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"

AI4HEALTHSEC Open Call Guidelines for Applicants

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

Lead contractor: CNR
Duration: 36 months

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

Table of Contents

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

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

List of tables

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

List of figures

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

1 Introduction

1.1 *Challenge*

Over the past decade, the healthcare sector has experienced a massive digitization, in particular nowadays the healthcare stakeholders are operating upon a variety of ICT components, ICT infrastructures and emerging medical technologies (including IoT devices, wearables, Big Data, and Electronic Health Records (EHRs) have appeared). However, the increased usage of information technology as well as the increasing interconnection between the medical devices and systems in the modern healthcare means that these healthcare operators have been transformed into large Health Care Information Infrastructures (HCIIs).

In addition, this evolving digital interconnectivity of medical devices has changed the threat landscape so now the HCIIs are becoming more vulnerable to the activities of all kinds malicious entities and individuals (including hackers, terrorist groups, criminal gangs etc.). Also, all these cyber-criminal actors have significantly evolved their tactics, techniques and procedures and they will continue to discover unexpected new ways to break into ICT processes and operations of the HCIIs.

Thus, there is an urgent, pressing challenge for the healthcare operators to tackle these attacks and ensure security and resilience of the overall healthcare ecosystem. To this end, the Healthcare stakeholders need new approaches that facilitate their collaboration and promote the security-related information sharing. These approaches should enable the healthcare entities to react on the security events and evaluate their risks as a sole intelligence and make decisions on how to deal with them.

1.2 *Motivation*

AI4HEALTHSEC proposes a state-of-the-art solution that improves the detection and analysis of cyber-attacks and threats on HCIIs, and increases the knowledge on the current cyber security risks. Additionally, **AI4HEALTHSEC** builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with capability to react in case of security events. Last but not least, **AI4HEALTHSEC** fosters the exchange of reliable and trusted incident-related information among ICT systems and entities composing the HCIIs without revealing sensitive corporate details.

1.3 *AI4HEALTHSEC Outcomes*

AI4HEALTHSEC introduces a **Dynamic Situational Awareness Framework (DSAF)** aiming to support the operators and the other stakeholders comprising the Health Care ecosystem to identify, model, and analyse their security risks, to respond to their threats and to handle their cyber-related incidents in an effective way. In particular, the goal of this framework is to support and help the healthcare operators and the decision makers to understand the technical aspects of the relevant risks, threats and attacks and draw conclusions on how to respond.

DSAF has been realized through a multi-layer architecture, depicted in Figure 1, that has been designed to support and provide two (2) main **business services**, namely:

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

- The **evidence-based risk management and assessment services**, in which DSAF provides mechanisms, and tools to assess the vulnerabilities related to the cyber assets of the ecosystem and forecast and evaluate the probability of cyber-attacks.
- The **multi-level incident identification and management services**, in which DSAF develops mechanisms and software solutions that enable the collection of evidence and automate the correlation of information regarding the evolution of incidents and the detection of anomalies.

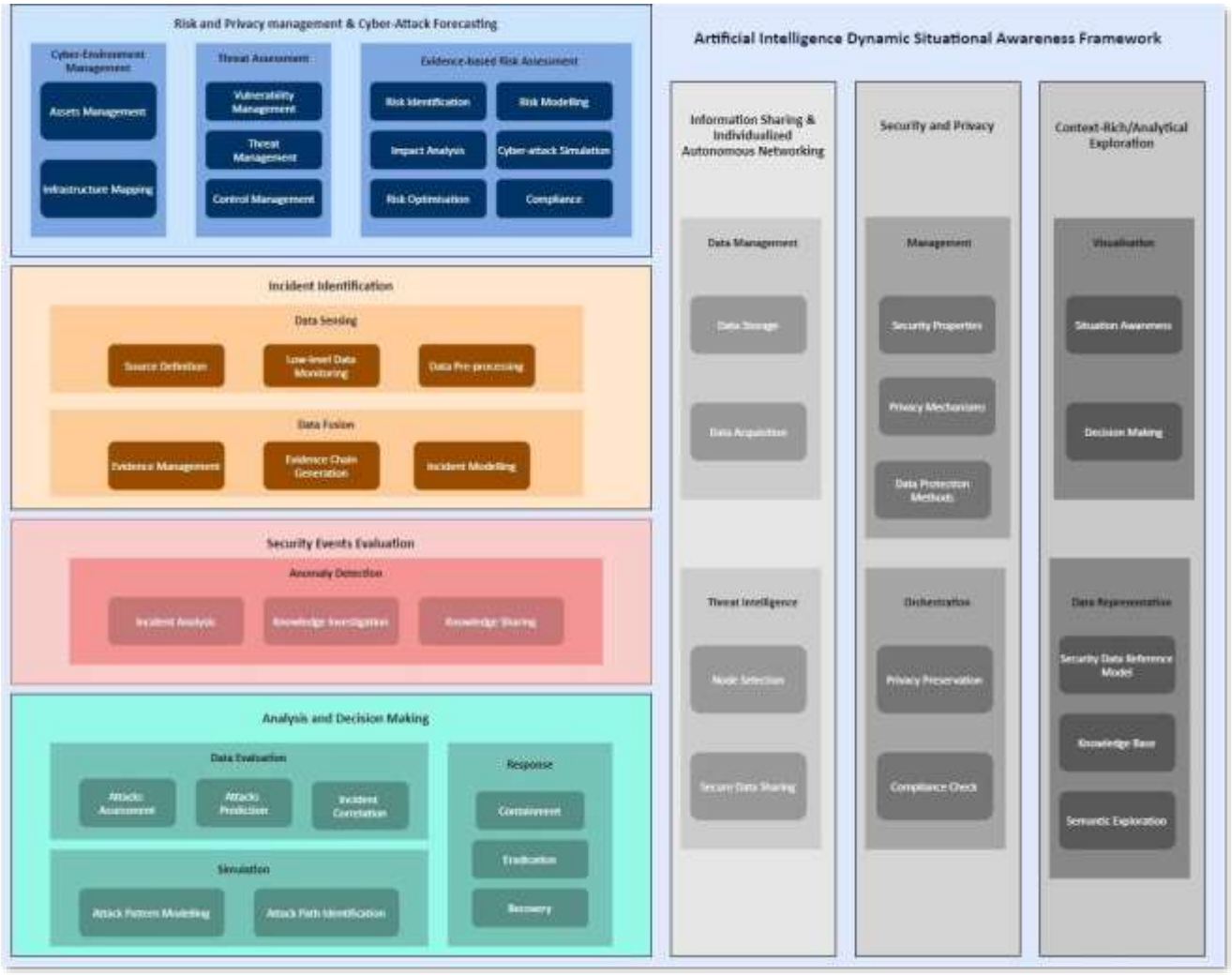

Figure 1. AI4HEALTHSEC architecture

The **AI4HEALTHSEC** multi-layer architecture consists of seven (7) conceptual layers, four horizontals, and three verticals. The 4 horizontals **("Risk and Privacy management & Cyber-Attack Forecasting", "Incident Identification", "Security Events Evaluation"** and **"Analysis and Decision-Making"**) are dealing with the situational awareness process and three vertical, the **"Information Sharing & Individualised Autonomous Networking"** are responsible to distribute, disseminate, self-publish,

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

broadcast or circulate the security-related information, the **"Security & Privacy"** are incorporating a set of security, privacy and data protection features and the **"Context-Rich/ Analytical Exploration"** are providing environment that allows the HCIIs' operators to have a better understanding of the cyber environment. In particular:

- **Horizontal Layer 1 – Risk and Privacy management & Cyber-Attack Forecasting:** This layer incorporates and implements all the necessary security and privacy processes, including threat assessment, identification of the vulnerabilities, impact estimation, calculation of the cascading effects, evaluation of all risks, to provide effective risk and privacy assessment and management in accordance with existing security standards and regulations (e.g. ISO27005, ISO28000).
- **Horizontal Layer 2 – Incident Identification:** This layer incorporates capabilities for preventing and detecting any kinds of anomalies, threats and risks.
- **Horizontal Layer 3 – Security Events Evaluation:** This layer includes proper anomalies identification mechanisms and is responsible to orchestrate and facilitate the initial evaluation of an incident.
- **Horizontal Layer 4 – Analysis and Decision-Making:** The main responsibility of this layer is to further investigate and analyse the security events occurred in the infrastructures in order to reveal the attacker's actions and to identify the means that were employed by the attacker, and in overall and to provide a better understanding of how the attack originated and evolved.
- **Vertical Layer 1 – Information Sharing & Individualized Autonomous Networking:** This Layer has the responsibility to disseminate and share information among the Interdependent HCIIs.
- **Vertical Layer 2 – Security and Privacy:** This layer aims to ensure the desired-levels of data protection for sensitive incident and risk-related information.
- **Vertical Layer 3 – Context-Rich/Analytical Exploration:** This Layer includes the visualization of information to effectively and quickly communicate this information enabling deep understanding of the situation and decision-making.

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

2 Open Call

2.1 *Objectives*

The Open call of the project involves the testing, validation and evaluation of the **AI4HEALTHSEC** architecture and services from a functional, technical and business perspective. The **AI4HEALTHSEC** Open Call is organised around two (2) topics. Each topic targets different stakeholders (under the guidance of the technological partners of the project):

- **Topic A - Use Cases from the Healthcare domain**: Involvement of 3rd party Healthcare Stakeholders, in particular, the following persons, teams and entities will be mobilized and engaged in the pilot operations: Security Officers, Members of Security Teams, IT administrators and internal users interacting with Healthcare ICT systems, as well as Supply Chain interacting entities with the Healthcare ICT systems.
- **Topic B - Use Cases from other Critical Sectors**: Involvement of 3rd party stakeholders operating in critical sectors other than healthcare (i.e. FinTech, Manufacturing, Energy, Water, E-Government, Transportation, Telecommunications etc.) with interest in supply chain security, risk management and incident handling processes, including entities participating in the critical sectors supply chain.

The AI4HEALTHSEC Open Call is devoted to external pilot operations activities towards attracting and engaging stakeholders in the pilot operations. The Open Call will include the selection of the third-party and stakeholders outside the consortium that will be engaged in the use and validation of the AI4HealthSec architecture & Services. Training of the selected end-users and stakeholders on the operation and use of the AI4HealthSec architecture & Services will be provided as part of the pilot implementation.

The evaluation outcomes will be analysed in order to produce best practices for the wider applicability and use of the **AI4HEALTHSEC** platform and associated collaborative approach. The best practices will cover the generalization of the approach for use in risk management and incident handling processes in other types of critical infrastructures that involve dynamic supply chains.

A summary of the Open Call is summarized in the following table.

AI4HEALTHSEC Open Call: Invitation to 3rd Parties	
Objectives	Validation of the AI4HEALTHSEC platform and associated collaborative approach in other entities of the Healthcare domain. Produce best practices for the wider applicability and use of the AI4HEALTHSEC platform and associated collaborative approach.
Benefits to 3rd-parties	Gain a better understanding of the threat landscape affecting their infrastructure. Adopting an innovative solution that will help them to deal with cybersecurity risks and incidents.
Activities to be funded	Deployment, testing, validation and evaluation of the **AI4HEALTHSEC** architecture and services.
Quality Assessment	A set of objectives and tasks will be defined, and the progress of each pilot

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

	project will be assessed, through evaluation and progress measures. Insufficient quality, poor performance, and/or commitment may stop the pilot project and payments.

Table 1. AI4HEALTHSEC Open call overview

2.2 *Funding scheme*

The Funding scheme of the open call is presented in the following table.

AI4HEALTHSEC Open Call: Invitation to 3rd Parties	
Total Budget	The Open Call will provide a total of € 180.000,00 in funding
Funding per pilot application	Up to €45.000 per pilot application (>=4 pilot applications will be funded, Total: €180.000,00)
Topic A - Healthcare domain	A Minimum of 2 pilot applications will be funded (>=2 pilot applications, Total: €90.000,00)
Topic B - Use Cases from other Critical Sectors	A Minimum of 2 pilot applications will be funded (>=2 pilot applications, Total: €90.000,00)
Number of participants per pilot application	A maximum of 2 participants (entities) per pilot application.
Duration of pilot application	3 months
The payment will be completed	The selected 3rd party will be paid against delivering activities submitted in Section 3 "Implementation and Deliverables". The payment will be released according to the Subgrant Agreement provisions.

Table 2. Funding scheme

An Evaluation Committee of experts in the domain of Cybersecurity and Supply Chain Services will review, assess and select the most promising applications.

2.3 *Criteria for calculating the exact amount of financial support*

The amount of financial support will be calculated on the basis of the estimated costs of the proponents. Each proposal will include milestones and deliverables, and a cost estimate justifying the costs and resources in relation to the plan. Checking the consistency between these costs and the expected work will be part of the evaluation. The estimated costs of the third party should be reasonable and comply with the principle of sound financial management in particular regarding economy and efficiency. The allowed overhead rate is a 25% flat rate. The third party cannot request any funding for activities that are already funded by other grants (the principle of no double funding). The industrial third parties will be funded 70% of their respective costs. Non-profit research institutes and public authorities can receive funding of up to 100% of their costs. Third parties can receive pre-financing of 20% of their respective total funding amount. Further payments will be made upon successful completion of milestones and/or deliverables as evaluated and approved in the mid-term and final reviews.

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

2.4 *Open Call Key dates*

The key dates of the open call are presented in the following table.

Activity	Dates
Call Announcement	February 1st, 2023
Submission Deadline	February 28th, 2023 (17.00 CET)
Evaluation and selection	March 17th, 2023
Contract's signature deadline	March 31st, 2023
Expected kick-off of the projects	April 1st, 2023

Table 3. Open call key dates

2.5 *Timing of the Open Call*

The timeline of the Open Call implementation can be analysed as follows:

Activity	Description	Dates
Open Call Submission Period	Deadline for proposal submission of the Open Call for both candidate applicants and external experts as evaluators	February 1th - February 28th, 2023
Open Call Evaluation Period	Evaluation of the submitted pilot applications	March 1st - March 17th, 2023
Selection and Contract Signature	Onboarding of winning applicants	March 18th - March 31st, 2023
Pilot Projects Implementation	Period of three (3) months for the winning applicants to run their use case	April 1nd – June 30th, 2023

Table 4. Open call timeline

Below is the presentation of the distribution of the call along the project timeline.

Figure 2. Open call timeline

Note: The dates shown in Figure 2 may change due to unforeseen events and situations.

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

3 Implementation and Deliverables

3.1 *Project Implementation Timeline*

Each pilot project will be split into three (3) phases: 1) DESIGN, 2) INTEGRATION, 3) VALIDATION & EVALUATION, each one lasting 1, 1 and 1 month respectively. The first phase will entail the planning for using, adapting and integrating **AI4HEALTHSEC** into the third-party infrastructures, feeding into the next phase which will be responsible for performing the work required to use them, and finally, the last phase will focus on testing and demonstrating the applications.

- ✓ Phase 1 – **Design (4/2023)**

  The participants will define the scope of the demonstrator, including the identification and in-depth analysis of their showcase scenarios. Appropriate Key Performance Indicators (KPIs) will be developed along with specific test cases associated with risks, threats and security incidents. Also, the participants have to drill down into a specific timeline and to develop integration and validation plans. Finally, the participants will be trained on the operation and use of the **AI4HEALTHSEC** infrastructure and services.

- ✓ Phase 2 – **INTEGRATION (5/2023)**

  This phase performs the integration of the demonstrator applications with the **AI4HEALTHSEC** infrastructure according to the integration and validation plans defined in Phase 1. The **AI4HEALTHSEC** team will allocate the necessary resources to closely monitor and coach the pilot projects. The team members will effectively monitor the projects, review their intermediate results to assess the progress of each pilot project and continuously provide feedback on what needs to be corrected in the whole process.

- ✓ Phase 3 – **Validation & Evaluation (5-6/2023)**

  This phase focuses on the actual validation of the **AI4HEALTHSEC** infrastructure and services at all applicants' sites allowing for the proper subsequent evaluation. It should be noted that the evaluation will be conducted in parallel with the validation. The evaluation will cover different perspectives, including business and functional perspectives. It will be primarily based on the completion of questionnaires developed by the consortium partners.

3.2 *Deliverables*

Two deliverables should be produced:

- **Report on Pilot Preparation and Detailed Pilot Operations Planning**: This deliverable will be a report on the status of preparatory actions at the pilot sites. Furthermore, it will provide the detailed pilot operations plan and the Test cases pilot scenarios. Finally, the deliverable will report all the information regarding the experiments and the corresponding evaluation results.
- **Costs and Resources Statement**: The report that will describe the costs during the evaluation and validation. No detailed documents are to be provided in order to justify the costs of the experiment. Nevertheless, recipients of the financial support will keep all their documents and

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

records to allow the Commission and the **AI4HEALTHSEC** partners to be informed about the costs in line with H2020 rules.

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

4 Eligibility criteria

The following section describes the eligibility criteria for the applicants in detail. All applicants will have to abide by all general requirements described in this section to be considered eligible for this Open Call. Proposals failing to comply with eligibility criteria will not be considered.

4.1 *Type of Applicants*

The call is open to entities operating in critical sectors other than healthcare (i.e. FinTech, Manufacturing, Energy, Water, E-Government, Transportation, Telecommunications etc.) with interest in supply chain security, risk management and incident handling processes, including entities participating in the critical sectors supply chain.

The participation is possible only for legal entities established in an eligible country (see section 3.2). Individuals cannot participate. The person submitting the proposal must be empowered to represent and commit the applying legal entity according to the relevant law. In case of multiple submissions by different individuals for the same legal entity, only the proposal submitted by the person empowered to do so will be considered eligible.

4.2 *Eligible Countries and Languages*

Applicants legally established in any of the following countries can apply for the Open Call: (i) Member States of the European Union; (ii) Associated Countries according to the updated list published by the EC; (iii) Third Countries according to the updated list published by the EC; and (iv) The UK applicants are eligible under the conditions set by the EC for H2020 participation at the time of the deadline of the call.

English is the official language for this Open Call.

4.3 *Conflict of Interest*

Applicants, their legal representatives and shareholders cannot be **AI4HEALTHSEC** Consortium partners or affiliated entities nor their employees or co-operators under a contractual agreement.

4.4 *Multiple submission*

Maximum funding request per proposal. A third party can be involved in several proposals, but the maximum amount of financial support to be granted to each third party is 75.000 €.

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

5 Submission Process

This Section shows the details of the submission process. Proposers will submit their proposal through a web portal available at https://ai4healthsec.submitsquare.com. The same web portal will include a downloadable template (word document) provided by the AI4HEALTHSEC consortium to support the writing of the proposal.

The submission will consist of a pdf file that will contain the description of the proposal, as well as the information of the applicant. As mentioned above, the proposal must follow the template provided by the consortium and will be downloadable from the submission web portal. The content of the template is described followingly in Section 5.1.

The proposal language is English. Proposals submitted in other languages will not be eligible.

Proposals are submitted in a one-stage process that means that applicants submit a full proposal prior to the deadline.

In the case of need of support, the applicant can contact via email the helpdesk and consult the FAQ (see Section 7 for further information).

Late submissions shall not be accepted. Late submitters shall receive by return email a "call closed" message from the system.

After the call closure no additions or changes to received proposals should be taken into account.

5.1 *Proposal template sections*

The applicants must follow the provided proposal template for writing their proposals, which must be submitted as a pdf file through the submission web portal.

The template includes the Sections described below.

5.1.1 Project Info

The first section of the proposal is formed by a Table, where the main information about the proposal must be included. In detail, this Table will include:

- **Proposal acronym** (max 12 characters)
- **Main type of the action**, where the sector of the proposal (Healthcare, FinTech, Manufacturing, Agrifood, etc.) must be indicated. Only one activity must be chosen.
- **Provider of the action,** where the applicant's name, the address, the responsible person and the contact email must be provided.

5.1.2 Excellence

This Section of the proposal must be up to 4 pages and includes two Sections: ***Objectives & Ambition*** and ***Methodology***.

The Section ***Objectives & Ambition*** must describe:

- How the domain/sector of the proposal is affected by cyber threats and the contribution that the proposal intends to make with the proposed use case.
- How the proposed use case contributes to achieving the AI4HEALTHSEC objectives.

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

- The technical/use case challenges that the proposal addresses and how these challenges materialize in the specific use case.
- Which project outcomes will be evaluated.

The Section ***Methodology*** must describe:

- The use cases that will serve as AI4HEALTHSEC demonstration scenarios.
- The use case in more details (e.g., available technologies, digital assets, critical services to safeguard in your application field & type of data, attack scenarios), including the current situation and the targeted situation.
- The conditions and the scope of the use case activities.

5.1.3 Impact

This Section of the proposal must be up to 2 pages and must present:

- The advantages and unique offerings that the use case will bring into the Supply Chain Services cybersecurity domain.
- What is the business value to your organization by adopting the AI4HEALTHSEC architecture and services
- A clear and realistic definition of at least 2 technical KPIs and 2 business KPIs, to introduce advances and evaluate the AI4HEALTHSEC architecture and services.

5.1.4 Impact

This Section of the proposal is up to 3 pages and must include the following points:

- A description of how the proposal will carry out the three main phases of the project implementation timeline, namely 1) DESIGN, 2) INTEGRATION, 3) VALIDATION & EVALUATION" (see previous Section 3.1 of this document). It must also provide a GANTT chart linked with the proposed tasks.
- A timeline for the project, considering that the duration of the project is fixed (3 months).
- Align the list of deliverables and milestones with the AI4HEALTHSEC Open Call Guidelines for Applicants for Project Implementation Timeline.
- Key risks and mitigation strategies.
- The human resources of the applicant via the budget distribution for the staff allocated to the project by means of person months, ensuring that the effort is proportional to the reward. A List with the corresponding justification of the equipment or other costs, along with a short explanation. (Costs for equipment are not compulsory to be allocated in advance).

5.1.5 List of Tasks

The list of tasks must be included in a Table, where the task number, the task name and its description, the start and the end months must be provided.

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

5.1.6 List of Deliverables

The list of deliverables must be included in a Table, where the deliverable number, the deliverable name and its description, the associated task and the delivery month must be provided.

5.1.7 List of Milestones

The list of milestones must be included in a Table, where the milestone number, the milestone name and its description, the type (mandatory or not mandatory) and the due date (in months) must be provided.

5.1.8 GANTT Chart

The GANTT chart must be provided in this subsection.

5.2 *Submission web portal*

The web portal at the https://ai4healthsec.submitsquare.com URL will include the required information for the submission of the proposal, the link for downloading the template, the FAQ, the email address of the helpdesk and the link to upload and submit the proposal. After a correct submission, the applicants will receive a notification.

5.3 *Submission deadline*

The deadline for the submission of the proposals is February 28th 2023.

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

6 Evaluation Process

This Section describes the details of the evaluation process, including the proposals' evaluation process, the criteria for awarding of support, as well as the selection process.

6.1 *Proposal evaluation*

The received proposals will be evaluated by a team of external experts. Such experts will be individuals from the fields of science, industry and/or with experience in the field of innovation and security and also with the highest level of knowledge, and who are recognised authorities in the relevant specialist area. The selected experts will sign a declaration of confidentiality concerning the contents of the proposals they read and a confirmation of the absence of any conflict of interest.

Each proposal will be evaluated by at least two external experts. To ensure fairness, equal treatment and impartiality, the reviewers will be independent of the AI4HEALTHSEC Consortium and of any proposer. In their evaluations, the experts will use a standardised evaluation form provided by the AI4HEALTHSEC consortium. The evaluation shall take place at a maximum of two weeks from the close of the call. The appointment of the experts will be confirmed only after the closure of the Call, when all the proposers are discovered; at that time, the experts can be selected without risk of conflict of interest.

6.2 *Criteria for awarding of support*

The proposals will be evaluated with respect to the following three categories:

i) *Excellence*, focused on technological aspects;
ii) *Impact*, focused on the potential impact through the development, dissemination and use of results;
iii) *Implementation*, focused on quality and efficiency of the implementation and management.

Concerning the potential impact of the proposal, and in order to ensure that the selected experiments support the objectives of AI4HEALTHSEC, the proposals shall build on the top of the AI4HEALTHSEC solution and strengthen its technological base, dissemination, and exploitation.

The overall maximum score will be 20. Each category will be scored on a scale from 0 to 5. The individual scores have the following interpretation:

- 0 - Fail: The proposal fails to address the criterion under examination; or, the proposal cannot be judged due to missing or incomplete information.
- 1 - Poor: The criterion is addressed in an inadequate manner, or there are serious inherent weaknesses.
- 2 - Fair: While the proposal broadly addresses the criterion, there are significant weaknesses.
- 3 - Good: The proposal addresses the criterion well, although improvements would be necessary.
- 4 - Very good: The proposal addresses the criterion very well, although certain improvements are still possible.

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

- 5 - Excellent: The proposal successfully addresses all relevant aspects of the criterion in question. Any possible shortcomings are minor.

The categories *Excellence* and *Implementation* will have a single weight, while *Impact* a double weight. There will be a score threshold of 3 out of 5 in the *Excellence* and *Implementation* categories, and 6 out of 10 in the Impact category. Inadequateness of the justification of costs and resources, as judged by the expert evaluators, will result in a below-threshold score in the Implementation category.

6.3 *Proposal selection*

Each of the two experts involved in the evaluation of a given proposal, will first record her/his evaluation of the proposal on the standardised evaluation form. Then, they will communicate together to prepare a single consensus form for each proposal, representing opinions and scores on which both agree and which both will sign. At the end of the process, by using the overall scores for each proposal, all the experts will jointly generate a ranked list, or several ranked lists if the Open Call is in different parts. If two or more proposals are tied with the same overall score, the experts will rank them using any appropriate discriminating element related to the Call. Using the scores given on the consensus form, a panel of AI4HEALTHSEC beneficiaries will generally select the highest ranked proposals for the call. However, it may overrule individual evaluations and ranking for ensuring a portfolio of experiments covering as complete as possible value-chains for the supported scenarios, or where it has objective grounds for objecting to the participant, for example commercial competition issues.

The final decisions on the funding of proposed experiments are made by the Project Coordinator (PC), the Project Technical Manager (PTM), the Risk Manager (RM) and the Legal/Ethical Manager (L/EM) of the AI4HEALTHSEC project. They may conclude that there are not enough proposals with an adequate quality, in which case they will make no selection or select fewer proposals than the Call allows. This conclusion is obligatory if not enough proposals score above the threshold given on the attached evaluation form. In the event of not enough selections being made, the AI4HEALTHSEC Consortium may re-open the Call at a later date.

6.4 *Communication with proposers*

At the end of the selection process, the AI4HEALTHSEC Consortium will get into contact with the successful proposers to prepare the conclusion of third party agreements. A contract will be signed between the AI4HEALTHSEC Coordinator and the third parties involved, and finally, the proposals' activities are kicked-off. The AI4HEALTHSEC Consortium will communicate to the other proposers that their proposal was not successful in the Call, and will enclose to each an unsigned version of the consensus report of their proposal.

6.5 *Transparency of the process*

At all stages of the Open Call process, the results will be made available to the EC Project Officer: the draft of the Open Call announcement (at least 30 days prior to its expected date of publication), the

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

selection of experts and the draft outcome of the evaluations will be provided to the EC Project Officer.

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

7 Open Call Support

Helpdesk: applicants can ask questions via email opencall_ai4healthsec@icar.cnr.it

Q&A: a list of FAQs will be published and updated during the application period.

Contact: Contact us at opencall_ai4healthsec@icar.cnr.it

Apply via: https://ai4healthsec.submitsquare.com

More info at: https://www.ai4healthsec.eu/opencall; https://ai4healthsec.submitsquare.com

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

Annex 1. Call announcement

Announcement of an open call for recipients of financial support, under the AI4HealthSec project

Project acronym: AI4HEALTHSEC

Project grant agreement number: 883273

Project full name: A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures

Project AI4HEALTHSEC, co-funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883273, foresees as an eligible activity the provision of financial support to third parties, as a means to achieve its own objectives.

The types of activities to perform that qualify for receiving financial support are the design, integration and validation & evaluation of the Dynamic Situational Awareness Framework (DSAF) of the AI4HealthSec project for a specific application scope.

Deadline: February 28th, 2023 (17.00 CET)

Expected duration of participation: 3 months

Maximum amount of financial support for each third party: €45.000

Call identifier: AI4HealthSec Open call 1.

Language in which proposal should be submitted: English

Web link for further information (full call text/proposal guidelines/call results) on official project web site: https://www.ai4healthsec.eu

Email address for further information: opencall_ai4healthsec@icar.cnr.it

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

Annex 2. Acknowledgment of receipt

Acknowledgement of receipt

Dear XXX,

Thank you for submitting your proposal for consideration as recipient of financial support in the frame of project AI4HealthSec.

The evaluation of all proposals received will take place in the next few weeks. You will be notified as soon as possible after this of whether your proposal has been successful or not.

On behalf of my colleagues in the project I would like to thank you for your interest in our activities.

Yours sincerely,

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