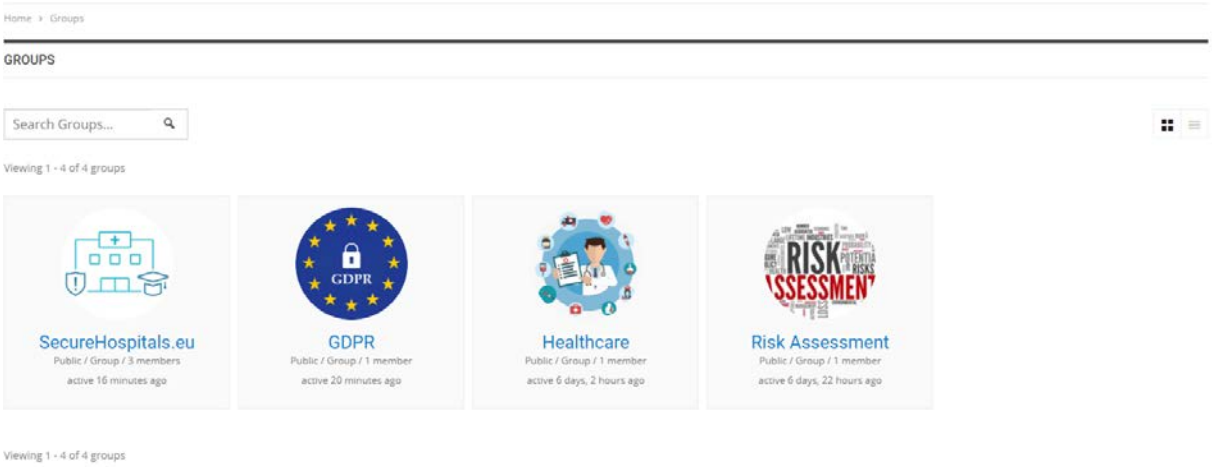

FIGURE 7: Community: Groups' Overview

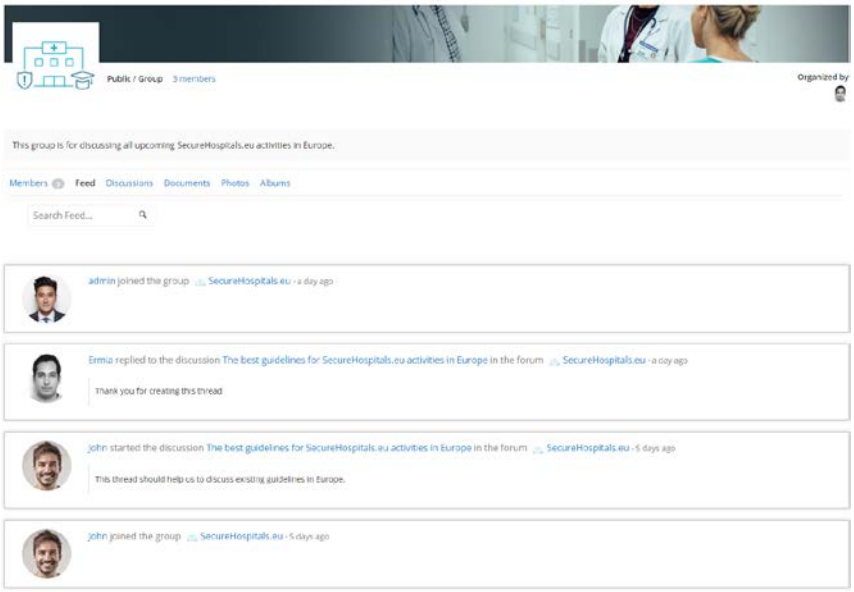

FIGURE 8: Community: Group Feed

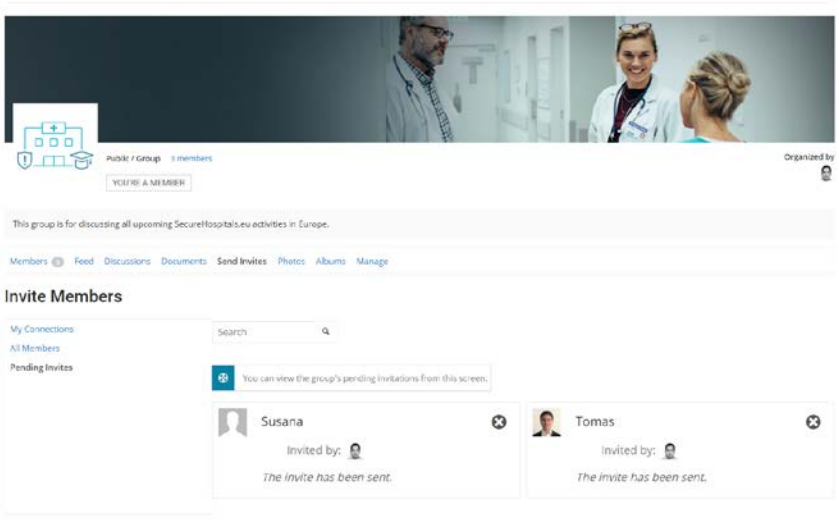

FIGURE 9: Community: Group Membership

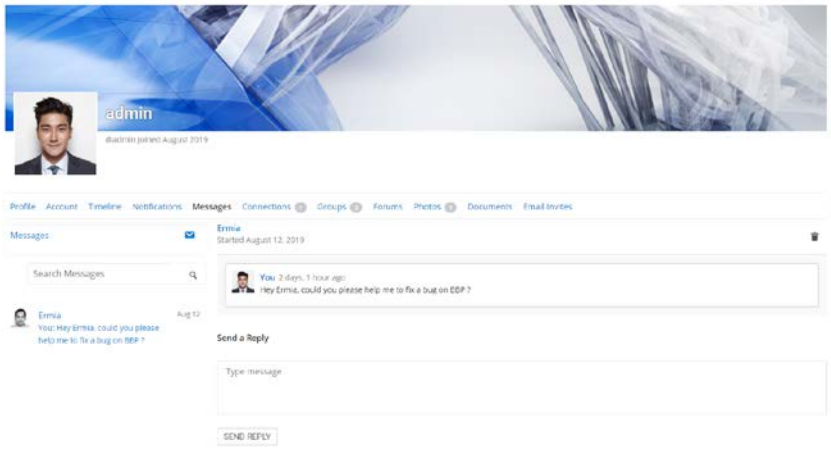

FIGURE 10: Community: Personal conversations

7 News

The news section will be filled in the upcoming stages of platform development and will primarily contain information related to the SecureHospitals.eu project. Project news include: reports on project events, reports on external events attended by the consortium, publications and press releases from the consortium on other media outlets, new publications related to the field as well as important news related to the community of training providers such as new training etc.

8 Conclusion

As outlined in the Description of Action, the SecureHospitals.eu Online Information and Awareness Hub will be developed in several iterations. This report presented an overview of the different functionalities of the platform as well as the technical framework. Using standard open access software standards, a flexible and scalable architecture is being developed to guarantee long-term sustainable usage of the platform.

The Alpha version of the online hub includes an overview of the modules, descriptions and announcement of what will be coming next. The Beta version will implement the first structure of the online knowledge materials, solutions and trainings, and open the registration for all providers of solutions (including training). It will also include the training setup utilities for enabling organisations/trainers already contacted and engaged by the consortium to initiate annotations on the platform for listing their organisation/trainer profiles and respective solutions. Further materials, infographics, visualisations and toolboxes will be adopted in the last iteration marking with the last stage of the SecureHospitals.eu project.

Intensive awareness raising and stakeholder engagement on the SecureHospitals.eu online hub will start from its first Alpha release through different channels such as the project's social media channels, project website and newsletter, through attendance of the external stakeholder events etc. The second project period which will include the delivery of a series of training activities, a core mission of which will also be to draw attention to the online hub as a tool for strengthening the knowledge provided during the training, finding the right solutions and connecting with other professionals to engage in knowledge exchange of best practices around Europe.