Scaling Up secure Processing, Anonymization and generation of Health Data for EU cross border collaborative research and Innovation

D1.9 — Dissemination and Exploitation plan

Funded by
the European Union

Grant Agreement Nr. 10109571

Project Information

Project Title	Scaling Up Secure Processing, Anonymization and Generation of Health Data for EU Cross Border Collaborative Research and Innovation		
Project Acronym	SECURED	**Project No.**	10109571
Start Date	01 January 2023	**Project Duration**	36 months
Project Website	https://secured-project.eu/		

Project Partners

Num.	Partner Name	Short Name	Country
1 (C)	Universiteit van Amsterdam	UvA	NL
2	Erasmus Universitair Medisch Centrum Rotterdam	EMC	NL
3	Budapesti Muszaki Es Gazdasagtudomanyi Egyetem	BME	HU
4	ATOS Spain SA	ATOS	ES
5	NXP Semiconductors Belgium NV	NXP	BE
6	THALES SIX GTS France SAS	THALES	FR
7	Barcelona Supercomputing Center Centro Nacional De Supercomputacion	BSC CNS	ES
8	Fundacion Para La Investigacion Biomedica Hospital Infantil Universitario Nino Jesus	HNJ	ES
9	Katholieke Universiteit Leuven	KUL	BE
10	Erevnitiko Panepistimiako Institouto Systimaton Epikoinonion Kai Ypolgiston-emp	ICCS	EL
11	Athina-Erevnitiko Kentro Kainotomias Stis Technologies Tis Pliroforias, Ton Epikoinonion Kai Tis Gnosis	ISI	EL
12	University College Cork - National University of Ireland, Cork	UCC	IE
13	Università Degli Studi di Sassari	UNISS	IT
14	Semmelweis Egyetem	SEM	HU
15	Fundacio Institut De Recerca Contra La Leucemia Josep Carreras	JCLRI	ES
16	Catalink Limited	CTL	CY
17	Circular Economy Foundation	CEF	BE

Project Coordinator: Francesco Regazzoni - University of Amsterdam - Amsterdam, The Netherlands

Copyright

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Deliverable Information

Workpackage	WP1
Workpakace Leader	Francesco Regazzoni (UvA)
Deliverable No.	D1.9
Deliverable Title	Dissemination and Exploitation plan
Lead Beneficiary	ISI
Type of Deliverable	Report
Dissemination Level	Public
Due Date	30/06/2023

Document Information

Delivery Date	30/06/2023
No. pages	34
Version | Status	1.0 | final
Deliverable Leader	Evangelos Haleplidis, Apostolos Fournaris (ISI), Konstantinos Avgerinos, Christina Michailidou, Christos Avgerinos (CTL)
Internal Reviewer #1	Juan Carlos Pérez Baun, ATOS
Internal Reviewer #2	Alberto Gutiérrez Torre, BSC

Quality Control

Approved by Internal Reviewer #1	28/06/2023
Approved by Internal Reviewer #2	30/06/2023
Approved by Workpackage Leader	03/07/2023
Approved by Quality Manager	04/07/2023
Approved by Project Coordinator	05/07/2023

List of Authors

Name(s)	Partner
Christos Tselios, Evangelos Haleplidis, Apostolos Fournaris	ISI

The list of authors reflects the major contributors to the activity described in the document. The list of authors does not imply any claim of ownership on the Intellectual Properties described in this document. The authors and the publishers make no expressed or implied warranty of any kind and assume no responsibilities for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information contained in this document.

Revision History

Date	Ver.	Author(s)	Summary of main changes
01.05.2023	0.1	Apostolos Fournaris(ISI)	Created the document and the initial version of its content
01.06.2023	0.2	Christos Tselios, Evangelos Haleplidis, Apostolos Fournaris (ISI)	Added deliverable text
15.06.2023	0.3	Konstantinos Avgerinos, Christina Michailidou, Christos Avgerinos (CTL)	Added Text for the Exploitation Section
28.06.2023	0.4	Evangelos Haleplidis, Christos Tselios, Apostolos Fournaris (ISI)	Added Text from requrested input from partners and made changes based on Francesco Regazzoni's (UvA) comments
29.06.2023	0.5	Evangelos Haleplidis, Christos Tselios, Apostolos Fournaris (ISI), Konstantinos Avgerinos, Christina Michailidou, Christos Avgerinos (CTL)	Made changes based on reviewer comments

Table of Contents

1 Executive Summary

This deliverable describes the Dissemination and Exploitation action plan regarding the results of the SECURED project, innovations, concepts and progress on communications activities.

While the project is still in its early stages, there has been extensive communication activities, including establishment of an active website with sections targeted at different groups and use of social media. The deliverable provides information on the way in which these have been used up to this stage in the project.

The dissemination and exploitation plan is mainly based on what was described in the proposal and GA, along with some refinements and current ongoing work and outcomes from the first six months of the project and outline the plan for the rest of the lifetime of the project.

Finally as monitoring and evaluation of the dissemination and exploitation activities are integral to ensure that the project's progress and effectiveness, this deliverable also contains a set of clearly quantifiable Key Performance Indicators (KPIs) that will be continuously monitored within the project's lifetime. This monitoring process allows for timely adjustments and improvements to the dissemination and exploitation plan, to make sure that the project will be able to achieve its goals.

1.1 Related Documents

- Grant Agreement (GA) Project 101095717 - SECURED; Description of Action (DoA) Annex 1
- Deliverable D1.1 “Project Handbook Quality, Management”
- Deliverable D1.7 “Project Website”
- Deliverable D1.6 “Data Management Plan”

2 Introduction

2.1 Intended audience

This deliverable is aimed at three distinct audiences:

- Internal partner (Consortium) members
- EU commission and independent reviewers

2.2 Purpose and scope of the document

One of the key Objectives in the DoA is to provide a viable dissemination, exploitation and business model of the SECURED solution that will build momentum and support the continuation of the SECURED privacy preserving collaborative health data ecosystem beyond the end of the project.

This document provides the communication strategy to effectively engage diverse audiences and to present the project's research findings in a clear and accessible manner as well as the financial benefits (including cost-effectiveness and efficiency gains) that the SECURED's hub, infrastructure and framework can introduce to the health industry. Foreseen improvements are mostly related to securing and scaling multi-party computation techniques while preserving original and synthetic data privacy, compliance within GDPR regulations, and avoiding bias in data, with quantifiable evidence.

Effective dissemination and communication of research results are crucial for scientific progress, and SECURED recognises the importance of sharing its findings with potential users in the research field, industry, and policymakers.

By doing so, the SECURED project aims to contribute to the advancement of science while achieving its project objectives.

The objectives of this document are as follows:

- Provide a clear Communication and Dissemination roadmap for the SECURED project, outlining the key principles and approaches during the project's lifespan.
- Assign specific roles and responsibilities to the partners involved in the task, ensuring a coordinated and efficient dissemination effort.
- Identify the most suitable channels and tools to be utilized during the project, considering both digital and offline mediums, to effectively reach the target audiences.
- Establish a robust methodology for evaluating the effectiveness of the communication and dissemination activities, allowing for continuous improvement and measurement of the project's overall success.
- Outline the exploitation strategy to maximize the potential of the SECURED project during and after the project's lifespan.

  The SECURED project aims to develop a comprehensive communication, dissemination and exploitation strategy to maximize the impact of the project itself. This rest of the document will describe the strategies followed and foreseen to achieve the planned impact goals.

2.3 Relation to Work Packages, Deliverables and Activities

Dissemination is directly connected to the project's activities and results. It is relevant across all work packages. WP2, WP3, WP4 and WP5 contribute the content to be disseminated, generating the knowledge that the consortium aims to share with the target audience.

2.4 Contribution to WP1 and Project Objectives

This report comprises the project's Deliverable D1.9 " Dissemination and Exploitation plan" that is associated with the T1.4 "Dissemination Activities, Training and Education Activities and Planning". As described in the Grant Agreement, this task organizes the transfer of knowledge and of project results, both within the consortium and to the outside world. It ensures that all involved organizations are kept informed and can promote project results. Thus, the interactive and online (professional social networks and project's website) dissemination channels are considered of particular importance for influencing prospective adopters of the SECURED framework. The aim of this task is to widely disseminate and present the SECURED project's [1] outcomes to the scientific and technical communities. More specifically this deliverable contributes to the following project objectives:

- Project Objective O8. Provide a viable dissemination, exploitation and business model of the SECURED solution that will build momentum and support the continuation of a SECURED privacy preserving collaborative health data ecosystem beyond the end of the project
- WP1 Objective 1.2: Produce a quality assessment and monitoring plan for the project.
- WP1 Objective 1.4: Plan and facilitate communication and interactions within the consortium.

2.5 Structure of the Document

More specific, this document is divided as follows:

- Section 3 outlines the dissemination and communication strategy of SECURED
- Section 4 outlines the exploitation strategy of SECURED
- Section 5 describes the means and activities that raises awareness of SECURED
- Section 6 provides the dissemination monitoring strategy, where the tools and KPIs to be used for performance monitoring are being suggested.
- Finally the deliverable finishes with the conclusion section.

3 Dissemination and Communication Strategy

3.1 Objectives

To achieve the dissemination goals defined in the DoA, it is crucial to define a clear dissemination and communication strategy. This strategy will ensure that the project outcomes timely reach the appropriate target communities through appropriate channels. The SECURED project has identified several key objectives for its dissemination and communication strategy.

- Create a clear dissemination and communication activities plan matching the goals of the project and ensure that all partners are aware and make practical and effective use of it.
- Utilize all available web presence and digital material to raise awareness about the project and aim at specific target groups based on the outreach of each tool.
- Engage and foster collaboration among stakeholders by inviting and collaborating with relevant projects as well as through the design, implementation and promotion of the SECURED open calls [1].
- Develop a strong and recognizable brand name for the project identified by its logo and known by all the disseminating material.
- Generate efficient and easy to understand dissemination material through the use of video and text for maximizing dissemination of the project's goals.
- Outline a schedule for the production of articles and scientific publications that disseminate project results through relevant events and established scientific conferences and journals.
- Support the overall promotion and organization of the project, including info days, webinars and developing and distributing materials.

3.2 Dissemination & Communication roadmap

To organize and better monitor the project objectives in regards to dissemination, the dissemination roadmap will be split into three distinct phases as seen in Figure 1.

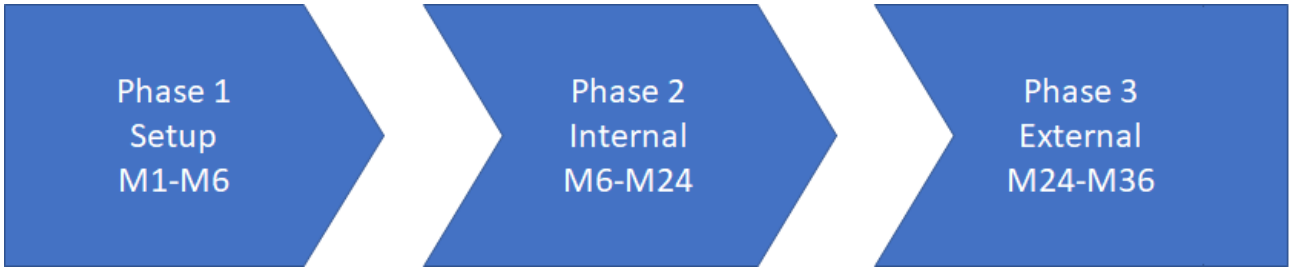


Figure 1 – Dissemination plan

Phase 1: Setup Phase (M1 – M6): This was the initialization phase of the whole project and the setup of the foundations of the dissemination plan for the SECURED project. This phase created the roadmap, specified the necessary mechanisms to collect dissemination material from the partners and created the necessary communication outlets of the project.

The establishment of a clear and concise roadmap early on (M6) was crucial to align all the consortium members to the dissemination objectives and actions planned in the project.

[1] At the end of the second year of the SECURED project, it is planned an open call where SMEs, innovators and researchers will be invited to experiment with the technologies under development

In parallel, this phase contained the creation of a dedicated project website, establishment of social media accounts, and development of various materials such as templates, logos, newsletters and social media content. These actions brought the communication plan to life and enabled the SECURED project to be able to engage with the target audiences effectively.

Table 1 showcases the results of the Setup Phase.

Action	Month	Expected Results
SECURED Website	M03	Website online
Social medial	M03	Social media accounts (Youtube, Facebook, Instagram, Twitter) setup
Workshop	M06	Creation of at least 1 end user workshop till M06

Table 1 – Setup Phase - Accumulated Results

The first news letter, originally expected for M6, has been postponed to M7, to be able to include information about the First End User Workshop.

Phase 2: Internal Phase (M6 – M24): In the internal phase, the primary focus is to proactively engaging the target stakeholders of the SECURED project and generate interest in the project's activities and outcomes and disseminate the project outcomes mainly developed by consortium members.

This engagement will be achieved by various strategies, all tailored to the specific needs and preferences of the stakeholders such as the organisation of targeted workshops, informative webinars, face-to-face meetings, on-site demonstrations or interactive virtual sessions.

In parallel, scientific material will be disseminated in high quality conferences and journals as well as participation of consortium members in conferences, events and fora. Since the dissemination of scientific results will follow the developement of the project, we expect however that the amount of scientific publications be much higher in the second part of this phase.

Table 2 showcases the results expected at the end of the Internal Phase.

Action	Month	Expected Results
SECURED Newsletter #2	M12	Publication of the second newsletter
Conference papers and participation in conferences	M12	At least 4 papers published and participated in at least 4 conferences till M12
Workshop	M12	Creation or participation in at least 1 workshop till M12
National Press Releases	M12	Participation in at least 1 national press releases till M12
Video	M12	Development of at least 1 video till M12
Brochure	M12	Publication of at least 1 brochure till M12
KPI updates	M12	Update KPIs with current metrics and adjust based on the current status of the project
SECURED Newsletter #3	M18	Publication of the third newsletter
Tutorial	M18	Publication of at least 1 tutorial till M18
SECURED Newsletter #4	M24	Publication of the fourth newsletter
Conference papers and participation in conferences	M14	At least 10 papers published and participated in at least 10 conferences till M14
Workshop	M24	Creation or participation in at least 2 workshop till M24
National Press Releases	M24	Participation in at least 3 national press releases till M24

Video	M24	Development of at least 2 videos till M24
Webinar	M24	Development of at least 1 webinar till M24
Brochure	M24	Publication of at least 2 brochure till M24
Tutorial	M24	Publication of at least 2 tutorial till M24
Journal papers	M24	At least 5 journal papers submitted or published till M24
On-site demonstration	M24	At least one on-site demonstration
Open Calls	M24	Open call publication
Collaborations	M24	Collaboration with at least 2 other projects or initiatives
KPI updates	M24	Second update of KPIs with current metrics and adjust based on the current status of the project

Table 2 – Internal Phase - Accumulated Results

Phase 3: External Phase (M24 – M36): In the external phase, the primary goal is to actively engage and promote the adoption and deployment of the tools and services developed by the SECURED project.

After reaching the 24-month milestone, the project will have a portfolio of tools and services, ready to be used by external partners via the SECURED Open Calls. At this point, the project will start to have a direct involvement of stakeholders and will thus support dissemination and exploitation of their results.

These activities will help ensure that the outcomes of the SECURED project will be beneficial and useful beyond its lifetime. By disseminating the project's outcomes effectively and exploiting them in a targeted manner, the goal is to create a lasting impact that drives growth and innovation in the relevant domains.

Table 3 showcases the results expected at the end of the External Phase.

Action	Month	Expected Results
Open Day	M28	Creation of an open day at M28
SECURED Newsletter #5	M30	Publication of the fifth newsletter
Webinar	M30	Development of at least 2 webinars till M30
Video	M30	Development of at least 3 videos till M30
Open Day	M32	Creation of the second open day at M32
SECURED Newsletter #6	M36	Publication of the sixth newsletter
Conference papers and participation in conferences	M36	At least 20 papers published and participated in at least 20 conferences till M36
Workshop	M36	Creation or participation in at least 3 workshop till M36
Open Calls	M36	Open call results published
National Press Releases	M36	Participation in at least 7 national press releases till M36
On-site demonstration	M36	At least 3 on-site demonstrations
Journal papers	M36	At least 10 journal papers submitted or published till M36
Collaborations	M36	Collaboration with at least 3 other projects or initiatives
KPI updates	M36	Final update of KPIs with current metrics

Table 3 – External Phase - Accumulated Results

It is important to note that the dissemination roadmap is an ongoing process moving along as the project progresses over time. To this effect, the dissemination goals will be regularly monitored and updated to ensure

their relevance and effectiveness. Adjustments to this plan are expected to occur within the project's lifetime in order to always be in alignment with the objectives and KPIs.

3.3 Roles & Responsibilities

To ensure effective dissemination and communication for the SECURED project, each partner will play a specific role in this effort based on their expertise, research and market position.

Table 4 outlines the roles and responsibilities of each individual partner in the dissemination and communication of the project designed to optimise their expertise to the project's best outcomes.

SECURED Member	Role and responsibilites
UvA	UvA dissemination activity is mostly focused to the dissemination and the diffusion of the research results. Towards the scientific community, dissemination will be carried out by publishing on high-quality journals and conferences in EDA and on security and privacy (e.g. DAC, DATE, TCHES, IEEE journals or ACM journals) and by participating and organizing scientific events (such as summer schools, special sessions or tutorials at leading conferences). Moreover, dissemination of results to network of excelences (such as HiPEAC), and Dutch associations of stakeholders involved in security (such as ACCSS) will be done. Finally, UvA will disseminate the results and the achievement of the project also towards the broader society though initiatives such as Open days, fairs or exhibitions. As project coordinator, UvA will also create and coodrinate the networking activities that the SECURED project will do to connect and collaborate with similar projects
EMC	As a prominent medical center in Europe, Erasmus MC will take measures to achieve comprehensive communication and dissemination of its activities and output throughout the project. Our dissemination plans aim to maximize the project's impact and encourage stakeholder collaboration. The key factors in Erasmus MC's strategy include: - Official digital & traditional media channels - Conferences & workshops - Invited Talks & guest lecturers - Collaborations with other EU-funded projects By implementing the aforementioned activities, Erasmus MC aims to ensure that SECURED's findings benefit stakeholders, fostering innovation and advancing the EU research agenda.
BME	The CrySyS Lab, also known as the Laboratory of Cryptography and System Security, is a research group located at the Budapest University of Technology and Economics (BME). It is dedicated to conducting research on security and privacy in computer systems and networks, as well as providing related educational courses at BME. CrySyS Lab aims to disseminate its research findings through publication in scientific journals and conferences that cater to specific scientific communities. To reach a wider audience and foster scientific discussions, the lab maintains a blog platform at (https://blog.crysys.hu/). Additionally, public communication channels such as Crysys's Twitter (https://twitter.com/crysyslab?lang=en). Facebook (https://m.facebook.com/Crysys-Lab-961417970606805/), and LinkedIn account (https://www.linkedin.com/company/crysyslab/) are utilized to promote the outputs of the SECURED project and raise awareness about SECURED events.

ATOS	Atos Research and Innovation, the R&D hub for new technologies within Eviden's BDS division with the largest expertise in research and development projects, will support the SECURED dissemination activities throughout the project lifecycle by: -ARI's Booklet: publishing the file and uploading of press releases and other relevant news at the request of the team involved. -ARI's SM: follow-up with reposting and creation of own posts at the request of the team involved. -ARI's internal newsletter (+140 project managers, researchers and developers across Spain): publishing news when the ARI team participates in events, papers, presentations, etc. -ARI team involved: participation in dissemination activities related to their WPs
NXP	The security group of NXP Belgium is part of the global Competence Center for Crypto and Security. One of the main focus areas of the group is to develop new innovation areas which can be transferred to the business units. Dissemination activities are expected to include: - Scientific articles at leading security and cryptography conferences, - Presentations of our work at relevant workshops and international events.
THALES	THERESIS is a Research and Technology entity inside Thales. Its role is to develop in short time breakthrough technologies that are transferred to our Global Business Units (BU). Dissemination activities inside the project concern: - internal dissemination with the BU involved in the healthcare domain and with the AI community inside Thales; - major international events: this will include both scientific, as well as more industry oriented events (see Publication tab for a list of events).
BSC CNS	Barcelona Supercomputing Center-Centro Nacional de Supercomputación (BSC-CNS) is the national supercomputing centre in Spain. We specialise in high performance computing (HPC) and manage MareNostrum, one of the most powerful supercomputers in Europe, located in the Torre Girona chapel. BSC has been successful in attracting talent, and our research focuses on four fields: Computer Sciences, Life Sciences, Earth Sciences and Computer Applications in Science and Engineering. In particular, the Data-Centric Computing group research is focused in data intensive applications leveraging HPC to provide results with a reasonable use of time and resources. In the particular case of SECURED, BSC leads the Synthetic Data Generation task. Through the project life we will promote the activities from SECURED publishing in conferences and journals but also in our social networks and educative workshops.
HNJ	Hospital Niño Jesús is the only thematic pediatric public hospital in Spain, so it is a national reference since more than a century. It is a showcase for new treatments in pediatric care. The hospital itself has its own web site managed by the regional healthcare authority. The Foundation has a web site and several social networks accounts where the research and innovation activities are posted for the general public. Besides, the hospital is part of a public university where the publication of scientific papers is actively promoted, and also the publication of articles in non medical magazines and web sites for general interest is encouraged. It is a common practice in the hospital to organize workshops on particular medical advancements for professionals of all specialties. The outcomes of SECURED project will be presented in several medical congresses and events during and after the lifetime of the project. The hospital is participating in other consortia where SECURED contributions are shared to look for effective synergies among European and National projects.

KUL	The KU Leuven CiTiP seeks to publish in scientific journals and conferences targeted towards dedicated scientific communities. The KU Leuven CiTiP also holds a blogpost platform, i.e., the CiTiP Blog (https://www.law.kuleuven.be/citip/blog/), which targets the communication of scientific discussions to a broader audience. Promoting SECURED project's outputs and raising awareness about SECURED events more generally should be reinforced through public communication means, including CiTiP's Twitter account (https://twitter.com/citip_kuleuven). Finally, liaison activities and interaction with other relevant EU projects are anticipated.
ICCS	As a research organization with substantial R&D activity in the fields of all diverse aspects of telecommunication systems, biomedical engineering, and distributed systems, control systems, computer systems and their applications, software and hardware engineering, ICCS will disseminate conceptual and actual architecture design of the knowledge base and the federation infrastructure. The corresponding results, along with the outcomes of AI algorithms that will be deployed during the project period, will be published at relevant, international conferences and journals.
ISI	ISI as an academic partner is focused on the dissemination of the research results of the project as well as the organisation and management of scientific events (special sessions, special issues etc.) related to the project and its activities. Furthermore, ISI will also focus on create synergies with other EU projects on which ISI participates or leads as well as the industrial network that the institute is associated with including related stakeholders from the Greek and Western Greece relevant community. ISI also aims to disseminate the projects overall results (beyond research publications) in Greek and EU forums and exhibitions that ISI traditionally participates (e.g., science festivals, CyberSecurity and Physical Security forums etc.). Finally ISI as the dissemination leader will oversee the overall realization of the SECURED's dissemination strategy.
UCC	In collaboration with other partners UCC, as an academic institution, will focus on disseminating the results of the research by publishing papers at international conferences and in international journals, and organizing special sessions and tutorials co-located with the main international conferences, as well as part of summer schools. UCC will also integrate the research into the teaching of relevant subjects at both undergraduate and postgraduate level.
UNISS	AIMET LAB is a research group located at the University of Sassari, which is an Italian medium sized university in Sardinia. Dissemination activities will be devoted to disseminate the original research carried out by AIMET LAB in the fields of formal methods, AI and machine learning algorithms. Original contributions will be presented and published in relevant conferences and/or journals.
SEM	The mission of the Semmelweis University Health Management Training Center (SE EMK) is to promote the development of health care in Hungary and the region by developing and disseminating the theory and practice of health management. With our educational programs, we strive to systematize and disseminate knowledge related to the management of healthcare systems and organizations, to expand the knowledge of healthcare professionals, and to shape the outlook of new generations of doctors and professionals. In our work, the dissemination of data-driven approach and knowledge is of particular importance, in the framework of which we also organized lectures for our students to identify the important characteristics of the human interpretation of data sets. With our research programs, we want to expand the body of knowledge related to the management of healthcare systems and organizations and the data-driven solutions that are extremely important for future patient care, and help professionals learn about current trends, explore and understand the connections. We publish our results in domestic and Q1 international journals and high impact conferences.

JCLRI	At the Josep Carreras Leukaemia Research Institute (IJC), we believe that effective communication and dissemination is crucial to advance in the mission of the SECURED project. Therefore, we have designed a communication strategy to reach diverse audiences, including the scientific community, healthcare professionals, patients and the general public. From the IJC, we will use various channels beyond those owned by the project, such as scientific publications, conferences, seminars and invited talks. We will actively share our research findings and contribute to the global scientific knowledge base. We are also committed to fostering societal engagement and increasing our outreach to the wider community. For this, our researchers will participate in the name of the SECURED project in scientific fairs and other local popular science events, to inspire scientific vocation and enhance scientific training. Additionally, we engage with the media, leveraging traditional and digital platforms to raise awareness about the impact of leukaemia and other malignant blood diseases
CTL	As our continuous goal is to contribute on the scientific and academia community and promote knowledge exchange, CTL will pursue to participate in 2-3 relevant workshops and conferences to present our work on federated learning infrastructure and AI-based framework. These events will allow the research community to obtain in-depth insights, methodologies, and results on the aforementioned fields and let them evaluate, replicate, and build upon our work, but it will also provide us the opportunity to connect with experts, receive feedback, and engage in discussions that will contribute on advancing our algorithms of the target scientific fields. CTL will also explore collaboration opportunities with industrial and SME partners, interested in exchanging knowledge and expertise on the domains of federated learning infrastructure and AI-based framework. This will might involve hosting webinars, giving invited talks, or conducting joint research projects. CTL also recognizes the importance of engaging the general public, thus we will leverage various communication channels, such as social media (https://www.linkedin.com/company/catalink-ltd/), (https://twitter.com/catalink_eu), online platforms, and public events to provide accessible and engaging content, such as blog posts, infographics, and demonstrations, to raise awareness, promote informed discussions, and foster public trust in AI technologies.
CEF	The Circular Economy Foundation, is responsible for disseminating the Open Call of the SECURED project. This includes effectively communicating the Open Call's purpose, objectives and requirements through various channels such as the foundation's website, social media platforms, newsletters and targeted communication with relevant stakeholders. It may also prepare reports on project progress and outcomes and collaborate with other teams to ensure widespread dissemination of SECURED Open Call's results.

Table 4 – Individual dissemination and communication plan

3.4 Target groups

We expect that companies and research organizations in the SECURED consortium together with the third parties involved in the SECURED open call will contribute to raising awareness and create a positive momentum around SECURED. To achieve a high outreach the dissemination strategy focuses on the target groups reported in table 5.

Target Group	Description	Actions
Leading Industry decision makers	Telecom Operators, IT equipment manufacturers	• Project Website • Social Media • Public Deliverables • Participation in targeted activities • Invitation to Open Calls

Innovators	SMEs, AI Health Care Providers	• Project Website • Social Media • Public Deliverables • Publishing of academic papers and scientific magazines • Presence in conferences & scientific workshops • Openly accessible repositories for source code • Invitation to Open Calls
Scientific Community	Focusing on mainly Health Data, Analysis Applications, Middleware Desing, Data privacy methodologies, event analytics, IT security	• Project Website • Social Media • Public Deliverables • Publishing of academic papers and scientific magazines • Presence in conferences & scientific workshops • Openly accessible repositories for source code
Health Data owners	Producers of Health Data, such as Hospitals, clinics.	• Project Website • Social Media • Public Deliverables • Invitation to Open Calls
Health Data Operators and Consumers	AI SMEs, Hospitals, clinics.	• Project Website • Social Media • Public Deliverables • Invitation to Open Calls
Policymakers	European Commision, European Regulators, Public agencies, National public Authorities	• Project Website • Social Media • Public Deliverables • Presence in conferences & scientific workshops

Table 5 – Target Groups

3.5 Assets to disseminate

The initial list of main components of the SECURED system architecture is reported in Table 11. We expect that the components of this list will act as driver for the overall promotion of the SECURED results with the target audience.

4 Exploitation Strategy

The Exploitation Strategy of the SECURED project is designed to ensure the effective utilization of project outcomes and maximize their impact within the healthcare data protection and cybersecurity domains. This strategy encompasses various elements, including objectives, an exploitation roadmap, roles and responsibilities, and target groups.

4.1 Objectives

It is of the utmost importance to ensure impact on external stakeholders and to maximize the exploitation potential and promote accountability. The exploitation of SECURED exploitable assets will undoubtedly strengthen the EU position in the Healthcare domain and establish the necessary innovation capacity for the European industries to lead in the sector. Exploitation strategic plan will initially exploit the well known principles of circular economy to identify the appropriate exploitation opportunities and promote market development. More specifically, the exploitation strategy of the SECURED project will target at achieving the following primary objectives:

1. **Engage public and private healthcare organizations as early adopters**: Encourage the participation of healthcare organizations in the early stages of the SECURED project's implementation, promoting the adoption of the project's results. By doing so, the strategy aims to improve the quality and security of healthcare data while positively impacting the technological capacity of all stakeholders involved.

2. **Evaluate the SECURED solution beyond the consortium partners**: Conduct thorough evaluations of the SECURED solution by reaching out to external innovators. This will be accomplished through the SECURED open call. By involving external researchers and innovators, the strategy aims to facilitate further research and innovation in healthcare data protection.

3. **Disseminate results to stakeholders and healthcare communities**: Act as a reference point for cybersecurity and promote the SECURED project's outcomes to stakeholders and relevant healthcare communities. Through targeted dissemination efforts, the strategy seeks to enhance EU Research and Innovation (R&I) capacities while ensuring the protection of healthcare data and its associated environment.

4. **Identify opportunities for commercialization**: Identify potential avenues for commercializing the project's outcomes, including the integrated and validated prototype. By driving business innovation and contributing to economic growth, the strategy aims to foster the adoption of SECURED project solutions within the healthcare sector. This will be achieved through increased awareness, demonstrations of effectiveness, and the establishment of strategic partnerships with relevant stakeholders.

5. **Contribute to the development of global standards**: Actively engage with standardization bodies to contribute to the development and establishment of global standards for health data protection. The strategy aims to share project insights and best practices, ensuring that the SECURED project plays a role in shaping the future of health data protection and promoting interoperability.

By pursuing these objectives, the Exploitation Strategy of the SECURED project aims to maximize the impact of its outcomes, both in terms of protecting healthcare data and promoting innovation and collaboration within the healthcare sector.

4.2 Market analysis

The use of AI in healthcare can be of use to acquire, store, analyze, share medical data, and act on this with the purpose of predicting an outcome. It is undoubted within the business community that the application of AI in healthcare will become greater in future, as the importance of these technologies is wider realized and socially accepted. People and companies realize that AI tools has the potential to lead to more accurate diagnoses,

better care, and less time spent by healthcare professionals on administrative tasks, which in turn enables more time spent on interacting and treating patients.

In 2021, the AI in healthcare market was worth over **11 billion U.S. dollars** worldwide, with a forecast for the market to reach around **188 billion U.S. dollars by 2030**[2]. Furthermore, as of 2021, around a fifth of healthcare organizations worldwide were in early-stage initiatives of using artificial intelligence in their organizations[3]. While a further quarter of hospitals and health systems reported to be in the pilot stage of rolling out artificial intelligence and machine learning technologies[4]. The most common types of AI software in use in healthcare worldwide in 2021 was healthcare data integration and natural language processing, without excluding the use of other technologies, such as computer vision, image processing and digital signal analysis.

A recent Gartner report[5] has also highlighted that keyplayer healthcare organizations are currently intensely investing at the AI data analysis technologies, revealing that significant investments (approximately 30% of the total various technologies investments) are made in Artificial Intelligence (AI)/Machine Learning (ML) domain. This indicates a significant market share to be assigned to innovation related to Healthcare AI based data analysis.

The number one concern, according to a survey carried out in the United States[6], surrounding the increased usage of AI in healthcare was threats to security and privacy. Other ethical concerns included safety issues and the potential of the AI being taken over by malicious entities. In Europe, a survey found that patients would be most trustful of AI being used in combination with expert judgements rather than decisions made purely by AI[7]. Although, in comparison to the concerns expressed by some potential patients, the majority of health executives believed that investment in AI will lead to both improved health outcomes and patient experience in hospitals and other healthcare settings.

As it is also reported by the DIGITALEUROPE leading trade association[8], while over 60% of the available data in Europe are health related, secondary usage of such data, by researchers and innovators, is not easy since the main issue to be resolved is a problem of trust. Given the sensitive nature of health data and the necessary national and EU legal restrictions (GDPR) to protect them, health data producers and health data lakes (or silos) are very reluctant to share their data with any third party. This makes the discovery and use of health data for data science very hard for innovators and researchers across Europe.

Anticipating a future market need, in SECURED, we plan to revolutionize the field of health data processing by establishing the groundbreaking SECURED Innohub - an impregnable collaborative innovation hub. Within this protected sharing platform, we shall unleash the unparalleled power cooperative processing through cutting-edge SMPC techniques, pawing the way to a new era of secure and trusted health data exchange and overcoming the aforementioned obstacles that currently exist in the market. Moreover, our pioneering efforts will encompass the creation of novel synthetic data, ensuring utmost confidentiality, and implementing robust anonymization assessments, fortifying the confidentiality of health data providers and users.

4.3 Exploitation roadmap

The exploitation roadmap outlines a structured plan for effectively leveraging the project's results. It encompasses the following key activities:

1. **Creating Synergies and Promoting Innovation**: Our roadmap focuses on creating strong synergies between the cybersecurity and health domains. By fostering collaboration, we aim to promote social and business innovation, contributing to job creation and economic growth. Additionally, we prioritize offering privacy guarantees on anonymized data, ensuring the highest level of data protection.

[2] https://www.statista.com/statistics/1334826/ai-in-healthcare-market-size-worldwide/
[3] https://www.statista.com/statistics/1225955/stage-of-ai-adoption-in-healthcare-worldwide/
[4] https://www.statista.com/statistics/1225986/ai-technologies-in-use-in-healthcare-worldwide/
[5] Gartner, "Healthcare and Life Science Business Driver: Strategic Technology Change", 22 February 2022 - ID G00758226
[6] https://www.statista.com/statistics/1256727/ethical-concerns-about-ai-in-healthcare-in-the-us/
[7] https://www.statista.com/statistics/1312896/attitudes-towards-ai-in-healthcare-in-the-eu/
[8] DIGITALEUROPE "A digital health decade: from ambition to action"

2. **Delivering Scientific Impacts**: We are committed to delivering cutting-edge advances in scientific impacts. Through comprehensive assessments using qualitative and quantitative Key Performance Indicators (KPIs), we will measure the effectiveness and success of our efforts. This will enable us to continuously enhance our solutions and contribute to the advancement of EU Research and Innovation (R& I) capacities.

3. **Exploitation Impact Indicators**: To assess the impact of our exploitation efforts and adjust our plan during the project, we will use appropriate indicators. These will include but not limited to:

    - End users of the SECURED platform and applications, involving all interested stakeholders.
    - Open-source projects resulting from the development of the SECURED platform and modules.
    - Products, processes, and methods introduced and developed during the project.
    - Start-ups and spin-offs created as part of our commercialization efforts. It should be clarified that in this Indicator we refer to start-ups/spin-offs projects from companies/organizations within or outside the SECURED consortium (e.g companies that participate in the open-call) that are created or updated by using the SECURED tools and services. Such new projects include new experimental products as well as services of existing enterprises and do not always require the founding of new enterprises from scratch.
    - Consultations provided to interested parties regarding SECURED technologies, modules, and the platform.
    - Demonstration cases implemented in real-world settings, showcasing the effectiveness of our solutions.
    - Thorough Testing and Validation: We will conduct rigorous testing and validation of the integrated prototype to ensure its robustness and efficacy in protecting healthcare data. Through continuous optimization based on feedback and real-world deployment experiences, we will refine our solution and ensure its reliability.

    Table 6, provided below, details these indicators:

Indicators	Metric	Target
SECURED uptake	• Demonstration to data health organizations • Demonstration to healthcare companies	• Target: 100 entities • Target: 500 users Website
SECURED output	• Number of open source projects	• Target: 20 projects
SECURED innovations	• Number of products developed as part of SECURED • Number of platform installations to the industry/organizations	• Target: >7 products • Target: 20 installations
Commercialization	• Number of startups and spinoffs	• Target: > 5 companies
Consultations	• Number of consultants • Number of participants	• Target: 20 consultations • 100 participants
Impact demonstration	• Number of indicative use cases	• Target: 20 cases

Table 6 – Exploitation Impact Indicators

4. **Comprehensive Market Analysis**: Our roadmap includes conducting a comprehensive analysis of the healthcare data protection market. This analysis will involve identifying potential customers, evaluating competitors, and monitoring emerging trends. The insights gained from this analysis will inform our project's commercialization strategy and help us tailor our solutions to meet market demands.

5. **Dissemination and Communication**: We will develop a targeted dissemination and communication plan to raise awareness about the SECURED project and its outcomes. This plan will include organizing

workshops, participating in conferences, publishing research papers, and leveraging digital channels. By actively engaging with stakeholders, we aim to share our knowledge, create a broader community in the healthcare environment, and raise general awareness of the SECURED project's aims and objectives.

Throughout the project lifecycle, media communication will play a vital role in raising awareness of the SECURED project and its mission. By disseminating information about our project's progress, achievements, and impact, we aim to foster collaboration and ensure broad stakeholder engagement.

4.4 Exploitation Leader

A crucial role in the overall coordination of the exploitation activities of the SECURED project is played by the **Exploitation Leader**. As described in the Deliverable D1.1 "Project Handbook Quality, Risk Management", the Exploitation Leader coordinates the SECURED exploitation and innovation activities, by monitoring the outcomes of the technical process and matching them to business opportunities. The Exploitation Leader is be responsible for linking with industry beyond the consortium. Finally, in cooperation with Dissemination Leader, the Exploitation Leader defines the optimal communication and dissemination strategies and channels to maximize the impact of the Action.

4.5 Target groups

The exploitation strategy of the project focuses on the following target groups :

- **Public and Private Healthcare Organizations**: These organizations will be our primary early adopters of the project's exploitable results. By collaborating with healthcare organizations, we aim to increase the quality, security, and resilience of medical services and devices. This, in turn, will enhance the security of sensitive patient data processed by these organizations.
- **IoT/Medical Device and Software Manufacturers and Providers**: This target group consists of manufacturers and providers of IoT devices and medical software. They play a crucial role as secondary stakeholders in the project's exploitable results. Our aim is to integrate the solutions developed in the project into their offered products, ensuring that the benefits of the SECURED project extend to a broader range of healthcare technologies.
- **Health Data Analysis Solution Providers**: This group represents the adjacent markets to healthcare, specifically providers of health data analysis solutions. They have the opportunity to adapt selected products from the SECURED project to other use cases, such as ensuring privacy in industrial devices or financial infrastructures. By engaging with these solution providers, we can explore potential cross-industry collaborations and leverage the expertise gained from the project.
- **Scientific Community**: The scientific community, specifically experts in the field of privacy and healthcare practitioners, are essential target groups. By involving the scientific community, we aim to foster collaboration, knowledge sharing, and the exchange of best practices. Their expertise and insights will contribute to the development and validation of the SECURED project's outcomes.

4.6 Assets to exploit

SECURED will deliver a collaboration centric hub system. In those terms, SECURED's exploitation outcomes will include the SECURED services and toolkit, in terms of cost, usability, adaptation and knowledge, consisting of the following the SECURED two flows: data flow, and processing flow, also the capacity to promote, disseminate and communicate the SECURED Knowledge base and the Medical Training. All these tools/services will be very likely part of the exploitable results. Further exploitation could be will be generated through software updates and system upgrade (e.g., basic/ premium package), training and/or technical support and through

maintenance activities. To become more specific, the SECURED project has identified several key assets that will be leveraged throughout the project lifetime to maximize the impact and exploitation of its results. These assets will encompass various aspects of the project's advancements, collaborations, and intellectual property. The exploitable assets will include, but not limited to the following list:

1. **Cutting-Edge Data Anonymization and Generation Techniques**: The project will develop and refine cutting-edge techniques for anonymizing and generating healthcare data. These techniques ensure the protection of sensitive information while enabling the utilization of the data for research and analysis purposes. These innovative approaches provide a valuable asset for healthcare organizations and data processors seeking to enhance data privacy and security.
2. **Compliance with GDPR Regulations**: The SECURED project is fully aligned with the General Data Protection Regulation (GDPR), which sets the standard for data protection and privacy in the European Union. This compliance ensures that the project's outcomes and solutions will adhere to the highest standards of data privacy, instilling trust and confidence in healthcare data hubs and their stakeholders.
3. **Cross-Sector Collaboration Networks**: The project actively promotes cross-sector collaboration, bringing together experts from the fields of cybersecurity, healthcare, data privacy, and technology. The established collaboration networks serve as valuable assets for further exploitation, fostering knowledge exchange, and enabling the transfer of expertise between sectors. These networks provide opportunities for future collaborations, joint ventures, and knowledge sharing initiatives.
4. **SECURED Innohub**: The SECURED project will established the SECURED Innohub, which serves as a legal compliance framework supporting EU legislation related to health data protection. This Innohub will act as a central reference point and resource hub for healthcare organizations, providing guidance and best practices in managing health data securely. It offers a valuable asset to stakeholders seeking to ensure compliance and gain insights into legal and regulatory requirements.
5. **Research and Innovation Capacities**: The SECURED project will significantly enhance the research and innovation capacities in the field of health data protection. The project will contribute to advancing the scientific knowledge, developing state-of-the-art technologies, and establishing best practices in the domain. These research and innovation capacities will serve as valuable assets for stakeholders looking to stay at the forefront of health data protection and leverage the latest advancements in the field.

By effectively exploiting these assets, the SECURED project aims to create tangible and sustainable benefits for stakeholders, including improved data privacy and security, increased quality of healthcare services, enhanced compliance with regulations, foster collaboration, and opportunities for business growth and innovation.

5 Means & activities to raise Awareness of SECURED

This section outlines all the available tools and mechanisms for the SECURED's project dissemination and awareness. Some of them are summarized from Deliverable D1.1 and Deliverable D1.7 and reported here for completeness.

5.1 Dissemination and Communication Toolkit

5.1.1 Project Logo

The project uses the logo, depicted in Figure 2, as a key element of the overall SECURED Project dissemination material which aims to provide a concrete project identity. The scope of its design is no other than to capture the concept behind the SECURED project, and the context of its use cases which navigated the description of the Pilots and defined the expected results. The logo will be used for any dissemination activity and created content.

Figure 2 – The SECURED Project Logo

5.1.2 The project website

As outlined in D1.7, the website contains all the essential information concerning the project and will be constantly updated with produced material, news, photos, etc. The SECURED website will be an essential tool for presenting the project and fostering communication between all project entities. The website will present the project's progress to the scientific, academic and technical communities, and overall, to promote and make visible the intermediate and final outcomes to the general public, thus facilitating collaboration between the project partners, stakeholders and the rest of the audience. The SECURED project website has been designed and developed by ISI and available at this link: https://secured-project.eu/

The website features a user-friendly design and is easily accessible to all stakeholders. Its primary purpose will be to disseminate information about the project in a timely and efficient manner. This includes publishing

all dissemination materials, which will be updated throughout the project duration. Additionally the project website will contain a link to the SECURED Innohub, which will include the SECURED Framework software, the SECURED Knowledge Base and all other publicly available outputs of the project, as well as information about the Open Calls.

SECURED's website provides an overview of the Work Packages and the Deliverables to ensure that the visitors stay informed about the project's progress. Additionally, an RSS service and Social Media accounts have been created to provide the user with easy access to the project's proceedings and to remind them on a regular basis at the frequency they prefer.

5.1.3 Social Media Accounts

Social media is a very important and vital outlet for enhancing communication, increasing project visibility and providing constant updates for the achievements of the project key objectives. The project to reach as much an audience as possible has created accounts on the most widely used social media channels, in regards to the target group and target goal, dissemination and exploitation. Table 7 reports the social media platforms created and their links.

Social Media	Link
YouTube	https://www.youtube.com/@securedeuproject
Twitter	https://twitter.com/SecuredEU
Facebook	https://www.facebook.com/securedeuproject
LinkedIn	https://www.linkedin.com/company/secured-project/

Table 7 – Social Media Channels

The YouTube channel will be populated with videos regarding relevant research activities, pilot-related videos, tutorial videos, webinars, videos from paper presentations from conferences and any commercial promotional material that will further broadcast SECURED project pilots, synergies as well as their benefits for end users and stakeholders. All postings on the YouTube channel will be performed by the dissemination leader. The YouTube channel is currently without content as the project is at a very early stage, yet accessible at `https://www.youtube.com/@securedeuproject`.

The Twitter page will be used for communication with related stakeholders and actors through networking, short updates on project news (tweets) and announcement of upcoming or completed activities. All postings on the twitter account will be performed by the dissemination leader. The project website has the appropriated functionality integrated for real time updates of the twitter account. The twitter account is currently publicly available at `https://twitter.com/SecuredEU`.

The Facebook page channel has been set up to spread information to the general public. The Facebook account will be used for public project communication in the form of text, pictures and videos from project meetings as well as dissemination and publicly available exploitation activities such as participation and presentation in conferences, attendance in forums, workshops, tutorials etc. All postings on the Facebook page will be performed by Dissemination Leader. The Facebook page is currently populated with a minital information about the project, as the project is at a very early stage, yet accessible at `https://www.facebook.com/securedeuproject`.

The LinkedIn page as a social media targeting mainly the professional networks and communities of Linkedin will be used for disseminating project results. The project's Linkedin page is accessible at `https://www.linkedin.com/company/secured-project/`.

As discussed before, all social media channels will be updated regularly by the Dissemination Leader in order to ensure that the content is current and accurate and will include all relevant information, photos and updates on the project's on-going activities.

Consortium members using their own social media accounts are encouraged to mention the SECURED project with **@SecuredEU** for Twitter, and mention **@secured-project** for use in LinkedIn. Additionally, it would be

beneficial to use the hashtags **#cybersecurity**, **#privacy** and any keyword relevant to the topic.

5.1.4 Online repository

During the course of the project, selected items will be offered as open source tools or solutions. These will be available on open online repository supporting versioning. The availability of open source tools will provide avenues both for dissemination and exploitation activities by displaying possible solutions to real problems. The public repositories will be linked from the project website and advertised in the relevant social media.

5.1.5 Printable Material

Alongside the digital material, the project will develop a series of printable material to enhance public engagement. These include posters, leaflets, newsletters, fact sheets, flyers, stickers and brochures.

5.2 Planned Dissemination and Communication Activities

5.2.1 Publications

Promoting a project within the scientific and research community can be effectively achieved through the development and publication of scientific papers in conferences, journals, and magazines. In line with this strategy, the SECURED project aims to disseminate its findings through top tier scientific journals and conferences.

Table 8 outlines examples of targeted Journals and Conferences

IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)
IEEE Hardware Oriented Security and Trust (IEEE HOST)
IEEE Transactions on Industrial Informatics
International Symposium on Research in Attacks, Intrusions and Defenses (RAID)
Springer Journal of Cryptographic Engineering (JCEN)
Springer Journal of Hardware and Systems Security
IEEE Transactions on Information Forensics and Security
IJCAI International Joint Conference on Artificial Intelligence
ACM Conference on Fairness, Accountability, and Transparency
International Cross-Domain Conference for Machine Learning and Knowledge Extraction
Journées Des Statistiques
Privacy Enhancing Technologies Symposium (PETS)
IEEE Transactions on Big Data
ACM Conference on Computer and Communications Security (CCS)
IEEE Journal of Biomedical and Health Informatics
IEEE Transactions on Medical Imaging
IEEE Open Journal of Engineering in Medicine and Biology
IEEE Transactions on Biomedical Engineering
IEEE Open Journal of Engineering in Medicine and Biology
Future Generation Computer Systems

IEEE Transactions on Parallel and Distributed Systems
Engineering Applications of Artificial Intelligence
High Performance, Edge And Cloud computing (HiPEAC)

Table 8 – Targeted Journal/Conferences

5.2.2 Events

The SECURED project will setup a series of events such as workshops, webinars, training sessions, open days and demonstrations tailored to the project's specific objectives. Stakeholders, such as healthcare and cybersecurity companies, associated with the project's goals will be actively invited and involved in these events. The purpose of these events is to disseminate information and outputs of the project.

Specifically, open and info days will provide potential stakeholders with necessary information and introduction to the project and its outcomes as well as serve as a means to create awareness, promote dialogue, and generate enthusiasm. Tutorials and Webinars will provide real-time and on-demand information to stakeholders. Workshops and demonstration events will be performed to real-time showcase the results and usage of the available tools of the SECURED architecture tools, achieved during the project's course. Finally open calls will actively engage stakeholders by utilizing all the available SECURED tools.

The intent is to inform, generate early interest, familiarization and engagement among key stakeholders, enabling them to witness the tangible outcomes and understand the practical implications of the project.

To allow for more thorough discussion regarding the use cases of the SECURED project in relation with the initial sketch of the architecture, the first end user workshop, originally planned for M3, was held in conjunction with the project general assembly in Barcelona on the 13 of June 2023.

The following open days and workshops, showcased in Table 9, have been initially planned for the duration of the SECURED project. More will be planned in the future in accordance to the KPIs defined in section 6.

Type	Month	Description
Demonstration Workshop	M20	SEM in Hungary, after the deployment of the 1st prototype
First Open Day	M28	HNJ to be held in Madrid after deployment of 2nd prototype
Second Open Day	M32	EMC to be hald in the Netherlands to demonstrate real use case deployment
Second Demonstration Workshop	M36	JCLRI in Spain, after the deployment of the 2nd prototype

Table 9 – Planned open days and workshops

5.3 Collaboration with other projects and initiatives

A fundamental part of the dissemination and exploitation activities is the collaboration with other project financed within the same call (or within the same cluster) and with other projects sharing the same goals.

Activities in this direction have been kicked off with a virtual meeting in March 2023. Envisioned form of collaboration include common organization of workshops, schools, tutorial or special session, common discussion about use case and developed technologies and cross-dissemination of project results.

6 Dissemination Monitoring

Key Performance Indicators (KPIs) are an quantifiable measure of performance over time that can be utilized to assess the execution of the dissemination and exploitation plan.

The following KPIs, depicted in Table 10 have been defined, covering all the necessary portions of the projected outcomes of the project and will server as a comprehensive evaluation of the dissemination and exploitation success.

KPIs	Description	Quantitative Measure	Target Audience
KPI1	SECURED Website	Distinct Visitors >= 2000	Health sector, general public, scientific & research community, public sector
KPI2	Twitter followers	Followers >= 150	Health sector, general public, scientific & research community, public sector
KPI3	Facebook followers	Followers >= 100	Health sector, general public, scientific & research community, public sector
KPI4	Linked Members	Members >= 100	Health sector, general public, scientific & research community, public sector
KPI5	Instagram followers	Followers >= 100	Health sector, general public, scientific & research community, public sector
KPI6	Videos & Webinars	Videos and Webinars >= 7	Health sector, general public, scientific & research community, public sector
KPI7	Videos & Webinars	Number of people viewing videos and webinars >= 200	Health sector, general public, scientific & research community, public sector
KPI8	Brochures & Leaflets	Number of brochures and leaflets >= 2	Health sector, general public, scientific & research community, public sector
KPI9	Newsletters	Number of newsletters >= 4	Health sector, general public, scientific & research community, public sector
KPI10	Newsletters	Number of subscription to newsletters >= 50	Health sector, general public, scientific & research community, public sector
KPI11	On site demonstrations	Number of on-site demonstrations >= 3	Industry and research
KPI12	On site demonstrations	Number of people attending on-site demonstrations >= 20 per event	Industry and research

KPI13	Active participation in conferences and other events	Number of conferences and events >= 20	All SECURED partners will participate in European and international conferences. Academic partners will organise special sessions and workshops in EU and International conferences
KPI14	Peer reviewed journal publications	Number of peer reviewed journal publications >= 10	Articles on magazines, technology roadmaps, and industry-led journals. The scientific publications will facilitate the efforts of professionals and researchers.
KPI15	Workshops/Tutorials	Number of workshops and tutorials organized >= 2	Organisation of Health sector focused events (i.e., workshops, symposiums, demonstrations, trainings, etc.) to disseminate project outcomes.
KPI16	Workshops/Tutorials	Number of participants >= 20 per event	Organisation of Health sector focused events (i.e., workshops, symposiums, demonstrations, trainings, etc.) to disseminate project outcomes.
KPI17	Co-operation with other initiatives	Number of collaborations with other projects and initiatives >= 3	Other EU projects, additional stakeholders.
KPI18	Healthcare providers involved	Number of healthcare providers validating SECURED framework and the Innohub >= 8	Organisations of Health sector
KPI19	Open Call participation	Number of healthcare open call participants >= 10	Health sector, general public, scientific & research community, public sector

Table 10 – SECURED Dissemination and Communication KPIS

6.1 Means to measure progress

To ensure the dissemination and communication activities, consortium partners will be required to provide input to the dissemination leader (ISI) for monitoring and evaluating the specified KPIs. To this end a robust and systematic process has been implemented. This process involves simple to follow rules based on different type of dissemination and involve use of web forms that serve as a centralised hub for partners to report and provide information about their dissemination activities.

ISI as the dissemination leader has prepared online forms for partners to report publications and events to be collected and processed for the purposes of monitoring KPIs. Figure 3 shows an excerpt of the publication form required by the consortium members to disclose relevant information and Figure 4 shows an excerpt of the event form required by the consortium members to disclose relevant information. Each partner is required to use the forms in a timely way to report their dissemination activity.

When a partner creates something interesting such as software, prototype, infographic, webinar, video, course, seminar, the partner must maximize its impact by informing the WP1 Dissemination leader (ISI) by email in order to be included in the upcoming newsletter or social media feed.

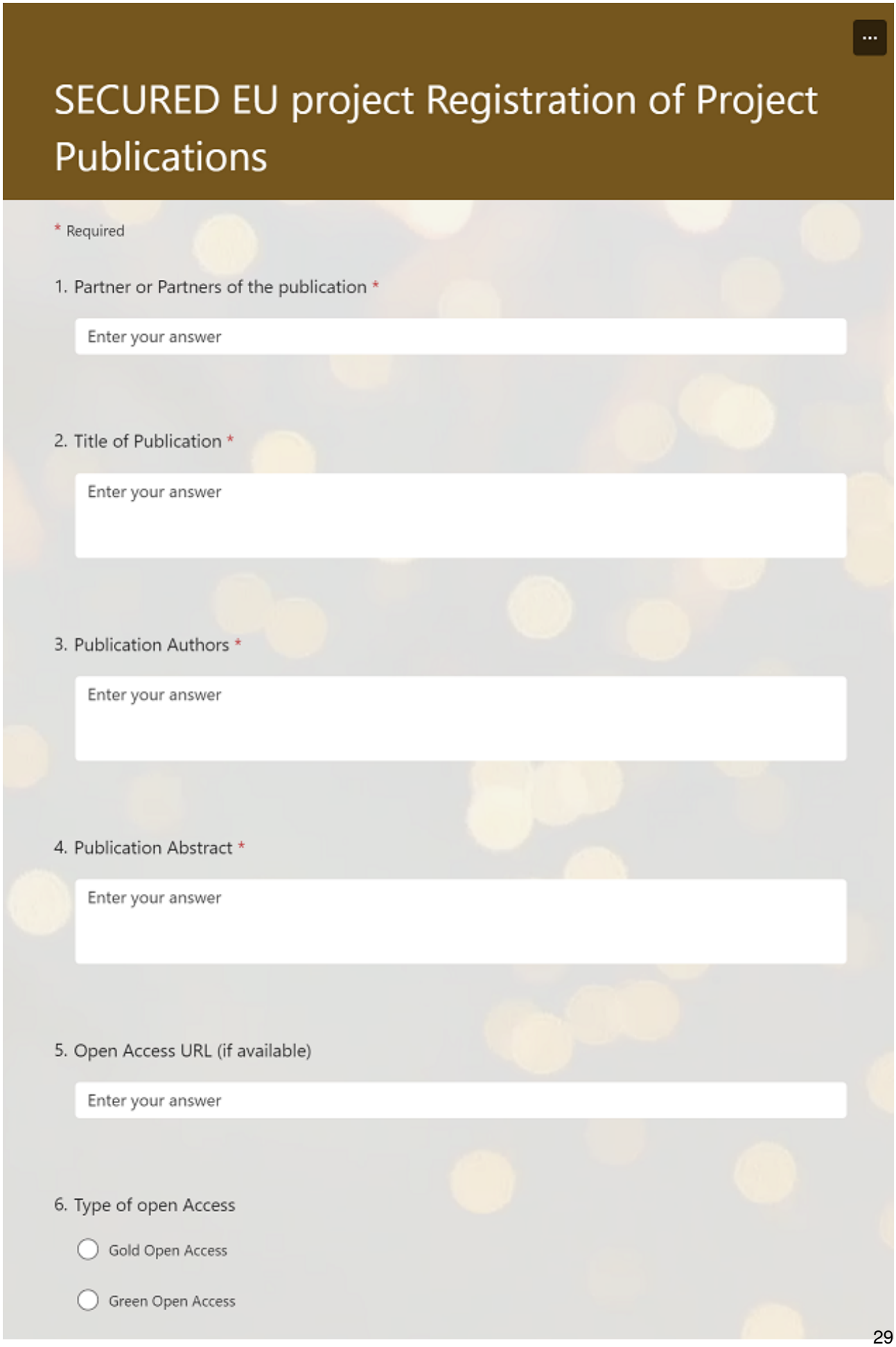
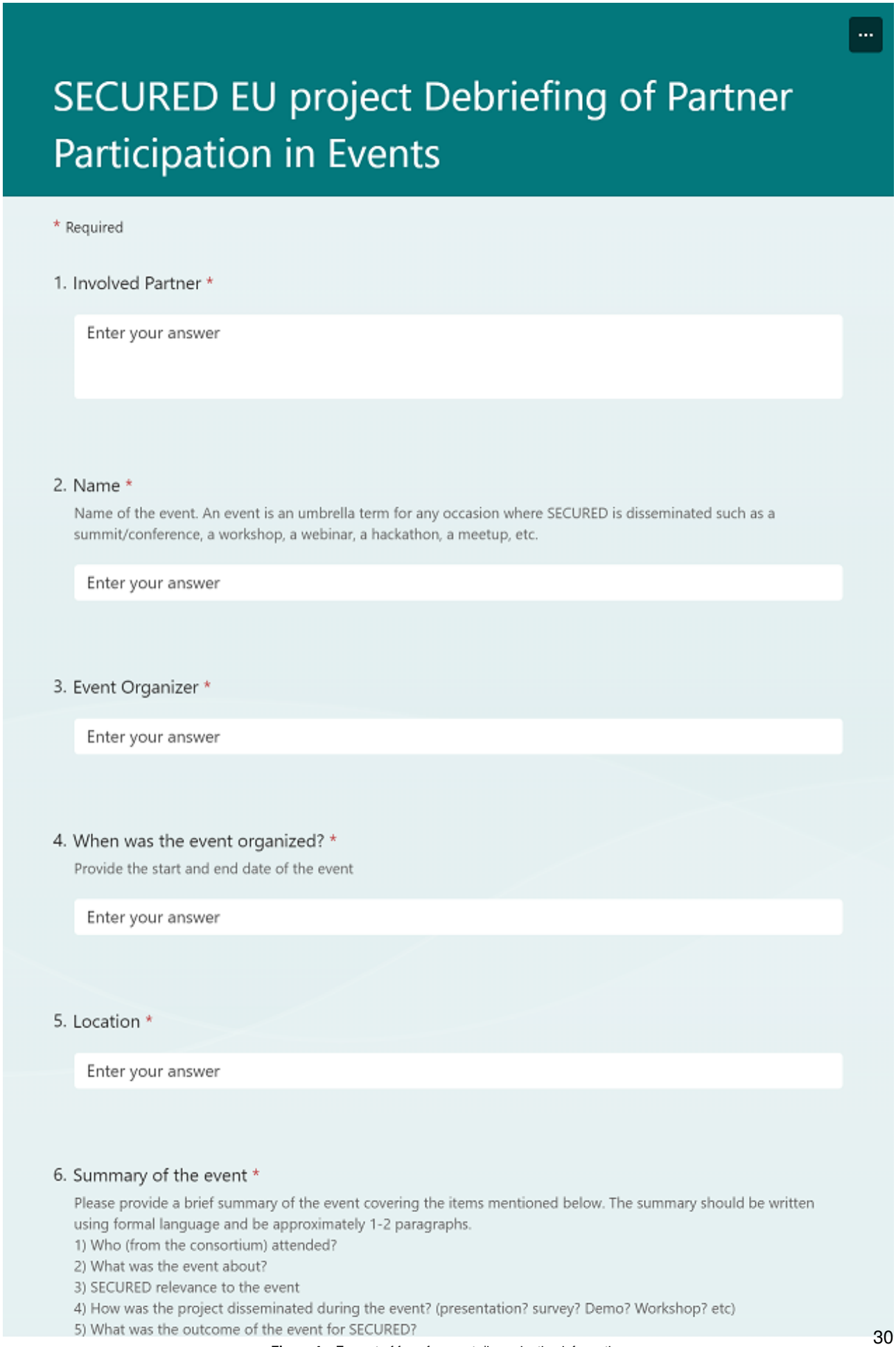


Figure 3 – Excerpt of form for publication dissemination information



SECURED EU project Debriefing of Partner Participation in Events

* Required

1. Involved Partner *

Enter your answer

2. Name *

Name of the event. An event is an umbrella term for any occasion where SECURED is disseminated such as a summit/conference, a workshop, a webinar, a hackathon, a meetup, etc.

Enter your answer

3. Event Organizer *

Enter your answer

4. When was the event organized? *

Provide the start and end date of the event

Enter your answer

5. Location *

Enter your answer

6. Summary of the event *

Please provide a brief summary of the event covering the items mentioned below. The summary should be written using formal language and be approximately 1-2 paragraphs.
1) Who (from the consortium) attended?
2) What was the event about?
3) SECURED relevance to the event
4) How was the project disseminated during the event? (presentation? survey? Demo? Workshop? etc)
5) What was the outcome of the event for SECURED?

Figure 4 – Excerpt of form for event dissemination information

7 Conclusions

In a nutshell, the current document includes a detailed plan for the dissemination and exploitation of the SECURED project. It provides a comprehensive overview of the objectives, roadmaps, roles and responsibilities associated with the strategy. Furthermore, it details the diverse range of means and activities employed to effectively raise awareness of the project.

The document highlights the dissemination and communication toolkit, which includes a variety of resources and channels utilized to convey project-related information, as well as the necessary means for the dissemination leader to collect all of the information to efficiently promote the SECURED project.

This document also highlights and enumerates all necessary monitoring KPIs for measuring the project's advancements to serve as a guide for consortium members on what should be achieved.

Finally, it must be emphasized that the dissemination strategy is an ongoing process moving along as the project progresses over time. To this effect, the dissemination goals will be regularly monitored and updated to ensure their relevance and effectiveness. Adjustments to this plan are expected to occur within the project's lifetime in order to always be in alignment with the objectives and KPIs. These adjustment will be timely reflected in the dissemination plan.

A Assets to Disseminate

SECURED Tools and Services	Description
SMPC hardware assisted software library	The library will offer support to the SECURED Infrastructure and can be used by involved parties to implement an SMPC compatible application operating as part of a SECURED collaborative cluster. The SECURED SMPC library will support highly scalable SMPC solutions by using the concept of cloud based SMPC and using dedicated hardware accelerated components for heterogenous MPSoC systems (that include multiple CPU cores, GPGPUs and FPGA fabric). The SECURED SMPC library will be compliant with the two-tier scalability enhancement infrastructure of the SECURED infrastructure and will be operational in both high-performance computing settings (in server units) as well as low performance setting (in edge or embedded system devices).
SMPC Transformation	This tool will be used to analyse/profile an existing AI based Data Analytics solution, identify the components that can be made SMPC compliant and using the SMPC software library to transform the existing solution into a SECURED compliant tool that can operate collaboratively within a SECURED cluster using that private datasets of the cluster's parties and the SECURED Federation
Anonymization tool	This tool is offered to SECURED Innohub members, developed using beyond the state of the art techniques researched in the project, to be used at the member's premises. This tool will anonymize private datasets and AI models before sharing with other parties or the SECURED Innohub knowledge base. This tool can also be part of the data flow or/and the processing flow of the project. The resulting anonymized datasets are registered in the data lake inventory of the SECURED knowledge base to be further accessed by the Innohub members.
Anonymization assessment tool	This tool is meant to assess the level of anonymity that is achieved in an anonymized dataset (been created with external tools, synthetic data generators or with the SECURED Anonymization tool). The "privacy risk assessment" followed in the tool rely on advanced de-anonymization techniques meant to retrieve information about the actual dataset from it's anonymized version as well as any privacy related attack that has been reported in the research literature.
Dataset Bias quality assessment and Dataset Unbiasing tool	Given a specific health dataset, the Bias assessment tool will aim at identifying how biased the dataset is and produce a bias score that will afterwards be associated with the dataset. An extension of this tool is the Unbiasing mechanism that is using the Synthetic Data Generation infrastructure in order to enhance a biased dataset with synthetic data in order to reduce the bias score.
Privacy preserving AI trained model "marketplace"	This service of the SECURED Innohub is acting as the front end of the SECURED AI model lake that includes series of anonymized, unbiased, trained models that have been produced by the SECURED federation. The service allows the Innohub members to search (through the SECURED Knowledge base capabilities) for specific AI models given the metadata that accompany such models, download the models in a given model format (eg ONNX format) and use them.

Anonymization decision support service	Given the various different anonymization techniques that are researched in SECURED that can be confusing for end users, in SECURED we provide a decision support mechanism to assist in choosing the appropriate anonymization technique that best fits the characteristics of a health dataset
Synthetic Data Generator	This service can act as the front end of the SECURED Synthetic Data generation infrastructure and provides "synthetic data-as-a-service" support to SECURED Innohub members. The involved parties can add their specifications regarding the dataset to be generated (they may include also an initial anonymized actual dataset) and the service will generate a high volume synthetic datasets that follows user's specifications.
Cross-border data processing legal compliance and GDPR compliance	Given that EU Health data hubs operate in various EU countries and also given that each dataset may have special characteristics, specifying the legal/GDPR framework under which such dataset can be used is very crucial. This becomes significantly important when considering the fact that datasets are been collaboratively processed through an SMPC scheme. The SECURED Innohub based on the characteristics of the dataset, their storage country, the used anonymization techniques and/or the SMPC schemes (as they scale up), will provide as a service the legal framework that is associated with such dataset.
Health sector Medical Education	This service extends the synthetic data generation service by generating datasets specifically for medical education (eg. training medical students on how to identify from datasets specific health problems).
SECURED Innohub	The SECURED Privacy-enhancing Hub that will provide all tools, services, and overall support to external involved third parties of the healthcare domain, including researchers, Innovators or Health Data users as well as EU data Hubs across Europe, thus facilitating them to perform accurate data analytics in a distributed and private matter.
SECURED Knowledge base	The consolidated knowledge and its representation that is accumulated in the SECURED Innohub solution. This includes 3 different data lakes, the SECURED Synthetic data lake, the SECURED data inventory and the SECURED AI model lake.

Table 11 – SECURED Assets to Disseminate

References

[1] "SECURED cordis announcement," https://cordis.europa.eu/project/id/101095717, accessed: 2023-01-01.