CALL H2020-SU-DS-2018-2019-2020
Digital Security
TOPIC SU-DS05-2018-2019
Digital security, privacy, data protection and accountability in critical sectors

AI4HEALTHSEC

"A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures"

D8.1 – Dissemination and Communication Plan

Due date of deliverable: 31.03.2021
Actual submission date: 31.03.2021

Grant agreement number: 883273
Start date of project: 01/10/2020
Revision: 1

Lead contractor: CNR
Duration: 36 months

Project funded by the European Commission within the EU Framework Programme for Research and Innovation HORIZON 2020	
Dissemination Level	
PU = Public, fully open, e.g. web	✓
CO = Confidential, restricted under conditions set out in Model Grant Agreement	
CI = Classified, information as referred to in Commission Decision 2001/844/EC.	
Int = Internal Working Document	

D8.1 - DISSEMINATION AND COMMUNICATION PLAN

Editor
Argyro Chatzopoulou (TUV)

Contributors
Apostolos Karras /TUV)
Mario Ciampi (CNR)
Spyros Papastergiou (FP)

Reviewers
Eftychia Lakka (FORTH)
Anca Bucur (PHILIPS)

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	30.03.2021	Chatzopoulou Argyro	Initial Version

The work described in this document has been conducted within the project AI4HEALTHSEC, started in October 2020. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273

Executive Summary

The purpose of this deliverable is to present the Communication and Dissemination strategy that will guide the development of activities envisaged for the whole project, to maximize the impact of the project on target audiences, and to present the KPIs defined for the project which will allow to monitor and evaluate the success of the work performed in T8.1.

The project's communication activities will call attention of multiple audiences about the research being implemented while at the same time address the public policy perspective of EU research and innovation funding.

At the same time dissemination means sharing research results with potential users - peers in the research field, industry, other commercial players and policymakers. By sharing the research results with the rest of the scientific community, the AI4HEALTHSEC project will contribute to the progress of science in general and to the achievement of the project goals.

This document contains information on

- The objectives to be fulfilled by the project and in particular by the dissemination and communication activities.
- The dissemination and communication strategy for the entire three-year duration of the project, at a high level.
- The dissemination and communication activities of the first year at a more detailed level.
- The different channels and means of communication and dissemination to be used by the AI4HEALTHSEC project.
- Details about the decisions that have been taken regarding the components of the AI4HEALTHSEC "brand" (e.g. Logo, colors, fonts, etc.).
- The KPIs that will be used for the monitoring, measurement, analysis and evaluation of the performance of Task 8.1 against the set objectives.

The activities regarding Dissemination and communication are expected to change based on the needs and the developments of the project.

This document contains an overview as seen during month 6 of the project.

Contents

List of acronyms

No	Name	Short name	Country
1	CONSIGLIO NAZIONALE DELLE RICERCHE	CNR	Italy
2	PHILIPS ELECTRONICS NEDERLAND BV	PHILIPS	Netherlands
3	KLINIKUM NURNBERG	KLINIK	Germany
4	EBIT S.R.L.	EBIT	Italy
5	IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	Greece
6	TUV TRUST IT GMBH UNTERNEHMENSGRUPPE TUV AUSTRIA	TUV	Germany
7	FOCAL POINT	FP	Belgium
8	FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.	FHG-IBMT	Germany
9	SPHYNX TECHNOLOGY SOLUTIONS AG	STS	Switzerland
10	UNIVERSITY OF BRIGHTON	UOB	United Kingdom
11	PDM E FC PROJECTO DESENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIALDA	PDMFC	Portugal
12	AEGIS IT RESEARCH GMBH	AEGIS	Germany
13	PRIVANOVA SAS	PN	France
14	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	ICCS	Greece

List of tables

List of figures

1 Introduction

1.1 *An Introduction to the AI4HEALTHSEC Project*

Over the past decade, the medical field has experienced a massive digitization. The value of personal medical data has increased on the black market and, therefore, adversaries of Health Care Information Infrastructures (HCIIs) are now more numerous and better-skilled.

- HCIIs today are unprotected because they address cybersecurity with individual and isolated products. They need to define a high-level security strategy capable of orchestrating multiple security components to identify system vulnerabilities and sophisticated attacks.
- Decomposing the problem of cybersecurity in the health sector into areas of concern based on the criticality of their assets, will prioritize emerging solutions and decrease its complexity.
- Attacks against the health sector have become highly sophisticated and target not only systems and technical vulnerabilities but also use social engineering to exploit people with insufficient technical background.
- EU health and cybersecurity experts must coordinate and build together policies and standards that will increase the levels of security maturity across the EU.
- Cyber security solutions in health must have a clear business impact and facilitate new kinds of services, collaborations and market opportunities.

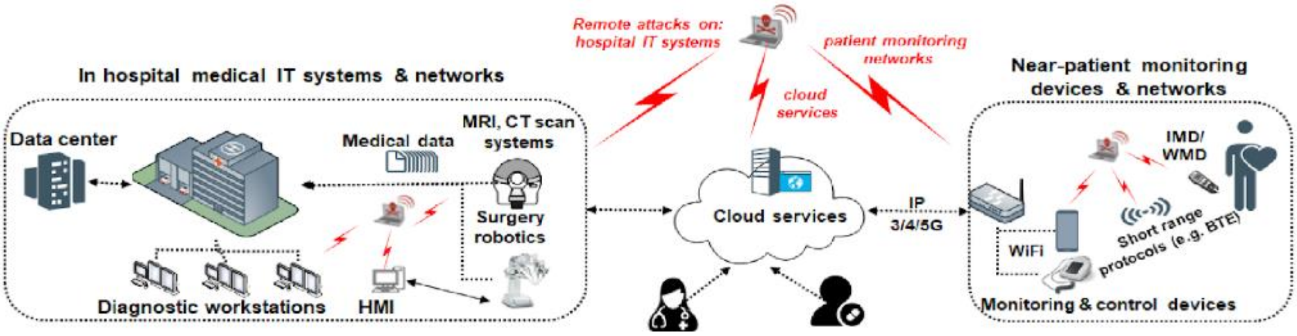

Remote attacks on: hospital IT systems
patient monitoring networks
cloud services
In hospital medical IT systems & networks
Data center
Medical data
MRI, CT scan systems
Surgery robotics
Diagnostic workstations
HMI
Cloud services
IP 3/4/5G
Near-patient monitoring devices & networks
IMD/ WMD
WiFi
Short range protocols (e.g. BTE)
Monitoring & control devices

Figure 1:Challenges in the HCIIs

AI4HEALTHSEC will deliver an Artificial Intelligence Dynamic Situational Awareness Framework (DSAF) able to:

- improve, intensify and coordinate the overall security efforts for the effective and efficient identification, evaluation, investigation and mitigation of realistic risks, threats and multi-dimensional attacks within the cyber assets.
- support, prepare and help the Interdependent HCIIs participating in different types of Health Care Supply Chain Services.

The DSAF will support:

- the HCIIs and the other stakeholders comprising the Health Care ecosystem to recognize, identify, model, and dynamically analyse cyber risks.
- forecasting, treatment and response to advanced persistent threats and handle daily cyber-security and privacy risks, incidents and data breaches.

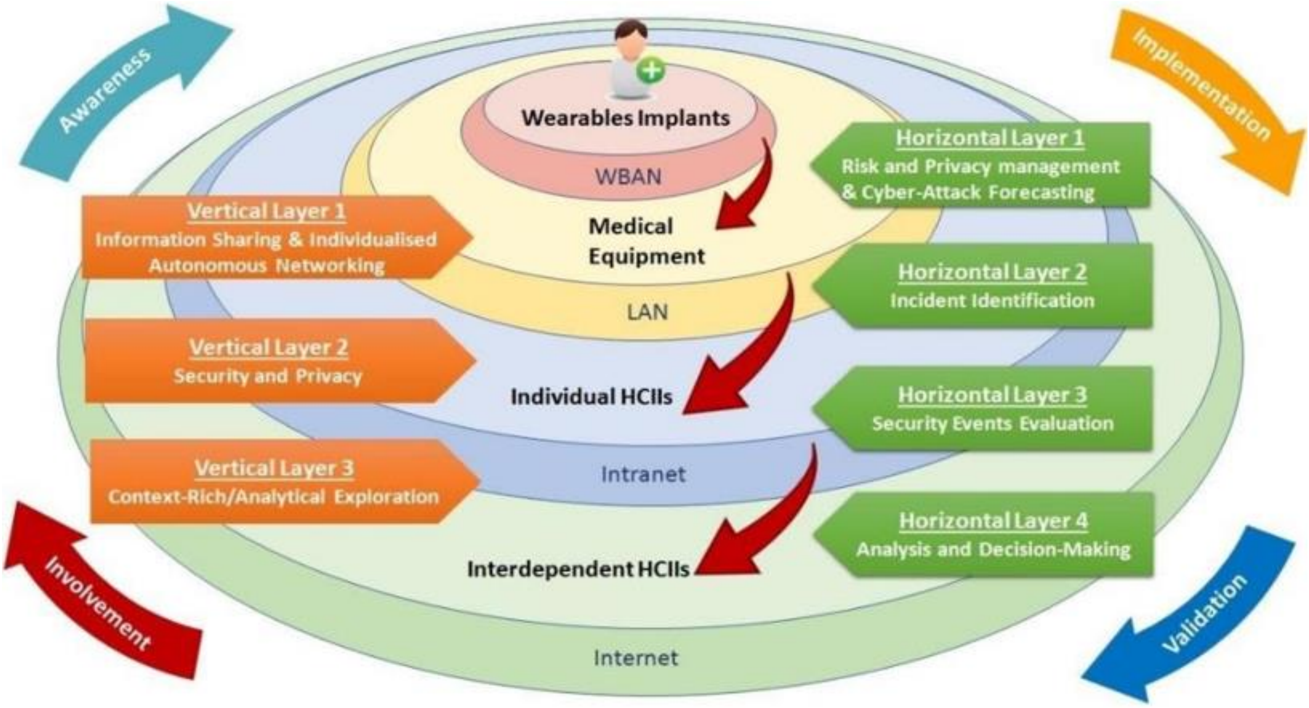


Figure 2: Structure of the Artificial Intelligence Dynamic Situational Awareness Framework (DSAF)

It is the intention of the consortium to implement the major principles of Integrated Project Structure, Approved Project Management Instruments and Binding decision provisions and agreements upon all partners, within the project management approach to assure that AI4HEALTHSEC meets its entire objectives on time, on budget, and with supreme quality results.

1.2 *The vision for the Dissemination and Communication activities of the project*

In this context, communication and dissemination activities of the project will aim, in general, at:

- Making the various stakeholders aware of the project and the related benefits.
- Improving the overall cyber situational awareness of the health care ecosystem and optimising the collaboration and interaction amongst HCSC stakeholders in order to exchange incident-related information.

- Introducing advanced capabilities to detect, assess and respond to security incidents (including threats, risks and vulnerabilities) for organizations (or generally stakeholders) within the specific area.
- Presenting a detailed specification of the AI4HEALTHSEC framework (a step-by-step approach) to support security-related incident forecasting, identification, assessment, investigation, recovery and warning that will be based upon accurate, credible and relevant information and proofs gathered by the underlying HCIIs (individual and independent HCIIs) and HCSCS.
- Presenting the AI4HEALTHSEC system based on the AI4HEALTHSEC framework as implemented for the project pilots.
- Sharing best practices elicited on the basis of the knowledge management and knowledge harvesting mechanisms of the project's incident management framework, which will reflect distributed intelligence/awareness from the handling of numerous incidents in the HC environment.
- Contributing to remedying gaps in standardization about situational awareness and incident management for HCIIs.
- Showing how the *AI4HEALTHSEC* solutions can reduce complexity regarding the implementation of cyber-security tools for healthcare European entities - thus decreasing the risk of accident or potential cyber-attacks as well as increasing preparedness and coordination response in case of a cyber-incident affecting digital technology and networks, etc.;
- Presenting better tools and algorithms so cyber-security may not affect the quality of the products / services, and dynamic testing and certifications for companies creating new tools, adjusting to modifications etc.;
- Making sure that the results are communicated to decision-makers and authorities to influence policy-making in the area of security services offering and digital protection as well as business concepts and models;
- Making sure that the results are communicated to the scientific community to ensure increased evidence of the benefits of the proposed security framework and its incorporation into public and private services;
- Showing how research outcomes can be relevant to our everyday lives, by creating jobs, introducing novel technologies, or making our lives more secure in other ways;
- Accounting for public spending by providing tangible proof that collaborative research adds value.

In the initial phase of the project, the communication actions will focus on presenting the consortium, the projects, its objectives, and expected outcomes, to raise awareness among stakeholders. The generation of research output dissemination will focus on reaching the primary beneficiaries such as hospitals, general practitioners, government/public health services, end-users, security professionals, health and security providers (SME and enterprises), academic institutes, standardisation organisations, and key industry representatives. In line with the technical development and progress, both communication and dissemination activities will focus on presenting the results of the AI4HEALTHSEC system through specific outreach activities to all audiences. By the end of the project, the focus will be oriented towards the development and results of the pilots, the system, and the generation of engaging opportunities to support the exploitation and sustainability activities.

All the activities will be detailed and broken down in this Communication and Dissemination Plan which constitutes the first deliverable from the WP8 – Dissemination, Exploitation, legal aspects and Sustainability.

As the project progresses, and the results become more tangible and concrete, the Communication and Dissemination Plan will evolve as well to incorporate the changes. The development of activities and any change or adaptation made on the Communication and Dissemination plan will be shown in the relevant reports e.g. D8.2 - Report on Dissemination and Communication Activities version 1, D8.3 - Report on Dissemination and Communication Activities version 2, D8.4 - Exploitation, Sustainability and Business Plans version 1 and D8.5 - Exploitation, Sustainability and Business Plans version 2.

2 Purpose and objectives

The purpose of this deliverable is to present the Communication and Dissemination strategy that will guide the development of activities envisioned for the whole project, to maximize the impact of the project on target audiences, and to present the KPIs defined for the project which will allow to monitor and evaluate the success of the work performed in T8.1.

The project's communication activities will call attention of multiple audiences about the research being implemented (in a way that it can be understood by different audiences) while at the same time address the public policy perspective of EU research and innovation funding.

Dissemination means sharing research results with potential users - peers in the research field, industry, other commercial players and policymakers). By sharing the research results with the rest of the scientific community, the AI4HEALTHSEC project will be contributing to the progress of science in general and to the achievement of the project goals.

The document aims to fulfill the following objectives:

- Define a clear strategy for AI4HEALTHSEC communication and dissemination activities
- Define the roles of partners involved in this task
- Identify the channels and tools which will be used throughout the duration of the project
- Set the methodology for the evaluation of the activities defined

2.1 *Structure of the document*

The deliverable is structured as follows:

- Chapter 3 presents the communication strategy for AI4HEALTHSEC project, and the individual communication and dissemination plans of the partners
- Chapter 4 presents the detailed channels defined in Chapter 3
- Chapter 5 describes the KPIs established for the whole project and the monitoring process that will follows to determine the success of the strategy

3 Communication and Dissemination Strategy

As mentioned in the proposal, the dissemination plan is based on major dissemination channels and is designed as a blend of dissemination activities from a variety of channels, with respect to the respective target groups that it aims to address.

The communication and dissemination activities are strategically planned and are not just ad-hoc efforts. This is the reason why the project has created this strategy and has panned for dissemination and communication activities.

Every project partner will ensure that dissemination activities will be carried out nationally, and if applicable, it will contribute to disseminate the project's results internationally. As such, dissemination aims at generating values for EU industries and academia.

As soon as the first exploitable deliverables and outputs are created, the project partners would disseminate the project's results to both scientific and industrial communities and other target groups in the EU, in order to stimulate awareness. The dissemination content will be prepared keeping in mind the relevant audience and their technical level of understanding. The reasoning behind the dissemination content will be to convince the audience for the benefits of the (expected) project outcomes.

3.1 *Communication and Dissemination Key Audiences*

The generation of research output dissemination will focus on reaching the primary beneficiaries such as hospitals, general practitioners, government/public health services, end-users, security professionals, health and security providers (SME and enterprises), academic institutes, standardisation organisations, agencies, key industry representatives and other related stakeholders.

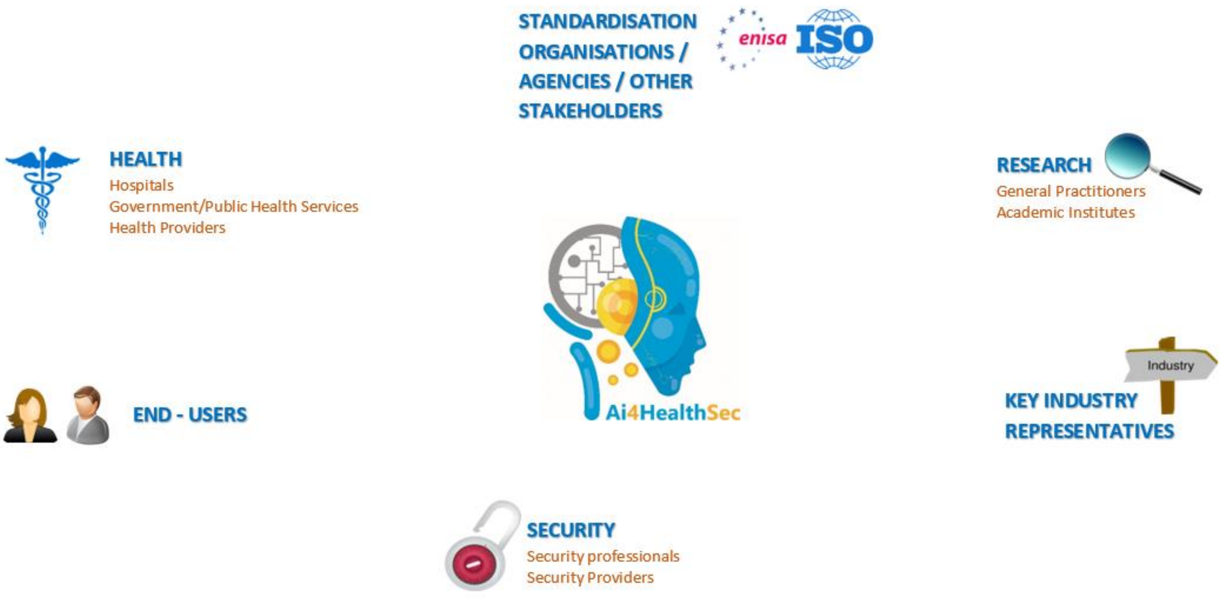


Figure 3: The Communication and Dissemination key audiences (categories)

In order to reach the key audiences mentioned above, the help of all project partners will be solicited. The project partners could help by

- Communicating to their extended ecosystem of partners, customers, associates, suppliers etc.
- Connecting with organizations they already have an established relationship (e.g. associations, standardization initiaves, etc.)
- Actively searching and inviting entities to learn more about the project and its outcomes during their daily interactions.

The contribution of all project partners is essential for the success of the communication and dissemination activities.

3.2 *Communication and Dissemination Channels and Activities*

AI4HEALTHSEC plans to utilize the following channels:

- Own (AI4HEALTHSEC) web and social media presence. As shown below, AI4HEALTHSEC has established (Project Month 3), a website. The website will be a key point for the propagation, initiation and archiving of the communication and dissemination activities of the project. The website will adapt to the project needs in content as well as in structure. Additionally, AI4HEALTHSEC has established (Project Month 3), accounts in three social media platforms (Facebook, twitter, LinkedIn). Based on the specific profile of the social media platform, communication messages will be propagated accordingly. For example, while the main messages and news will be propagated in all platforms with the suitable alterations, the happenings during a workshop or an event will be communicated only via twitter.
- Project partners web and social media presence. Each partner has at least a website and one social media account. All partners are expected to use their official channels of communication to support the project and increase its outreach. A list of the websites and social media accounts of the partners of the AI4HEALTHSEC project is depicted in Appendix A.
- Events, conferences and workshops. AI4HEALTHSEC will participate in scientific and industrial events to promote the project. Moreover, AI4HEALTHSEC will organize conferences, workshops and training sessions to discuss issues of interest for the project, based on the needs and stages of development of the project.
- Newsletter. AI4HEALTHSEC will periodically produce a regular awareness newsletter that will be sent to interested parties. Until Project Month 12, at least 2 Newsletters will be issued.
- Other related projects. AI4HEALTHSEC will cooperate with other related European Projects that have overlapping fields, so as to enhance the required unity of the European research taskforce and increase the innovation impact.
- Standardization organizations. AI4HEALTHSEC will establish relationships with standardization organization, through which the results of the project will be communicated. The AI4HEALTHSEC project team will invest effort in order to provide valuable input for relevant standardization activities. To achieve this relevant standardization plans will be designed and implemented as part of the activities of Task 8.3. Standardization and Certification Activities.

- Relevant authorities. AI4HEALTHSEC will establish channels to relevant agencies (European or national) as well as relevant competent authorities, through which the results of the project will be communicated and if possible, valuable feedback will be received. These entities will also be identified as part of other tasks of the project (e.g. market analysis, stakeholder requirement analysis and validation etc).

To better coordinate these activities each partner was requested to nominate at least one member of their organization that will act as a communication and dissemination contact point. All partners have supplied this contact person and a specific mailing list has been created, to facilitate communication.

3.3 *Individual Communication and Dissemination Plans*

As discusses above, the success of the dissemination activities of the AI4HEALTHSEC project cannot be based only on the efforts by the project team. Each partner has to partake on the responsibility to pass along and spread the information and messages of the project.

So, apart from the strategy for the entire project mentioned below, each partner has committed to an individual communication and Dissemination plan for the AI4HEALTHSEC project. These plans at this point (at month 6 of the project), are generic and will be further enriched as the project progresses.

In the following paragraphs, the individual communication and Dissemination plans of the partners are displayed.

CONSIGLIO NAZIONALE DELLE RICERCHE (hereinafter, referred as CNR)

The main role of CNR in the project is the coordination of the AI4HEALTHSEC (leading WP1), by exploiting its experience in the management of a variety of research projects and in particular in the coordination of a European project funded under H2020 Programme. Moreover, CNR will provide its contribution in the application of security techniques in the e-health domain by using its expertise acquired in project focused on electronic health records interoperability. It will lead the development of the Security Incident/Attack Simulation Environments in T5.5 and will assist in increasing participation and awareness of the project results by leading T8.5.

Based on the above description, CNR will contribute significantly in the activities of the project and will utilize all its channels for the successful dissemination and communication of the project results at the different points in the project life. Based on the needs and the purpose of each outcome or development, CNR will select the best fitting channel and method. CNR is committed to disseminate and communicate the outcomes of the project through means like Scientific Publications, Workshops, Virtual Events, Website and Social Media.

AEGIS IT RESEARCH UG (hereafter, referred as AEGIS)

AEGIS leads the system architecture definition (T2.4) while also contributes in the privacy, situational awareness and incident handling specifications (T3.4, T4.1 and T4.3). It is also leading the development of the Individualized Autonomous Networking Layer (T5.1) and assists in the development of incident-handling and attack simulation systems (T5.4 and T5.5). Additionally, AEGIS contributes to integration activities in WP7 and is responsible for framework Goal assessment and refinement, convergence with pilots (T7.3) and the security and privacy evaluation (T7.4). Finally, AEGIS leads T8.4 on market analysis and business planning.

For all the reasons above, it stands to reason that AEGIS will heavily contribute to activities of the project. AEGIS is using its social media channels and its website to communicate and disseminate all progress done as the project development unfolds, as well as every exploitable outcome. Additionally, AEGIS will constantly raise awareness for AI4HEALTHSEC among its customers and partners in other EU-funded projects that is engaged to. Finally, AEGIS plans to promote project's achievements by participating in events and workshops.

EBIT S.R.L. – ESAOTE GROUP (hereinafter, referred as EBIT)

Esaote Group is one of the world's leading producers of medical diagnostic systems (Ultrasound, dedicated MRI, Healthcare IT) and internationally acknowledged to be the world leader in dedicated MRI. The Esaote Group is also one of the main players in the sector of Information Technology for healthcare.

Ebit is the Esaote's Healthcare IT Company focused on Enterprise IT software systems for seamless integrated workflows processes in multiple departments, enterprise and regional network architectures to facilitate information sharing.

EBIT will contribute to the requirements (functional and nonfunctional) (T2.1 and T2.3) and standardization, Technology System Integration, Pilot development (T6.1, T6.4) and Evaluation (T7.3), Exploitation and Dissemination (T8.1).

As part of the outgoing activities of the project, EBIT will adopt the AI4HEALTHSEC framework to facilitate the introduction of innovative security technologies. In this context, in order to define appropriate ready-to-market solutions, EBIT will to focus on delivery necessary technology requirements to the technology providers and integrators. The results of these practical applications will be communicated internally and externally by EBIT using the channels and media to its disposal.

These channels include amongst others the website of the organization and of the Esaote group and the relevant social media accounts.

FOCAL POINT (hereinafter, referred as FP)

FP will contribute to T2.4, by supporting the specification of the AI4HEALTHSEC platform architecture; will lead WP3, by supporting the design of the Self Organised Swarm intelligence system, and participate in WP4 towards the design of the Dynamic Cyber Situational Awareness Framework. Moreover, FP will be involved in the development of the Dynamic Cyber Situational Awareness Framework (WP5) and on WP8 (Dissemination and communication).

FP was founded in 2012 in Belgium providing comprehensive solutions mainly on Cyber Security issues related to Cyber Incident Response. With a head office in Belgium and satellite offices in Denmark and UAE, FP is a specialist cyber security services organisation offering consulting, managed services, security assessments & training. FP is focused on improving its client’s ability to manage the cyber threat landscape and achieving their business objectives.

FP participates in related European funded research projects and has already contributed in the identification of security vulnerabilities.

FP will communicate the results and developments of the AI4HEALTHSEC project through the website and social media presence of the company. Moreover, and depending on the project developments will participate in events, conferences and workshops. Finally, FP plans to (based on the project results and research developments) participate in relevant conferences and publish articles or other publications.

FOUNDATION FOR RESEARCH AND TECHNOLOGY HELLAS (hereinafter, referred as FORTH)

FORTH will contribute to the requirements gathering (T2.1) and system architecture definition (T2.4). In addition, it will utilize its expertise in security and privacy contributing to the development of security and privacy modelling methods and techniques in all WP3 tasks, T7.1, T7.2 and leading T4.3 and T5.4.

FORTHcert, which is part of FORTH, is a CSIRTs accredited by ENISA. FORTH will utilize the current links to enable AI4HEALTHSEC to demonstrate sharing of information with relevant parties at all required levels, including industry and CSIRTs. Also, FORTH participates in a variety of European funded research projects. Through these interfaces, FORTH will communicate information regarding the developments and results of the AI4HEALTHSEC Project. Information regarding the project will be communicated through the channel and method that seems more effective (in relation to the subject, scope and purpose of the message, result or development) each time. The available channels include the web presence of FORTH, the various social media accounts as well as the various partnerships and memberships in related groups, associations and initiatives.

Finally, FORTH will disseminate project results through the publication of scientific articles and their presentation to scientific conferences.

FRAUNHOFER GESELLSCHAFT ZUR FÖRDERUNG DER ANGEWANDTEN FORSCHUNG E.V. (hereinafter, referred as FHG-IBMT)

FHG-IBMT is a leading organization for applied research and technology development. It will contribute in this project to the analysis of requirements (T2.1), the evaluation metrics (T2.3) and provide its technical competency in the domain of health information systems and medical implants. Furthermore, it will lead WP6 by defining the pilot implementation strategy and will implement and demonstrate a pilot study in its areas of expertise (T6.2). For this purpose, FhG-IBMT will modify its implants platform, and its eHealth- and biobank information systems used in the pilots to leverage the AI4HEALTHSEC framework. It will contribute to the assessment and pilot alignment of the framework in T7.2, T7.3 and T7.4 and lead the formulation of policy recommendations in T7.6. Finally, it will participate in standardisation activities (T8.3) and third-parties involvement activities (T8.5).

FHG-IBMT will focus amongst other on building the scientific community around the cyber-security domain for the healthcare sector, designing a number of follow-up research projects and initiatives at both national and international level. Within this context, FHG-IBMT will communicate the results and significant parts of the developed technologies to other European funded projects, other linked parties and its research ecosystem.

As mentioned above, FHG-IBMT, leads the Task 7.6. Policy Recommendations and Guidelines for Wider Applicability and Use. This task is concerned with the formulation of policy recommendations for public authorities dealing with regulatory aspects of the fight against both cyber-attacks, risks and threats in HCIIs. These best practices will provide guidelines for successfully extending and applying the AI4HEALTHSEC results in other critical information infrastructures, as it will be demonstrated by the mini-projects implemented through the open call organized as part of WP8.

FHG-IBMT will use its links to authorities, security organizations and other related stakeholders to communicate the project, the project developments and results. FHG-IBMT will communicate the results and developments of the AI4HEALTHSEC project through the website and social media presence of the company. Moreover, and depending on the project developments will participate in events, conferences and workshops.

INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS (hereinafter, referred as ICCS)

ICCS, as a research entity with particular interest in real-world problems encapsulating challenges which can potentially expand and enrich its research potential, will primarily focus their dissemination activities on the publication of high quality research papers in international, well-reputed conferences and journals. Moreover, given its strong links with both national and European academia and industry, ICCS will present, discuss, and promote the AI4HEALTHSEC findings, outcomes and results to its wide network of collaborators. Also, as ICCS has strong involvement in numerous national and EU projects, it will engage in boosting awareness of the AI4HEALTHSEC solution to all stakeholders involved. Although AI4HEALTHSEC primarily focuses on the healthcare domain, its expandability and applicability to other critical infrastructures will be a key driver in the dissemination of the project's developments to the energy and the drinking water supply sectors, with whom ICCS has close bonds in Greece and in the EU.

KLINIKUM NURNBERG (hereinafter, referred as KLINIK)

KLINIK contributes to the project as piloting partner. That encompasses the definition and selection of a pilot area, collaboration in creating a pilot plan (T6.1), conducting the pilot (T6.3) and collaboration in assessing pilot results (T7.3, T7.4). Further KN will gather requirements from its ICT business unit, its executive staff and users (T2.1). KN will also test the propagated R&D solutions to contribute concerning validation of objectives of the project.

KN represents scenarios with highly interconnected hospital IT and special challenges such as the need to validate security patches from IT providers before implementing them in the running system. Furthermore, hospital staff directly interacts with critical infrastructure during often stressful daily work.

KLINIK will endeavor to integrate the project results in master thesis of students from external universities (supervision of master thesis by KLINIK and external universities), contribute and publish results in scientific papers and other publication (concerning user requirements analysis especially in the hospital environment and findings on how to create higher cyber-security awareness at hospitals through external framework). Possible publications could include scientific journals (e.g. Journal of Medical Internet Research) and national/international conferences (e.g. GMDS annual conference or Medical Informatics Europe). Finally, KLINIK will utilize the website and social media presence as appropriate.

PHILIPS ELECTRONICS NEDERLAND B.V. (hereinafter, referred as PHILIPS)

An important aspect in the dissemination and communication activities for PHILIPS (among the other partners) is to raise awareness with respect to the advantages and effects of the novel solutions offered by the project considering the risks and challenges of cyber-security for the European health sector.

Based on the above description, PHILIPS will contribute to the activities of the project and will utilize all its channels for the successful dissemination and communication of the project results at the different points in the project life (especially keeping in mind the leading role that PHILIPS is playing in tasks 1.5 and 8.2). Based on the needs and the purpose of each outcome or development, PHILIPS will select the best fitting channel and method. PHILIPS is committed to disseminate and communicate the outcomes of the project through means like Scientific Publications, Workshops, Virtual Events, Website and Social Media. Moreover, PHILIPS will explore links to various standardization bodies and other industrial organizations, in order to influence the adoption of models and guidelines developed by the project. Finally, PHILIPS, through its links to professional and scientific associations will promote the developed frameworks in those communities, through the methods and channel to its disposal as mentioned above.

PRIVANOVA SAS (hereinafter, referred as PN)

PN will lead the tasks concerning the legal and ethical aspects of the project. The work varies from general guidance of the consortium towards legal and ethical compliance, via guidance for the implementation of the data protection principles and provisions as well as guidance towards ethically compliant trials and testing, to research of aspects of the data protection framework that are specific to the development of a solution for sharing, computing and extracting the desired value out of personal data.

To that end, PN will lead task T1.6 'Ethical, Privacy, GDPR Compliance and Security Coordination' in order to address the legal and ethical issues arising from the research activities, the trials and testing, especially insofar as they include the processing of personal data. Moreover, PN will also lead task T2.2 Basis of Legal and Ethical Requirements in order to provide for the generally applicable legal frameworks with particular emphasis on the application and implementation of the General Data Protection Regulation. Finally, PN will lead the legal validation of the project by assessing the integration of all identified requirements in the course of developing the AI4HEALTHSEC project in

task T7.5 Legal and ethical implementation, oversight and evaluation and contribute to dissemination and exploitation activities in WP8

Based on the above mentioned involvement, PN will contribute significantly in the activities of the project and will utilize all its channels for the successful dissemination and communication of the project results at the different points in the project life. Based on the needs and the purpose of each outcome or development, PN will select the best fitting channel and method. PN is committed to disseminate and communicate the outcomes of the project through means like Scientific Publications, Workshops, Virtual Events, Website and Social Media.

PROJECTO SEDENVOLVIMENTO MANUTENCAO FORMACAO E CONSULTADORIA (hereinafter, referred as PDMFC)

PDMFC will contribute to WP2 providing support for the platform requirements and the architectural specification. PDMFC will also lead T3.4, T4.4 and T5.3 and contribute to the rest of the tasks in the relevant WPs with expertise in security and privacy engineering. PDMFC will also lead the WP7 platform integration activities and contribute to WP8 exploitation and communication tasks.

PDMFC will communicate the results and developments of the AI4HEALTHSEC project through the website and social media presence of the company. Moreover and depending on the project developments will participate in events, conferences and workshops. Finally, PDMFC plans to (based on the project results and research developments) participate and publish articles or other publications.

SPHYNX TECHNOLOGY SOLUTIONS AG (hereinafter, referred as STS)

STS will contribute to the system architecture definition (T2.4), will lead WP4 in the work towards modelling and specification of the AI4HEALTHSEC Dynamic Cyber Situational Awareness framework and will also participate in its development by contributing to technical tasks of WP5. Finally, STS will contribute to the dissemination of the project results and the standardisation activities.

STS will use its links to authorities, security organizations and other related stakeholders to communicate the project, the project developments and results. STS will communicate the results and developments of the AI4HEALTHSEC project through the website and social media presence of the company. Moreover and depending on the project developments will participate in events, conferences and workshops.

TÜV TRUST IT GMBH UNTERNEHMENSGRUPPE TÜV AUSTRIA (hereinafter, referred as TUV)

Based in Cologne and Vienna, TÜV TRUST IT is the neutral, objective and independent partner for the industry with regard to information security and data privacy. TÜV TRUST IT's mission is to support companies in protecting their information assets.

TÜV TRUST IT GmbH is a daughter company of the TÜV AUSTRIA Group. The TÜV AUSTRIA Group is a leading group of companies dedicated to the provision of high quality services in the subjects of safety, security, environmental protection and health. The accredited testing, inspection, calibration, certification, verification, and notified bodies of the TÜV AUSTRIA Group are "Third Party", and meet national and international requirements for operating a testing laboratory, an inspection body (Type A), a calibration body, a certification authority, a verification centre, and a notified body.

TUV is responsible for risk and quality assurance, leading T1.4 and contributing to T4.2, T4.5. Based on its longstanding expertise it will be also leading WP8 work, mainly focusing on dissemination and standardization and certification activities.

As the leader of the Dissemination and Communication task, TUV will invest considerable efforts in the communication and dissemination of the project results and developments through all of its channels. The websites and social media accounts of TUV and the TÜV AUSTRIA Group will be appropriately utilized.

The Group's Annual Report will also be utilized to communicate the project's information and results. (TÜV AUSTRIA Group Annual Report | Jahresbericht (tuv.at)). Depending on the results of the project, TUV could also issue a relevant Whitepaper.

(e.g. https://www.tuv.at/fileadmin/user_upload/docs/group/innovation/tuv-austria-white-paper-iv-highly-automated-driving_web.pdf)

UNIVERSITY OF BRIGHTON (hereinafter, referred as UOB)

UoB will provide technical contributions to the project, through requirements and architecture specification (WP2), and Cyber Situational Awareness analysis (WP4). UoB will also contribute towards the practical evaluation of the AI4HEALTHSEC platform (T7.3, T7.4) through the provision of pilot 4 (T6.1, T6.5). Finally, UoB will support the dissemination and communication activities of the project (WP8).

UoB will communicate the progress and results of the AI4HEALTHSEC project through our website and social media accounts and through our existing large network of collaborators, partner institutions and stakeholders. Moreover, UoB plans to participate in relevant dissemination and communication events and publish articles on conferences and journals.

3.4 *AI4HEALTHSEC's dissemination plan*

As early as during the drafting of the proposal, a draft dissemination and communication plan for the AI4HEALTHSEC project was drafted. The following figure displays the different components of the dissemination and communication plan for the AI4HEALTHSEC project within the project duration.

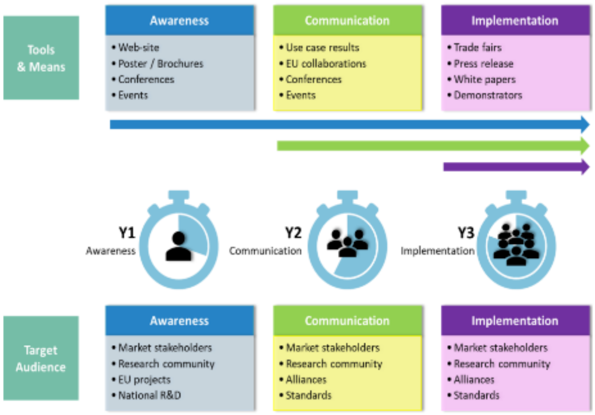


Figure 4: An overview of the Tools, means and audience of the dissemination plan of AI4HEALTHSEC project

The information shown briefly in the above figure, is described followingly in a more detailed manner.

Concept regarding the communication and dissemination objectives over time

All dissemination activities should have a purpose and should support or inform the project development in some way.
Possible options regarding the purpose of an activity may be to:

- **raise** awareness;
- extend the **impact**;
- **engage** stakeholders and target groups;
- **share** solutions and know how;
- **influence** policy and practice;
- **develop** new partnerships.

Defining the purpose of dissemination is a first step to decide on the audience, message, method, and timing of the dissemination.

The first goal of dissemination is to spread projects' results. The second goal is to contribute to the implementation and shaping of national and European policies and systems.
Communication on the other hand, is a broader concept. It includes information and promotion activities to raise awareness and enhance the visibility of the project's activities in addition to the dissemination and exploitation of the project results.
However, very often it is difficult to make a clear distinction between these areas. For this reason, planning an overall strategy framework covering both fields can be a more efficient way to make the most of the available resources. Dissemination and exploitation of results should form a crucial part of any communication activities taking place during the project's lifetime.[1]

What can be disseminated

The results of the project are of diverse nature and consist of both concrete (tangible) results as well as of skills and personal experiences that both project organisers and participants to the activities have acquired (intangible results).

Tangible results may include for example:

- an approach or a model to solve a problem;
- a practical tool or product, such as handbooks, curricula, e-learning tools;
- research reports or studies;
- good practice guides or case studies;
- evaluation reports;
- recognition certificates;
- newsletters or information leaflets.

[1] https://ec.europa.eu/programmes/erasmus-plus/book/export/html/378_en

Intangible results may include for example:

- knowledge and experience gained by participants, learners or staff;
- increased skills or achievements;
- improved cultural awareness;
- better language skills.

AI4HEALTHSEC's dissemination and communication strategy

Having considered the above, the project team has designed the following stepped process for dissemination and communication. In each step, the objective is identified and some initial methods to achieve the objectives are presented.

Since this document is drafted during month 6 of the project, it is expected to be enriched and changed throughout the duration of the project as needed. The goal is for the dissemination and communication plan to be an effective tool that will facilitate the accomplishment of the project goals.

The following table, presents the relevant activities over time:

	Objective	Methods
Raising Awareness **Year 1**	• Promote project visibility and awareness • Identification of target audience and set up the tools and branding to raise awareness about AI4HEALTHSEC • Dissemination in strategic networks of the partners. • Engaging stakeholders and target groups	• Creation of the project's logo and other components that will help create the "brand" of the AI4HEALTHSEC project (e.g. logo, color palette, fonts etc). • Creation of interactive project´s website, the information hub for the project dissemination. This website will include the last news about the project development, demonstration videos, links to download the latest outcomes, etc. • Selection among the available social media platforms and implementation of the relevant social media presence of the AI4HEALTHSEC project. • Generation of supporting material: flyers, posters, brochures etc., for use at any events and conferences attended by the different partners. • Publish press releases and liaison with relevant dissemination channels of the industry. • Develop a newsletter concept and deliver at least two newsletters within this first year. The goal of the first newsletters would be to introduce the project and increase the circle of influence of the project. • Engage the public at large through social media and communities. • Create preliminary liaison with scientific and business stakeholders • Identification and alignment of events with similar EU or national projects.

	Objective	Methods
Communication Year 2	• Communication of on-going progress, results and key achievements • Special focus on digital security, health technology and ICT industry and target potential users (year 2 of the dissemination and communication activities will build upon the progress achieved by the project during the first year. The aim is no longer to provide generic awareness and spreading the word regarding the project, but about engaging the stakeholders and other groups, sharing solutions and know how thus far extracted and developing new partnership).	• Early development of market-specific material associated with software prototypes to maximize their potential influence on the market. • Elaboration of a business whitepaper describing the AI4HEALTHSEC solution, its added value and the benefits for its different stakeholders • Publication of papers/articles in scientific journals. • Participation in both scientific and industrial events to promote the project and showcase the latest outcomes. • Organizing workshops where outcomes can be tested by interested groups. • Produce a newsletter at least twice within this second year. The goal of these newsletters would be to extend the impact of the project results, to share solutions and attract more stakeholders. (It should be noted that during month 17 of the project, a high number of deliverables are expected to be completed and thus relevant information should be communicated to all interested parties.)
Implementation Year 3	• Implementation of project´s outcomes • Generation of marketing material to target industrial stakeholders (year 3 of the dissemination and communication activities will build upon the progress achieved by the project during the first two years. After presenting the draft and initial outcomes of the AI4HEALTHSEC framework and system, the activities of this year will present the results regarding the final version of the system, the benefits and lessons learned).	• Intensify participation in events and conferences where the project´s outcomes will be showcased. • Generation of workshops / training sessions providing Demonstration of AI4HEALTHSEC benefits through the real-world use cases identified. • Publication of new press releases, generation of a commercial video, a how-to guide about project functioning, etc. • Produce a newsletter at least twice within this third year. The goal of these newsletters would be to extend the impact of the project results, to share solutions and attract more stakeholders. • Intensify the activities focusing on standardization organizations and on relevant authorities, since the Task 7.6. Policy Recommendations and Guidelines for Wider Applicability and Use is commensing on month 34. (It should be noted that during month 33 of the project, the AI4HEALTHSEC system is planned to be finalized and thus relevant information should be communicated to all interested parties.)

Table 1: AI4HEALTHSEC's dissemination and communication strategy

Target groups

The dissemination plan sets out specific, relevant target groups covering the full range of potential stakeholders of *AI4HEALTHSEC* solutions. The Key audiences in their generic form are identified in section 3.1 and are elaborated more (in terms of purpose) in the following paragraphs.

Each dissemination activity will be tailored to the specific group according to the specific message to be conveyed:

- **Industry and customers**: Dissemination will focus on the benefits to be gained by the health industry (from the several range of health sector value chain: HW chip, end-devices, SWW tools, etc.) becoming active agents of testing and developing the *AI4HEALTHSEC* solutions.
- **Local and regional government, operators & policy makers**: Dissemination will focus on developing contacts with official and policy makers that play a key role in security and health sector as well as decision-making at various levels.
- **European institutions and NGOs**: Dissemination to this group will focus on European institutions, and on other European regional bodies that are either involved in industrial business (or related) or provide relevant services for the health sector.
- **General public and user groups:** Dissemination activities will target general public (citizens, commuters, etc.) and user groups (i.e. communities active in environmental policies, citizens safety organisations and special interest groups, such as the European Cities and Regions Networking) in order to raise awareness about *AI4HEALTHSEC* solutions and encourage them to be more aware about digital security and cyber-security threats.
- **Developers and innovation communities**: Dissemination will also target independent developers and entrepreneurs in order to show the flexibility of the solutions developed by *AI4HEALTHSEC* and stimulate the creation of new, innovative and secure applications. The activities for this target group will be mainly based on the organization of and participation to specific events (e.g. innovation and technology road-show, hackathons, etc.).
- **Other European projects and initiatives**: The transfer of knowledge and experience within the whole set of the European projects in overlapping fields is a primary requirement of the *AI4HEALTHSEC* dissemination activities, so as to enhance the required unity of the European research taskforce and increase the innovation impact.
- **Scientific and research community:** Dissemination to this group will focus on disseminating the innovation on technological and business aspects. This will be done through European and international conferences/workshops, scientific newsletters, magazines, website articles, etc. Links and synergies with other regions and regional actors will also be sought.

Contacts to the above target groups are already established by the partners within the project consortium, especially for what regards the industrial partners. As such, as soon as possible, AI4HEALTHSEC results will be communicated for creating external awareness and knowledge building within the targeted industrial communities. Furthermore, relevant project results will be disseminated as early as from the first stage of development. Prototypes will also be made available to support dissemination actions, comprising both technical dissemination and presentations at sectorial events, as well as through wider demonstration activities. Dissemination and demonstration activities to health industry will take into account industrial markets of reference, selecting best and most relevant events for dissemination, and for planning demonstration activities, and these events will be mainly centered on raising awareness and transfer of knowledge, solutions, and technology.

Throughout the project lifetime, relevant dissemination and communication KPIs will be measured, monitored, analyzed and evaluated. More information can be found in section 5 (Dissemination and Communication Reporting) below.

AI4HEALTHSEC's 1st year dissemination and communication activities plan

Based on all the above, the following

<table>
<tr><th colspan="2">Website and Social Media</th><th>Scientific Publications</th></tr>
<tr><td colspan="2"><b>M1-M3:</b> Design and Development of website; Design and Development of Social Media (Facebook, Twitter, LinkedIn)
<b>M3-M12:</b> Regular update of the website content (news, public deliverables, summary of confidential deliverables…); Regular actions on Social Media (Facebook, Twitter)
<b>Monitoring Indicators (to be measured every six months*):</b>
Number of page visits to the website; Number of references to the project on search engines; Number of links/followers/interactions on Social Media
* the frequency of monitoring may change based on the project needs and relevant developments.</td><td><b>M1-M12:</b> (i) 4 scientific/academic papers; (ii) 1 academic paper covering the core of the project
<b>Monitoring Indicators (to be measured for each year):</b>
Number of papers accepted per year
Distribution per journal / top-level conference / mid-level conference publications.
Proportion of joint publications
Number of different partners authoring each paper.</td></tr>
<tr><th colspan="2">Promotional Content and Dissemination Material</th><th>Pilot Workshops</th></tr>
<tr><td colspan="2"><b>M6-M12:</b> Creation of the newsletter concept and relevant functionality in the webpage. Posting and circulation of 2 newsletters issues. At least 1 project fact sheet/brochure. At least 3 press releases
<b>Monitoring Indicators (to be measured for each year):</b>
Quantity of materials produced per year. Downloads of materials at the website / visualizations of the promotional videos.</td><td><b>M1-M12:</b> Participation in at least 2 conferences
<b>Monitoring Indicators (to be measured for each year):</b>
Number of attendees in the workshops
Number of Follow-up activities resulting from the workshops</td></tr>
<tr><th colspan="3">Relevant Scientific Journals</th></tr>
<tr><td><b>Classic Scientific Journals (ISI Indexed or equivalent)</b></td><td>IEEE Trans. on Affective Computing, IEEE Security & Privacy, International Journal of Critical Infrastructure Protection, ACM Transactions and Networking, COMPSEC – Comp. &amp; Sec.</td><td>International Journal of Disaster Risk Reduction, IEEE Control Systems Magazine, IEEE Transactions on Industrial Informatics, IEEE Transaction on Smart Grid, ACM Transactions on Cyber-Physical Systems, ACM Transactions on Information and Systems Security</td></tr>
<tr><th colspan="3">Non-exhaustive list of candidate Scientific Conferences and Workshops</th></tr>
<tr><td colspan="3">Digital Health World Congress, European Healthcare Conference, WoHIT, World of Health IT Conference & Exhibition, Conference "Computer, Privacy and Data Protection (CPDP)", Future Healthcare, Medtec Europe, ICSE, ASE, MoDELS, ESSOS, FASE, CAISE, HIMSS, ASCO, AMIA, BIBE, BIBM, ENISA eHealth Security Conference; IEEE International Conference on E-health Networking, Application & Services; CEBIT; International Conference on e-Health (MCCSIS); eHealth Forum, IAPP Europe Data Protection Congress, CPDP</td></tr>
<tr><th colspan="3">Non-exhaustive List of Fora, Associations, Initiatives and Working Groups</th></tr>
<tr><td colspan="3">Working Party on Pharmaceuticals and Medical Devices, International Medical Device Regulators Forum, C-ITS Platform working group on Security & Certification, BISA European Security Working Group, CERL Security Working group, innovation and technology road-show, hackathons</td></tr>
</table>

Table 2: AI4HEALTHSEC's 1st year dissemination and communication activities plan

Internal Communication

In order to accomplish all the above mentioned goals, internal and external dissemination activities are of paramount importance in the *AI4HEALTHSEC* project.

Internal communication: To guarantee continuous collective awareness of project goals and progress, collaboration, synchronization, and convergence of efforts. This is mainly guaranteed through the following activities:

- Presentations of work progress during periodic technical meetings (by WP leaders, and the partners involved);
- Presentation of a comprehensive overview of the project status at the beginning of each periodic general meeting (by the PC). This is intended to help all partners reach quickly at a common level of awareness on the current status of the project and the ongoing goals;
- At the start of major tasks that require specific knowledge not possessed by the majority of the consortium, the partner owning that expertise will be asked to prepare a tutorial presentation for the benefit of the other members, and thus facilitating the speed of building the needed competence level and improving future interactions;
- Sharing of documents through the “internal section” of the project’s web site; and
- Organization of web-conference to allow participants effective interactions.

4 Communication and Dissemination Activities

The communication and dissemination activities presented in this section will be executed and performed according to the communication needs of each one of the phases presented in Chapter 3. All of them will follow the branding of the project, which must be considered as a key element of the communication strategy as it reflects the soul of the project in a visual way. All partners in all communications must consider the guidelines to ensure coherence and contribute to the positioning of AI4HEALTHSEC among stakeholders.

This section is dedicated on the components of the “brand” of the AI4HEALTHSEC project. The “brand” is more than a single logo, but rather is a cohesive set of components that correlate and together create a story. The components of the “brand” of the AI4HEALTHSEC project are:

- The logo
- The colours
- The layout of the documents
- The pictures used
- The fonts
- The language

Below you may find more information for each one of these components. The details provided try to convey the concept that each choice will reflect. The exact way that these components will be applied, will depend each time on the specific communication and dissemination activity.

4.1 *Logo*

The Logo features a (robotic) head containing the representation of a circuit where the brain is positioned. The combination of these figures is a common representation of the Artificial Intelligence concept. The name of the project is depicted at the bottom of the head in bold letters of alternating colors. The Health and Sec (=Security) words are represented in different colors drawing the focus on both concepts. The logo of the project is meant to inform the various audiences that this is a project that refers to the Security in the Health sector using artificial intelligence.

The logo displayed below represents the selection found by the project team to best represent the objectives and scope of this project. During the design phase, other logos were proposed to the project partners (more information regarding the communication, the options and the results of the voting process is shown in Annex A.)

The project logo on different versions is available for all partners at the repository:

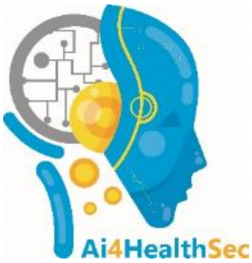


Figure 5: The AI4HEALTHSEC Logo

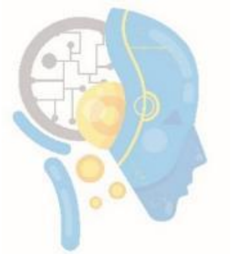


Figure 6: The AI4HEALTHSEC Washed-out Logo

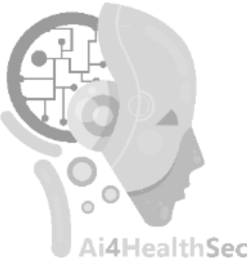


Figure 7: The AI4HEALTHSEC BW Logo for dark background

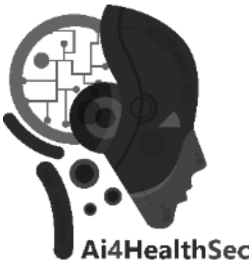


Figure 8: The AI4HEALTHSEC BW Logo for light coloured background

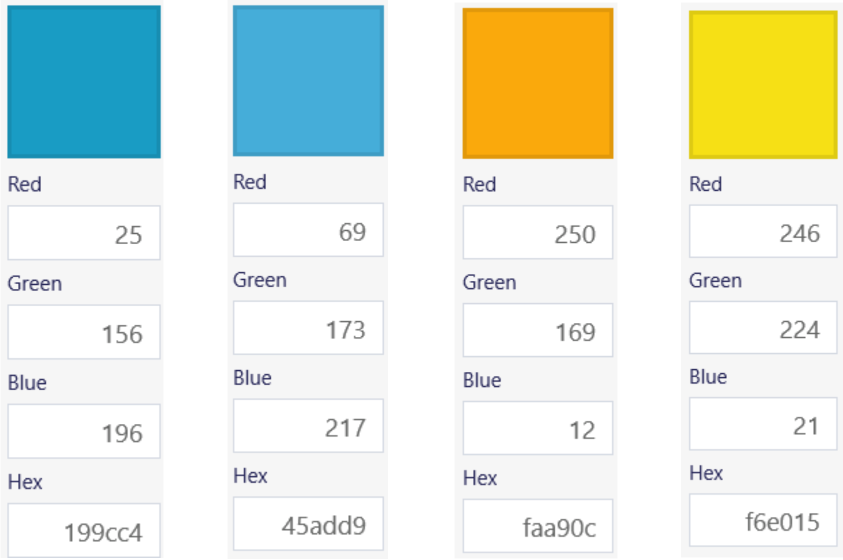
Since the colours of the logo are vivid, the logo could be displayed also on a dark background. The result (depending on the colour of the background) could be less than optimum at cases. If the use of dark background cannot be avoided, either the washed-out version of the logo should be used or the all white one (depicted above as BW Logo for dark coloured background).

4.2 *Colors*

Based on the logo, the colour pallet of all project communication and dissemination activities are determined.

Blue and yellow (in two different shades) are the predominant colours of the "brand" of the AI4HEALTHSEC project.

Below, the RGB and Hex settings of the colours are shown:



Red	25	69	250	246
Green	156	173	169	224
Blue	196	217	12	21
Hex	199cc4	45add9	faa90c	f6e015

Figure 9: RGB and Hex settings of the basic colors

4.3 *Document Layout*

It is important, for the be communication of the project activities, to use a homogenized structure of the documents and the deliverables of the project.

A document template has been created, featuring the components of "brand" of the AI4HEALTHSEC project as described above (e.g. Logos, elements in the basic colours, fonts, tables etc)

The template for the main deliverable documents is presented below:

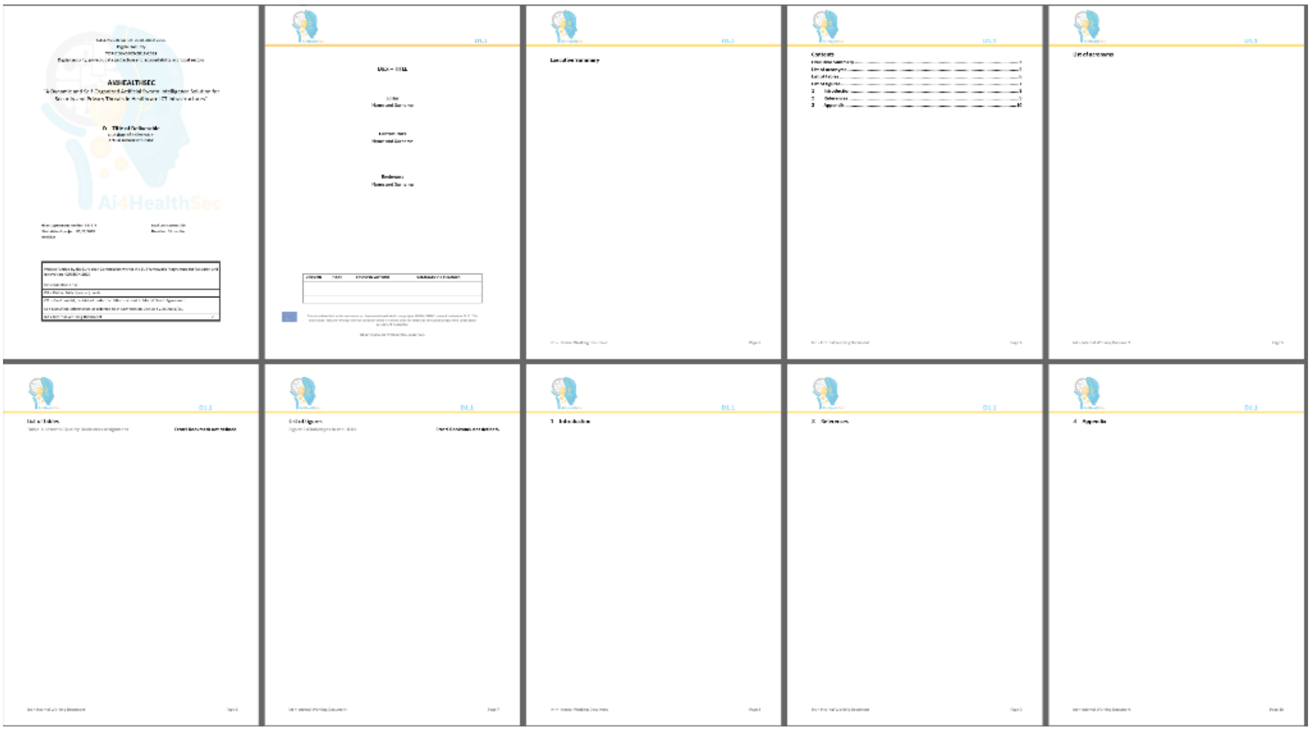
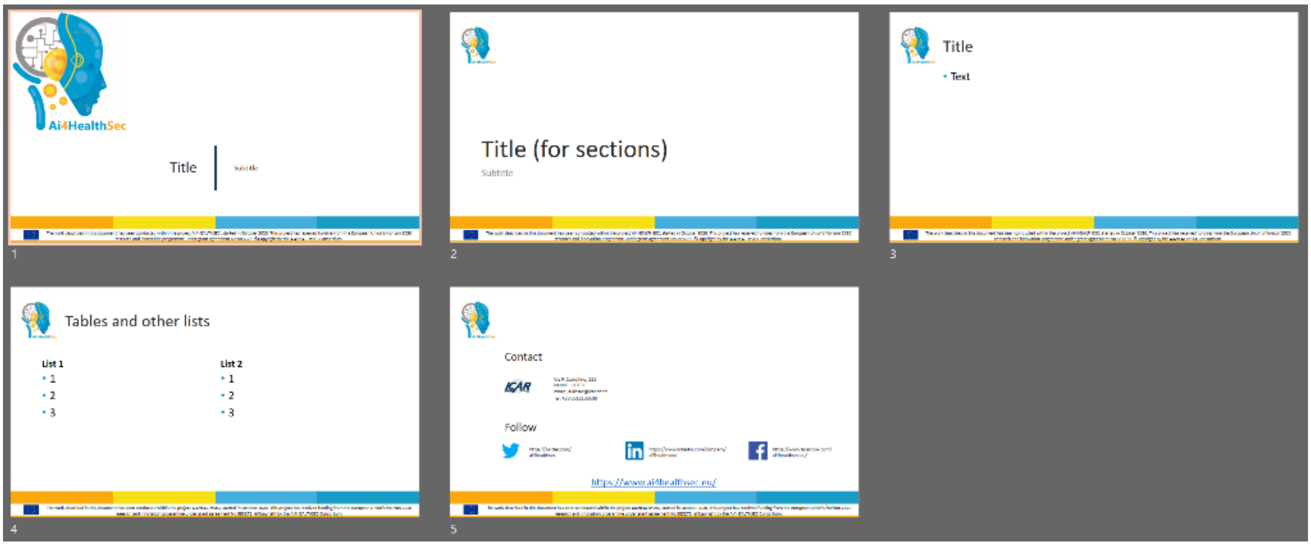


Figure 10: Deliverable template

Similarly, the template for a presentation is presented below:



Ai4HealthSec

Title | Subtitle

Title (for sections)

Subtitle

Title

- Text

Tables and other lists

List 1

- 1
- 2
- 3

List 2

- 1
- 2
- 3

Contact

Follow

https://www.ai4healthsec.eu/

Figure 11: Presentation template

Based on the needs of the project, other templates will be similarly created and stored in the relevant space of the Basecamp platform of the project.

4.4 *Pictures*

Pictures will be used in many of the communication and dissemination materials of the AI4HEALTHSEC project (e.g. the website, the brochures, the newsletter, the social media, etc).

These pictures are selected adhering to the following rules:

- The picture should convey the message or topic in a professional manner
- The source of the picture should be identified and the copyright provisions (e.g. attributes) respected (pictures of unknown origin or questionable copyright rules shall not be used).
- The search for pictures will be facilitated through well known platforms based on key words related to the project and the intended message. Some of these keywords and a selection of relevant pictures is displayed below.

4.5 *Fonts*

The project team has selected Calibri as the preferred font, to be used in official communications. This does not mean that another font cannot be selected for specific messages, if it is found to be more fitting (in relation to the purpose of the communication and the rest of the creative components).

The templates mentioned above have predetermined styles incorporating the Calibri font and allowing the authors to systematically use the correct fonts and outline settings.

For example, the following Styles have been created for the basic template and presentation:

- Main Body: Example (Calibri 12)
- Heading 1: **Example**
- Heading 2: ***Example***
- Heading 3: **Example**
- Heading 4: **Example**
- Heading 5: ***Example***
- Intense Emphasis: *Example*
- Bullets: •

4.6 *The language*

The official language of all communication and dissemination activities of the AI4HEALTHSEC project is English.

The project partners originate from the following countries:

Italy, the Netherlands, Germany, Greece, Belgium, Switzerland, United Kingdom, Portugal and France.

Each partner may choose to translate the project's messages and communications to their native languages if desired.

Finally, the project partners will use appropriate language within each communication and dissemination activity taking into consideration the targeted audience (e.g. degree of technical jargon to be used, level of detail etc).

4.7 *The funding information*

As mentioned in the Grant Agreement, any communication activity related to the project (including in electronic form, via social media, etc.) and any infrastructure, equipment and major results funded by the grant must:

(a) display the EU emblem

and (b) include the following text:

For communication activities:
“This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273”.
For infrastructure, equipment and major results:
“This [infrastructure][equipment][insert type of result] is part of a project that has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883273”.

4.8 *AI4HEALTHSEC Website*

The AI4HEALTHSEC website has been available since M3 of the project at https://www.ai4healthsec.eu/. This website was created in order to present the project and the relevant information related to the project, such as the partners involved in the project, the objectives of the project, the challenges and the impact for the implementation of the project. It will also provide ongoing information on project activities such as events, meetings, etc. and disseminate the public deliverables of the project, relevant publications and presentations.

The website has been developed by CNR and will as well be managed and updated regularly according to the communication needs of each stage of the communication plan by CNR and by APIROPLUS SOLUTIONS.
The website, in its initialversion, has the following options and information:

- **Homepage:** Offers a comprehensive view of the sections of the website and the content available. It includes the challenges and the impact of the project and it also features the icons and links to the project social media accounts such as Twitter, Facebook and LinkedIn. Finally, the footer includes the disclaimer of the EC that contains the Grand Agreement number.

- **Project:** Presents and provides a description of the project and other relevant information such as the duration of the project.
- **Partners:** Includes information about the consortium partners such as logo, name, location and partner web site.
- **Events:** Provides information on events and meetings that have taken place.
- **Contact us:** Provides information and contact details about the project coordinators.

During month 6 of the project, the structure of the website will be expanded to contain also the following:

- **Newsletter**: The newsletter will be one of the channels used by the AI4HEALTHSEC project in order to communicate with the various interested parties. A campaign is planned for month 7, during which subscriptions will be collected internally and externally. The first newsletter is planned for circulation on month 8 (containing a brief introduction of the AI4HEALTHSEC project) and another one on month 11 (containing some developments of the project). The website will contain an archive of the newsletters and a form where a person can subscribe to the newsletter. The terms for the subscription along with the privacy policy will be finalized in collaboration with the project's DPO and responsible for Task 1.6. Ethical, Privacy, GDPR Compliance and Security Coordination (PN).
- **Deliverables**: The website will contain a list of the deliverables of the project that based on their classification level are allowed to be publicly available. (During the time that this document was being drafted, only one Deliverable has been completed (D1.1. Project Management Handbook – classification CO), so there are no related entries so far. At the end of the document (Appendix C), there is a list of all expected deliverables of the AI4HEALTHSEC project, accompanied by information on the classification / dissemination level and the project month each of them is due.
- **Publications**: As mentioned already in Section 3, one of the envisioned channels for the dissemination of the information, developments and outcomes of the AI4HEALTHSEC project, is the publication of articles and white papers. Such documents will be posted within this section of the website when available. (The applicable copyright rules will be adhered for every individual case).

Privacy policy and privacy considerations

At this point, the website does not retain any personal information (there are no cookies used).

As mentioned before, the terms for the subscription to the newsletter along with the privacy policy will be finalized in collaboration with the project's DPO and responsible for Task 1.6. Ethical, Privacy, GDPR Compliance and Security Coordination (PN). This is expected to end by the end of month six. After this period, necessary cookies will be activated allowing for (amongst others) the monitoring of the impact of the website.

4.9 *Social Media*

Social media will help raise awareness and recognition of the project as well as to disseminate information as widely as possible. As mentioned above, in 3.2 Communication and Dissemination Channels and Activities, AI4HEALTHSEC has established (Project Month 3) accounts in three social media platforms (Facebook, Twitter, LinkedIn).

Since some of the platforms do not allow numbers within the account names, the following accounts were created:

Platform	Account Name	Link
f	Aifourhealthsec Eu	https://www.facebook.com/aifourhealthsec.eu
🐦	@aifourhealthsec	https://twitter.com/aifourhealthsec
in	Aifourhealthsec Eu	https://www.linkedin.com/in/aifourhealthsec-eu

4.10 *Communication Material*

It is the decision of the project team to avoid (to the degree possible) using printed communication and dissemination material.

If and when needed, such material will be created and printed following the basic rules described within this document.

During the project lifetime, digital communication and dissemination material will be designed, created and circulated to fulfil the relevant needs of the project.

So far, the development of material has been focused on templates to be used by the consortium, but the plan for the first year foresees the development of a newsletter.

For the complete duration of the project, the AI4HEALTHSEC project will produce at least 2 newsletters per year and any other material of various forms (video, brochures, etc).

The templates created are already presented in section 4.3 above.

4.11 *Journal Publications, Scientific Papers and Conferences*

As mentioned above, the development and publication of scientific papers and white papers in specialized magazines, journals, and conferences is an essential activity to attract the attention of interested and related parties within the development and results of the AI4HEALTHSEC project. Therefore, AI4HEALTHSEC consortium will seek to publish this kind of scientific content on several international refereed, scientific and technical journals and conferences in security, such as:

Journals	Link
IEEE Transactions on Affective Computing	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5165369
IEEE Security & Privacy	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
International Journal of Critical Infrastructure Protection	https://www.journals.elsevier.com/international-journal-of-critical-infrastructure-protection
IEEE/ACM Transactions on Networking	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=90
Computers & Security	https://www.journals.elsevier.com/computers-and-security
International Journal of Disaster Risk Reduction	https://www.journals.elsevier.com/international-journal-of-disaster-risk-reduction
IEEE Control Systems magazine	http://ieeecss.org/publication/ieee-control-systems-magazine
IEEE Transactions on Industrial Informatics	http://www.ieee-ies.org/pubs/transactions-on-industrial-informatics
IEEE Transaction on Smart Grid	https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=5165411
ACM Transactions on Cyber-Physical Systems	https://dl.acm.org/journal/tcps
ACM Transactions on Information and System Security	https://www.scimagojr.com/journalsearch.php?q=28875&tip=sid

Table 3: AI4HEALTHSEC's indicative targeted scientific and technical journals for submission

Conferences	Link
Digital Health World Congress	https://digitalhealthcareworldcongress.com/
17th World Congress on Healthcare & Technologies	https://europe.healthconferences.org/
WoHIT - The World of Health IT Conference & Exhibition 2022	https://www.himss.org
CPDP2022	https://www.cpdpconferences.org/
Critical Infrastructure Protection & Resilience Europe 2021	https://www.cipre-expo.com/?ref=infosec-conferences.com
7th International Conference on Artificial Intelligence and Security (ICAIS 2021)	https://www.icaisconf.com/?ref=infosec-conferences.com
HEALTHINF 2022	http://www.healthinf.biostec.org/
AIME 2022 : Artificial Intelligence in Medicine in Europe	http://aime21.aimedicine.info/
2021 European Researcher's Night – NTUA - Greece	https://www.ece.ntua.gr/en/article/435
2021 European Researcher's Night - FORTH	https://www.ics.forth.gr/

Conferences	Link
CRITIS: International Conference on Critical Information Infrastructures Security	https://critis2021.org/call-for-papers/
43rd IEEE Symposium on Security and Privacy	http://www.ieee-security.org/TC/SP2022/cfpapers.html
ENISA - eHealth Security Conference	https://www.enisa.europa.eu/events/ehealth-security-conference-2020-online-series
IEEE International Conference on E-health Networking, Application & Services	https://healthcom2020.ieee-healthcom.org/
International Conference on Information Security and Privacy Protection	https://www.ifipsec.org/
InfoSec	https://www.infosecurityeurope.com/
15th Multi Conference on Computer Science and Information Systems	https://mccsis.org/
IAPP Europe Data Protection Congress 2021	https://iapp.org/conference/iapp-europe-data-protection-congress/
The future health summit	https://futurehealthsummit.com/
The MedTech Forum 2021	https://www.medtecheurope.org/
43rd International Conference of Software Engineering	https://conf.researchr.org/home/icse-2021
MODELS 2021: ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MODELS)	http://www.modelsconference.org/
7th Network and Information Security (NIS'21) Summer School	https://nis-summer-school.enisa.europa.eu/

Table 4: AI4HEALTHSEC's indicative targeted conferences

Although dates are mentioned in the entries in Table 4, it should be noted that the information above is only given as an indicative list and a possible participation and presentation within these conferences will depend on the progress of the work carried out within the project.

A special space will be created within Basecamp within month 7, that will contain a list of the participations to the events as well as entries for upcoming events, workshops and conferences.

Lastly, AI4HEALTHSEC will create a maintain links to several related European funded projects, and will participate in relevant events, workshops and conferences (based on the affinity of the subjects and the developments of the project).

An indicative list of such project is contained in the table below:

Acronym	Title	Teaser	URL
PANACEA	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people	PANACEA will deliver people-centric cybersecurity solutions in healthcare. The Partners will execute on a leanly-orchestrated research workplan, which envisages continuous involvement of the end-user Partners at three European health care centres, including also devices...	https://cordis.europa.eu/project/id/826293
cyberwatching.eu	The European watch on cybersecurity privacy	"cyberwatching,eu addresses the DS-05 call by defining and promoting a pragmatic approach to implement and maintain an EU Observatory to monitor R&I initiatives on cybersecurity & privacy, throughout EU & Associated Countries. These initiatives will be clustered, with a...	https://cordis.europa.eu/project/id/740129

Acronym	Title	Teaser	URL
CUREX	seCUre and pRivate hEalth data eXchange	The Health sector is increasing dependence on digital information and communication infrastructures renders it vulnerable to threats to privacy and cybersecurity, especially as the theft of health data has become particularly lucrative for cyber criminals. At the same time, a...	https://cordis.europa.eu/project/id/826404
CyberSec4Europe	Cyber Security Network of Competence Centres for Europe	CyberSec4Europe is a research-based consortium with 44 participants covering 21 EU Member States and Associated Countries. It has received more than 40 support letters and promises of cooperation from public administrations, international organisations, and key associations...	https://cordis.europa.eu/project/id/830929
SPARTA	Strategic programs for advanced research and technology in Europe	In the domain of Cybersecurity Research and innovation, European scientists hold pioneering positions in fields such as cryptography, formal methods, or secure components. Yet this excellence on focused domains does not translate into larger-scale, system-level advantages...	https://cordis.europa.eu/project/id/830892
SecureHospitals.eu	Raising Awareness on Cybersecurity in Hospitals across Europe and Boosting Training Initiatives Driven by an Online Information Hub	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...	https://cordis.europa.eu/project/id/826497
ASCLEPIOS	Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare	The vision of ASCLEPIOS is to maximize and fortify the trust of users on cloud-based healthcare services by developing mechanisms for protecting both corporate and personal sensitive data. The core idea of the project is derived from two observations. The first is based on an...	https://cordis.europa.eu/project/id/826093
ProTego	Data-protection toolkit reducing risks in hospitals and care centers	Health care is an essential service that uses a great deal of sensitive personal data which has a high black market value being a lucrative target for data theft and ransomware attacks. The EU NIS Directive (EU 2016/1148) and GDPR (EU 2016/679) will harmonize and improve...	https://cordis.europa.eu/project/id/826284
HEIR	A SECURE HEALTHCARE ENVIRONMENT FOR INFORMATICS RESILIENCE	The health sector is steadily becoming the de facto target for cyberattacks. Based on the most recent ENISA report at the end of 2018, cybersecurity incidents have shown that the healthcare sector is one of the most vulnerable. Focusing specifically on Electronic Medical...	https://cordis.europa.eu/project/id/883275
SPHINX	A Universal Cyber Security Toolkit for Health-Care Industry	Hospitals and care centres are prime targets for cyber criminals, especially concerning data theft, denial-of-service and ransomware. This reflects the need of Healthcare Institutions for a Holistic Cyber Security vulnerability assessment toolkit, that will be able to...	https://cordis.europa.eu/project/id/826183
AI4HEALTHSEC	A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures	The increasing interconnection of technology in healthcare between devices at the physical and cyber levels has transformed these infrastructures into large Health Care Information Infrastructures. Such HCIIs are considered critical and sensitive infrastructures due to their...	https://cordis.europa.eu/project/id/883273
X-eHealth	X-eHealth: eXchanging electronic Health Records in a common framework	X-eHealth project stands herein for a project of strategic relevance for tomorrow European eHealth Union. Assembling at the time of this proposal submission a shared commitment of 47 health actors, the underlying idea of this project is to develop the basis for a...	https://cordis.europa.eu/project/id/951938
SERUMS	Securing Medical Data in Smart Patient-Centric Healthcare Systems	In order to achieve high quality healthcare provision, it is increasingly important to collect highly confidential and personal medical data that has been obtained from a variety of sources, including personal medical devices and to share this through a variety of...	https://cordis.europa.eu/project/id/826278

Acronym	Title	Teaser	URL
SIMARGL	Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware	With the prevailing risk of cybersecurity breaches, improving the cyber security posture and detection algorithms is of utmost importance. Malware is now recognized as the severe threat for commercial and critical IT systems (e.g. financial sector) , but also for citizens...	https://cordis.europa.eu/project/id/833042
DEFeND	Data Governance for Supporting GDPR	The rapid advances in ICT have raised the need to adapt to this progress for organisations (pushing them towards e-services and increase their efficiency), public authorities (stimulating new services to citizens and reducing complexity) and individuals (enabling them to...	https://cordis.europa.eu/project/id/787068
PANELFIT	Participatory Approaches to a New Ethical and Legal Framework for ICT	Changes in the regulation of ICT research and innovation are opening up a new scenario. It is expected that stakeholders, policy makers, and end users adapt to them as soon as possible. This, however, might be hard, especially for SMEs. PANELFIT is firmly committed to...	https://cordis.europa.eu/project/id/788039
CyberSANE	Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures	In the digital era, Critical Infrastructures (CIs) are operating under the premise of robust and reliable ICT components, complex ICT infrastructures and emerging technologies and are transforming into Critical Information Infrastructures (CIIs) that can offer a high degree of...	https://cordis.europa.eu/project/id/833683
CitySCAPE	CitySCAPE: City-level Cyber-Secure Multimodal Transport Ecosystem	With the emergence of the digitization of information, ICT infrastructure and communications gave an unprecedented push towards the realization of truly interconnected passenger transport ecosystems at city-level. The emerging notion of multimodality supports a plethora of...	https://cordis.europa.eu/project/id/883321
SOTER	cyberSecurity Optimization and Training for Enhanced Resilience in finance	The Digitalization Era implies many advantages for businesses and citizens. However, new threats arise, especially in what concerns data privacy and the use of digital identities. These threats must be tackled under a holistic approach and pointing at their different origins...	https://cordis.europa.eu/project/id/833923
NearUS	Network for European Research and Innovation acceleration in the US	NearUS aims at establishing a Butterfly Network of Centres of European Research and Innovation as central contact point for support to EU research and innovation (R&I) actors seeking collaboration with and in the US. The NearUS Network/Centre will be coordinated through two...	https://cordis.europa.eu/project/id/733286
CyberKit4SME	Democratizing a Cyber Security Toolkit for SMEs and MEs	CyberKit4SME aims to democratize a kit of cyber security tools and methods enabling SMEs/MEs to: Increase awareness of cybersecurity risks, vulnerabilities and attacks; Monitor and forecast risks; Manage risks using organisational, human and technical security measures with...	https://cordis.europa.eu/project/id/883188
PDP4E	Methods and tools for GDPR compliance through Privacy and Data Protection Engineering	PDP4E is an innovation action that will provide software and system engineers with methods and software tools to systematically apply data protection principles in the projects they carry out, so that the products they create comply with the General Data Protection Regulation...	https://cordis.europa.eu/project/id/787034
AERAS	A CybEr range tRaining platform for medicAl organisations and systems Security	AERAS aims to develop a realistic and rapidly adjustable cyber range platform for systems and organisations in the critical healthcare sector, to effectively prepare stakeholders with different types of responsibility and levels of expertise in defending high-risk, critical...	https://cordis.europa.eu/project/id/872735
BRAINTEASER	BRinging Artificial INTelligencE home for a better cAre of amyotrophic lateral sclerosis and multiple SclERosis	Amyotrophic Lateral Sclerosis (ALS) and Multiple Sclerosis (MS) are chronic diseases characterized by progressive or alternate impairment of neurological functions (motor, sensory, visual, cognitive). Patients have to manage alternated periods in hospital with care at home...	https://cordis.europa.eu/project/id/101017598

Acronym	Title	Teaser	URL
CONCORDIA	Cyber security cOmpeteNce fOr Research anD Innovation	Europe needs to step up its efforts and strengthen its very own security capacities to secure its digital society, economy, and democracy. It is time to reconquer Europe's digital sovereignty. The vision for Europe can only be to join forces across Europe's research...	https://cordis.europa.eu/project/id/830927

Table 5: AI4HEALTHSEC indicative list of possible related European funded projects

5 Dissemination and Communication Reporting

This chapter presents the KPIs established to have quantitative measures regarding the effectiveness of the communication and dissemination plan of AI4HEALTHSEC described in this deliverable. The continuous measurement and reporting of activities will allow the project team to determine if the current strategy and plans are effective or not. Moreover, the KPI values will allow the project team to determine if new actions or plans should be designed and implemented in order to effectively achieve the objectives of the project.

Description of the KPI	KPI target
The % of tasks, etc. completed on time according to the action plan.	>=95%
The existence of a well-established and functioning community	>=10 members (at least)
Number of periodic meeting.	>=6 general meeting
Number of workshops.	>=3
Number of contributions to roadmaps, discussion papers:	>=2
Number of contribution to policy-makers:	>=2
Number of external workshops, seminars, etc. attended:	>=10
Number of press releases issued:	>=4
Number of registered members of the project's website:	>=50
Number of journal publications:	>=8
Number of conference papers and presentations:	>=10
Number of events attended:	>=15

Table 6: AI4HEALTHSEC Dissemination and Communication KPIs

A list and a dedicated space is retained within the Basecamp platform containing all the information to facilitate the monitoring and reporting the above mentioned KPIs.

6 Appendix A

AI4HEALTHSEC Partners Websites and Social media accounts

Partner Name	Website	Social media accounts
National Research Council	http://www.icar.cnr.it/	Facebook: @ComunicazioneICAR Twitter: @ICAR_CNR LinkedIn: ICAR-CNR
Philips Electronics Nederland B.V.	http://www.philips.com/	Facebook: @Philips Twitter: @Philips
Klinikum Nuernberg	https://www.klinikum-nuernberg.de/EN/index.html	Facebook: @Klinikum.Nuernberg Twitter: @KlinikumNbg
EBIT S.r.l. – ESAOTE Group	http://www.esaote.com/it-IT/healthcare-it/	Facebook: @EsaoteGroup LinkedIn: Esaote
Foundation for Research and Technology – Hellas	http://www.forth.gr/	Facebook: @FORTH.ITE Twitter: @FORTH_ITE LinkedIn: Foundation for Research and Technology - Hellas (FORTH)
TÜV TRUST IT GMBH UNTERNEHMENSGRUPPE TÜV AUSTRIA	https://it-tuv.com/	Facebook: @TUEVAUSTRIA Twitter: @tuevtrustit LinkedIn: TÜV TRUST IT Unternehmensgruppe TÜV AUSTRIA
FOCAL POINT	https://www.focalpoint-sprl.be/	Facebook: @focalpointsprl Twitter: @focalpointsprl
Fraunhofer Gesellschaft zur Förderung der Angewandten Forschung e.V.	https://www.ibmt.fraunhofer.de/	Facebook: @fraunhoferde Twitter: @Fraunhofer LinkedIn: Fraunhofer-Gesellschaft
SPHYNX TECHNOLOGY SOLUTIONS AG	http://www.sphynx.ch/	Facebook: @SPHYNXTS Twitter: @SPHYNXTS
University of Brighton	http://www.brighton.ac.uk/	Facebook: @universityofbrighton Twitter: @uniofbrighton LinkedIn: University of Brighton
Projecto Desenvolvimento Manutenção Formação e Consultadoria	http://www.pdmfc.com/	Facebook: @PDMFC Twitter: @PDMFC LinkedIn: PDMFC
AEGIS IT RESEARCH UG	http://aegisresearch.eu/	Facebook: @AEGISITCompany Twitter: @AegisITResearch LinkedIn: AEGIS IT RESEARCH
Privanova SAS	http://www.privanova.com/	LinkedIn: Privanova
INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	http://www.iccs.gr/	Facebook: Institute of Communications and Computer Systems Twitter: @IccsNtua LinkedIn: ICCS – NTUA

Table 7: AI4HEALTHSEC's Partners Websites and Social media accounts

7 Appendix B

Process followed for the design and selection of the AI4HEALTHSEC Logo.

During the initial discussions of the project management team, the basic ideas and concepts that represented the AI4HEALTHSEC project were discussed.

Followingly, the relevant team of the partners TUV and CNR created 8 different logos.

(In all the instantiations of our logo we chose to include a connection to Artificial intelligence or Health or IT or the holistic approach to security that the project is trying to convey)

Figure 7 contains the different options:

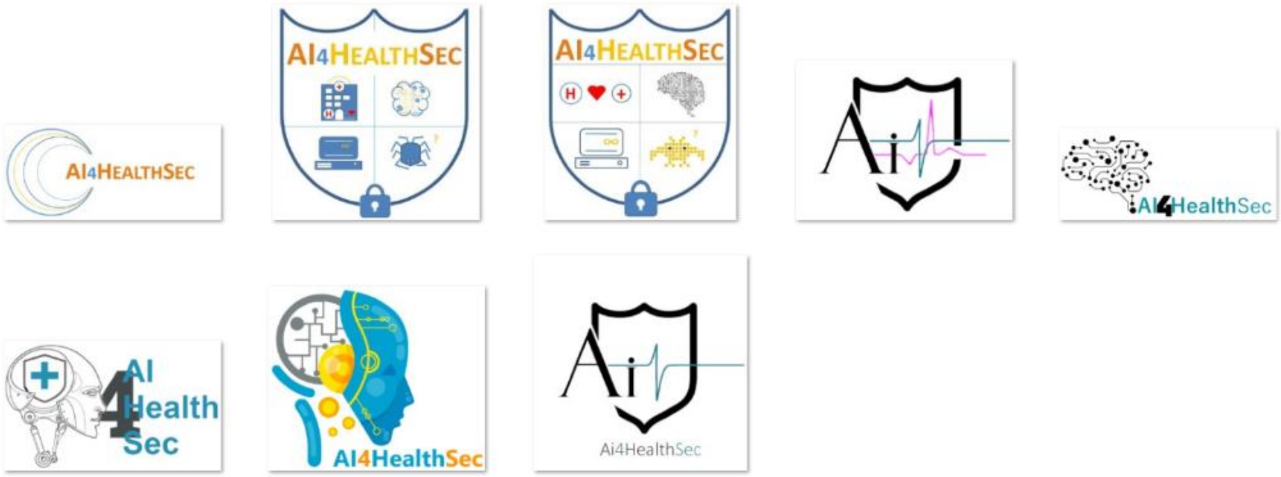
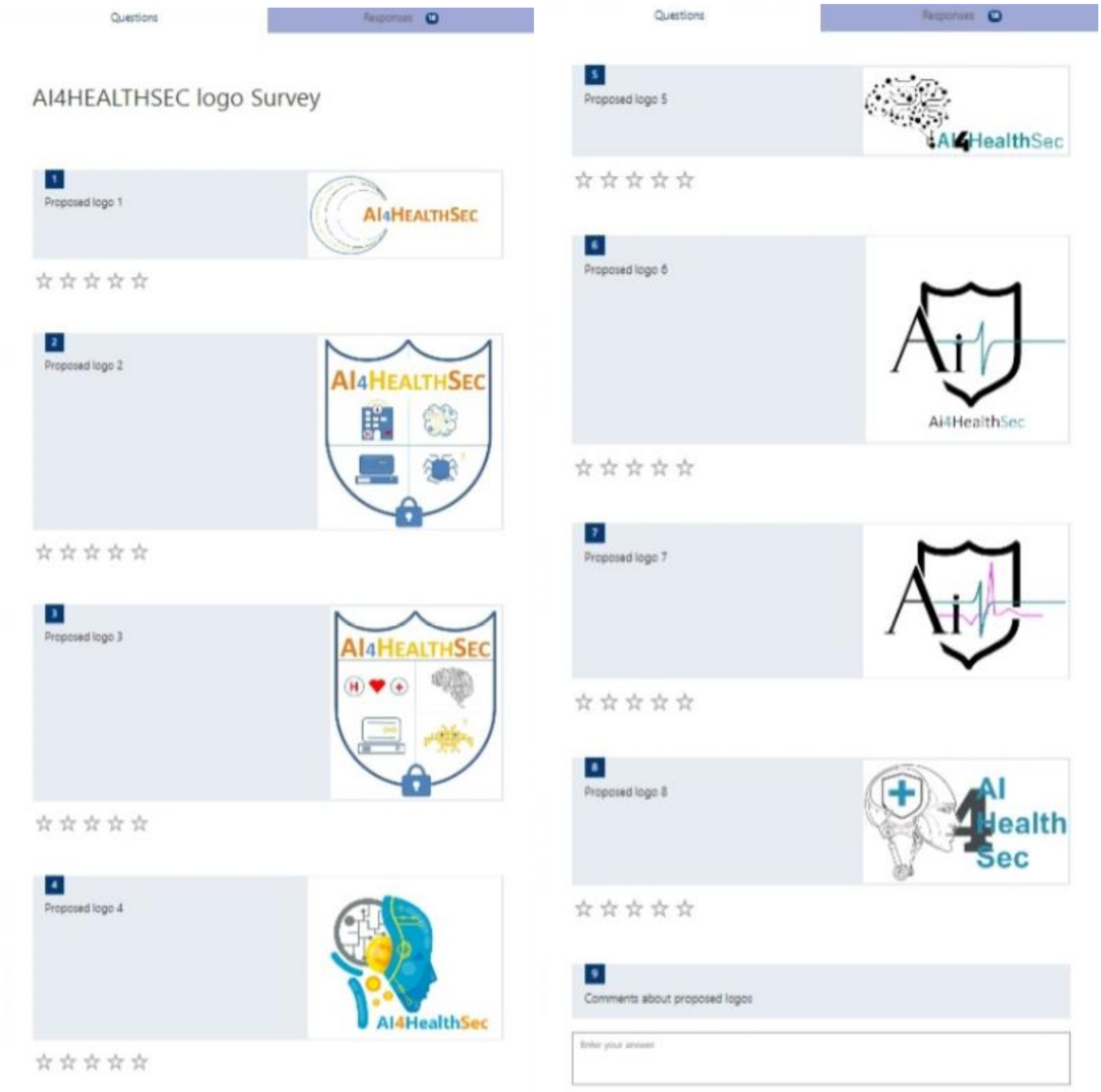


Figure 12: AI4HealthSec proposed logos

Through an internal email communication, AI4HEALTHSEC contact persons, were asked to rate the logos through https://forms.office.com platform.



Questions Responses

AI4HEALTHSEC logo Survey

1
Proposed logo 1

☆ ☆ ☆ ☆ ☆

2
Proposed logo 2

☆ ☆ ☆ ☆ ☆

3
Proposed logo 3

☆ ☆ ☆ ☆ ☆

4
Proposed logo 4

☆ ☆ ☆ ☆ ☆

Questions Responses

5
Proposed logo 5

☆ ☆ ☆ ☆ ☆

6
Proposed logo 6

☆ ☆ ☆ ☆ ☆

7
Proposed logo 7

☆ ☆ ☆ ☆ ☆

8
Proposed logo 8

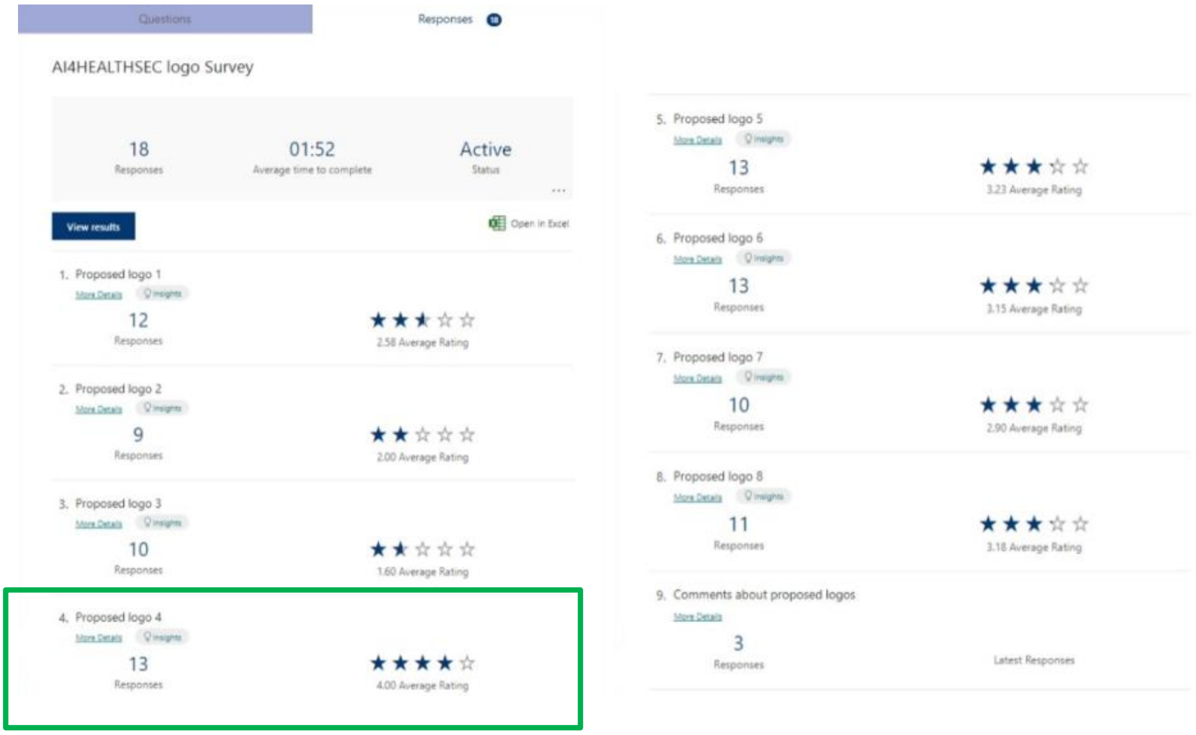
☆ ☆ ☆ ☆ ☆

9
Comments about proposed logos

Enter your answer

Figure 13: Voting page - logos

The results of the voting are depicted in Figure 9.



AI4HEALTHSEC logo Survey

18 Responses | 01:52 Average time to complete | Active Status

1. Proposed logo 1
12 Responses | 2.58 Average Rating

2. Proposed logo 2
9 Responses | 2.00 Average Rating

3. Proposed logo 3
10 Responses | 1.60 Average Rating

4. Proposed logo 4
13 Responses | 4.00 Average Rating

5. Proposed logo 5
13 Responses | 3.23 Average Rating

6. Proposed logo 6
13 Responses | 3.15 Average Rating

7. Proposed logo 7
10 Responses | 2.90 Average Rating

8. Proposed logo 8
11 Responses | 3.18 Average Rating

9. Comments about proposed logos
3 Responses | Latest Responses

Figure 14: AI4HEALTHSEC logo voting results

8 Appendix C

The following table contains all planned deliverables of the AI4HEALTHSEC project along with their Classification / Dissemination level and the project month they are due.

R. No	Title	Lead	Type	Diss.	Due Date
D1.1	Project management handbook	CNR	R	CO	4
D1.2	Risk Identification and Management & Privacy and Quality plan	CNR	R	CO	6
D1.3	Periodic activity report version 1	CNR	R	CO	12
D1.4	Periodic activity report version 2	CNR	R	CO	18
D1.5	Periodic activity report version 3	CNR	R	CO	36
D1.6	Ethics, Privacy, Security and Data Management Plan	PN	R	CO	6
D1.7	Public Final management report	CNR	R	CO	36
D2.1	AI4HEALTHSEC Requirements and Research Directives	KLINIK	R	PU	6
D2.2	Legal and Ethical Requirements	PN	R	PU	6
D2.3	User and Stakeholders Reference Scenarios and *AI4HEALTHSEC* evaluation metrics and criteria principl	EBIT	R	PU	8
D2.4	System architecture and technical specifications	AEGIS	R	CO	8
D3.1	Self-organized Swarm Intelligence Model version 1	FP	R	CO	12
D3.2	Self-organized Swarm Intelligence Model version 2	FP	R	CO	24
D3.3	Privacy, Data Protection and Visualisation Schemes Specification version 1	PDMFC	R	CO	12
D3.4	Privacy, Data Protection and Visualisation Schemes Specification version 2	PDMFC	R	CO	24
D4.1	1st Horizontal Layer Specifications version 1	STS	R	CO	12
D4.2	1st Horizontal Layer Specifications version 2	STS	R	CO	24
D4.3	2nd, 3rd and 4th Horizontal Layer Specifications version 1	STS	R	CO	12
D4.4	2nd, 3rd and 4th Horizontal Layer Specifications version 2	STS	R	CO	24
D4.5	Cyber-Attack Forecasting & Security Incident Simulation Specifications	FP	R	CO	16
D5.1	Fully Implemented 1st Vertical Layer Report version 1	AEGIS	R	CO	17
D5.10	Fully Implemented 2nd Vertical Layer version 1	PDMFC	DEM	CO	17
D5.11	Fully Implemented 2nd Vertical Layer Report version 2	PDMFC	R	CO	30
D5.12	Fully Implemented 2nd Vertical Layer version 2	PDMFC	DEM	CO	30
D5.13	Fully Implemented 2nd, 3rd and 4th Horizontal Layers Report version 1	FORTH	R	CO	17
D5.14	Fully Implemented 2nd, 3rd and 4th Horizontal Layers version 1	FORTH	DEM	CO	17
D5.15	Fully Implemented 2nd, 3rd and 4th Horizontal Layers Report version 2	FORTH	R	CO	30
D5.16	Fully Implemented 2nd, 3rd and 4th Horizontal Layers version 2	FORTH	DEM	CO	30
D5.17	Cyber-Attack Forecasting & Security Incident Simulator Report	CNR	R	CO	30
D5.18	Cyber-Attack Forecasting & Security Incident Simulator	CNR	DEM	CO	30
D5.2	Fully Implemented 1st Vertical Layer version 1	AEGIS	DEM	CO	17
D5.3	Fully Implemented 1st Vertical Layer Report version 2	AEGIS	R	CO	30
D5.4	Fully Implemented 1st Vertical Layer version 2	AEGIS	DEM	CO	30
D5.5	Fully Implemented 1st Horizontal Layer Report version 1	PHILIPS	R	CO	17
D5.6	Fully Implemented 1st Horizontal Layer version 1	PHILIPS	DEM	CO	17
D5.7	Fully Implemented 1st Horizontal Layer Report version 2	PHILIPS	R	CO	30
D5.8	Fully Implemented 1st Horizontal Layer version 2	PHILIPS	DEM	CO	30
D5.9	Fully Implemented 2nd Vertical Layer Report version 1	PDMFC	R	CO	17
D6.1	Implementation strategy and evaluation plan	FHG-IBMT	R	CO	17
D6.2	Pilot Preliminary Integration and Validation report	KLINIK	R	CO	21
D6.3	Pilot Final Integration and Validation report	EBIT	R	CO	33
D7.1	Fully Implemented 3rd Vertical Layer Report version 1	PHILIPS	R	CO	17
D7.10	Evaluation Report version 2	AEGIS	R	CO	36
D7.11	Best Practices and Policy Development Guidelines for Replicability and Wider Use	FHG-IBMT	R	PU	36
D7.2	Fully Implemented 3rd Vertical Layer version 1	PHILIPS	DEM	CO	17
D7.3	Fully Implemented 3rd Vertical Layer Report version 2	PHILIPS	R	CO	30
D7.4	Fully Implemented 3rd Vertical Layer version 2	PHILIPS	DEM	CO	30
D7.5	Integrated and Validation of the *AI4HEALTHSEC* System Report version 1	PDMFC	R	CO	20
D7.6	Integrated and Validation of the *AI4HEALTHSEC* System version 1	PDMFC	DEM	CO	20
D7.7	Integrated and Validation of the *AI4HEALTHSEC* System Report version 2	PDMFC	R	CO	32
D7.8	Integrated and Validation of the *AI4HEALTHSEC* System version 2	PDMFC	DEM	CO	32
D7.9	Evaluation Report version 1	AEGIS	R	CO	23
D8.1	Dissemination and Communication Plan	TUV	R	PU	6
D8.2	Report on Dissemination and Communication Activities version 1	TUV	R	PU	20
D8.3	Report on Dissemination and Communication Activities version 2	TUV	R	PU	36
D8.4	Exploitation, Sustainability and Business Plans version 1	PHILIPS	R	CO	20
D8.5	Exploitation, Sustainability and Business Plans version 2	PHILIPS	R	CO	36
D8.6	Organization and Selection of Open Call	CNR	R	CO	33
D8.7	Outcome of Open Call	CNR	R	CO	36
D9.1	H - Requirement No. 1	CNR	ETHICS	CO	6
D9.2	POPD - Requirement No. 3	CNR	ETHICS	CO	6
D9.3	GEN - Requirement No. 5	CNR	ETHICS	CO	12
D9.4	GEN - Requirement No. 6	CNR	ETHICS	CO	24

Table 8: AI4HEALTHSEC's Deliverables