CYBERHIMPREX
Cybersecurity of Healthcare
Improved in a X-border perspective

Project Title	**Cyber**security of **H**ealthcare **Impro**ved in a **X**-border perspective
Project Acronym	CYBERHIMPREX
Project Number	101101322
Type of action	DIGITAL-SME Digital SME Support Actions
Topic	DIGITAL-2022-CYBER-02-SUPPORTHEALTH-Support To Cybersecurity In The Health Sector
Starting date of Project	01/01/2023
Duration of the project	24
Website	https://cyberhimprex.policlinicogemelli.it

D1.3 1st Communication, Dissemination, Exploitation plan

Work Package	WP 1 Project coordination
Lead author	Pasquale Mari (FPG)
Contributors	Diana Navarro Llobet (FPHAG), Aimilia Magkanaraki (7HRC)
Peer reviewers	Sabina Magalini (FPG), Marc Jofre Cruanyes (FPHAG)
Version	1.0
Due Date	30/06/2023
Submission Date	30/06/2023

Dissemination Level:

x	PU — Public
	SEN — Sensitive
	R-UE/EU-R — EU Classified
	C-UE/EU-C — EU Classified
	S-UE/EU-S — EU Classified

The work described in this document has been conducted within the CYBERHIMPREX project.
This project has received funding by the European Union Digital Europe Programme (DIGITAL)
under grant agreement No. 101101322.

Version History

Revision	Date	Editor	Comments
0.1	22/06/2023	Pasquale Mari (FPG)	
0.2	23/06/2023	Sabina Magalini (FPG)	Review
0.3	28/06/2023	Marc Jofre Cruanyes (FPHAG)	Review
0.4	28/06/2023	Marc Jofre Cruanyes (FPHAG), Aimilia Magkanaraki (7HRC)	Additional content from FPHAG (activities performed up to M6) and 7HRC (Greek target stakeholders)
1.0	30/06/2023	Pasquale Mari (FPG)	Document Closed

List of Contributors

The list of contributors to this deliverable are presented in the following table:

Section	Author(s)
1, 2, 3	Pasquale Mari (FPG)
4	Pasquale Mari (FPG), Diana Navarro Llobet (FPHAG)
5	Pasquale Mari (FPG),
6	Pasquale Mari (FPG), Diana Navarro Llobet (FPHAG), Aimilia Magkanaraki (7HRC)
7-8	Pasquale Mari (FPG)
9	Saverio Caruso (FPG)
10	Pasquale Mari (FPG),

Keywords

Dissemination, communication, exploitation, lessons learned, stakeholders, communication channels, dissemination channels

Disclaimer

This document contains information which is proprietary to the CYBERHIMPREX consortium. This document the information contained herein can be used, duplicated or communicated by any means to any third party, in whole or parts, only if the source is cited and visibility is given to the CYBERHIPREX project and to the funding mechanism (Digital Europe Programme) and to the funding authority (European Union) and only if the dissemination level is public and no other restrictions or classifications are indicated.

Executive Summary

The document describes in detail target groups, main messages, tools, and channels which are planned in order to promote communication and dissemination the activities/results and maximise the impact. It also defines how the results of the project will be exploited.

Communication and dissemination activities are based on three entities:

- **10 Intermediate Target groups**, i.e. groups of organizations/associations the allow to reach the real people that are the target recipients of the project's information and results (e.g. professional associations, healthcare authorities).
- **10 Final Target groups**, i.e. the groups of real people, e.g. Chief Information Security Officers (CISO) and Information Technology Directors of Healthcare Organizations (HCOs).
- **9 types of communication and dissemination channels**, i.e. the vehicles to transfer information and results to the real people (e.g. the project website, webinars, events); five of them will be used mainly for communication (e.g. the project website), four of them mainly for dissemination (e.g. the webinars).

The communication and dissemination strategy consists in performing three types of activity:

1) **Focused engagement activities** aimed at engaging the intermediate stakeholders and, indirectly, their members
2) **Communication activities** aimed at i) engaging the Final stakeholders that are not reached via the Intermediate stakeholders and ii) communicating content on the project and its results (in a non-technical format)
3) **Dissemination activities** towards all the Final stakeholders that will have been engaged (either via Intermediate stakeholders or the "broadcast" communication channels)

Activities 1) and 2) have already started and a plan until M18 is provided

Activity 3), dissemination, has not yet started because the project has not yet delivered results; when results will be available, the dissemination will be performed via the channels that are most suitable for dissemination. The dissemination activities planned until M18 are provided.

The **exploitation** of the project's results will mainly consists in the fact that the three HCOs of CYBERHIMPREX will use the solutions adopted through the initiatives

An additional thread of exploitation regards the results of initiatives that involve third parties and/or deserve to be adopted by other HCOs. The analysis of the initiatives has shown that 7 of the 11 initiative produce results that can be transferred to other HCOs

For each initiative, when it ends, a *post-initiative "exploitation process"* will be described, in order to embed the solution in the routine cybersecurity activities of each of the three participant HCOs.

The nature of exploitation activities (e.g. renew the licenses activated during the project) included in the *post-initiative "exploitation process"* depends on the type of initiative, as follows. Seven categories of initiatives have been identified:

A. Initiatives that reduce the vulnerability of the technology
B. Initiatives that reduce the vulnerability of the people
C. Initiatives with pilots.
D. Initiatives that require the adhesion of third parties
E. Initiatives that inject new know-how in the HCOs
F. Initiatives that set-up a new organization or process
G. Initiatives that produce results that deserve to be adopted by other HCOs across Europe.

An initiative may belong to more than one of the above seven categories.

Table of Contents

List of figures

List of tables

1. Introduction

1.1 Scope and purpose of the document

This document has the purpose to describe in detail target groups, main messages, tools, and channels which are planned in order to promote communication and dissemination of the activities/results of the CYBERHIMPREX project and maximise its impact.

It also provides a high level description of the expected use that the three Healthcare Organizations (HCOs) that are partners of the CYBERHIMPREX project will do to exploit the output of the initiatives. More detailed description will be provided in D1.6-2nd Communication, Dissemination, Exploitation plan, due in M18.

1.2 Objects of the communication, dissemination and exploitation activities

The communication, dissemination and exploitation activities of the CYBERHIMPREX project regard two main objects:

- The project: its structure and objectives, the consortium members, its funding mechanism, the lessons learned during its implementation. Table 1 summarizes its key features

Table 1 Key features of the CYBERHIMPREX project

PARTNERS

ITALY (Rome)

- UCSC-Università Cattolica del Sacro Cuore (Coordinator)
- FPG-Fondazione Policlinico Universitario A. Gemelli IRCSS (Private University and Research Hospital)

GREECE (Crete)

- 7HRC-Seventh Healthcare Region of Crete

SPAIN (near Barcelona)

- FPHAG-Fundació Privada Hospital Asil de Granollers (University Hospital)

PURPOSE

- Improving the cybersecurity capabilities of the three Healthcare Organizations (FPG, 7HRC,FPHAG) also by the adoption of innovative solutions, in a cross border perspective

TIMING

- January 2022-December 2024

VALUE AND FUNDING

- 2,7 Million € , EU funding 50% by the Digital Europe programme

- The 11 initiatives of the project: their content and their results. Table 2 lists the initiatives, the adopting Healthcare Organizations (HCOs) and the adopted innovative solutions[1] is provided in Table 2

[1] The innovative solutions have been developed mainly in two H2020 projects (PANACEA and CUREX). One solution, taken from the ECHO project, will be taken into consideration as a possible training method. The meaning of the acronyms is provided in Table 5

Table 2 The 11 CYBERHIMPREX initiatives

Investment areas and Lines of intervention		HCOs and [Initiatives]			Solution (EU Project)
		FPG	FPHAG	7HRC	
Cross border Data/Knowledge sharing					
1	Set-up a cross-border inter-organizational secure data sharing capability via a new tool.	[1]	[1]		SISP (PANACEA)
People					
2	Improve cybersecurity skills of technical staff, via multi-method training	[2]		[3]	NCSF (CUREX), AWA (ECHO)
3	Raise cybersecurity staff awareness via customized nudging and education pills	[4]			SBNT, TECT (PANACEA), CH (CUREX)
4	Set-up the new cybersecurity "angel" role via dedicated training	[5]			RGT (PANACEA)
Organization/Processes					
5	Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines	[6]	[6]		
6	Improve the cybersecurity governance organization and system via a stakeholder involvement approach and new tools	[7]			RGT (PANACEA)
Technology					
7	Improve web navigation system security via *web proxy*.	[8]			
8	Improve business continuity via an immutable backup system.	[9]			
9	Reduce the Attack Surface via Operating Systems (OS) update	[10]			
10	Improve Security by Design capability via new supporting tools	[11]			SDSP, CST (PANACEA)

1.3 Structure of the document

The document is structured in the following manner:

- Sections 1, 2 and 3 provide introduction, sources and acronyms
- Section 4 provides an indication on the organizational arrangements in the project for performing the communication, dissemination and exploitation activities.
- Sections 5, 6 are dedicated to communication and dissemination, in terms of framework and actions performed so far (M6) and planned until M18
- Sections 7 and 8 is dedicated to exploitation, in terms of framework and activities planned until M18.
- Section 9 examines the ethical and data management aspects
- Section 10 draws the conclusions.

2. Applicable documents and sources

The following documents contain requirements applicable to the generation of this document:

Table 3 Applicable documents

Reference	Document Title	Document Reference	Version	Date
[GA]	Grant Agreement 101101322	Description of Action	Ares 2022 8813177	19/12/2022
[D1.1]	Ethics Monitoring Plan	CYBERHIMPREX deliverable	v1.0	28/02/2023
[D1.2]	Project Website	CYBERHIMPREX deliverable	V1.0	28/02/2023

The following sources of information/data have been used to draft this document:

Table 4 Sources

Reference	Document Title	Document Reference	Version	Date
[CODE1]	Nuovo Codice degli Appalti, dlgs 36/2023	https://www.gazzettaufficiale.it/eli/id/2023/04/13/23A02179/sg		31/03/2023
[CODE2]	La cyber security entra nel Codice Appalti: perché è un cambio di passo fondamentale	Article of L. Franchina, T. Ruocco published on Agenda Digitale https://www.agendadigitale.eu/procurement/la-cyber-security-entra-nel-codice-appalti-perche-e-un-cambio-di-passo-fondamentale/?utm_campaign=agenda_nl_20230429&utm_source=agenda_nl_20230429&utm_medium=email&sfdcid=0030O000002LZ3tpQAD		28/04/2023

3. Glossary of Acronyms

Table 5 Acronyms

Acronym	Description
AWA	Hands-on Cyber Awareness
CH	Human-centric Cyber Hygiene
CISO	Chief Information Security Officer
CST	Security by Design- Compliance Support Tool
EH ISAC	European Health Information Sharing and Analysis Centre
FPG	Fondazione Policlinico Universitario A. Gemelli IRCSS
FPHAG	Fundació Privada Hospital Asil de Granollers
HCO	Healthcare Organization
IT	Information Technology
NCSF	Network and Computer Security Fundamentals
SBNT	Secure Behaviour Nudging Tool
SDSP	Security by Design- Secure Design Support Platform
SISP	Secure Information Sharing Platform
SME	Small and Medium Enterprise
TECT	Training & Education for Cybersecurity Tool
UCSC	Università Cattolica del Sacro Cuore
7HRC	Seventh Healthcare Region of Crete

4. Communication, dissemination, exploitation: organization

In the CYBERHIMPREX project the communication, dissemination and exploitation activities are ensured by Task 1.4.

FPG is the task leader. FPHAG and 7HRC contribute to the activities.

This task has activated the project website (at M2, https://cyberhimprex.policlinicogemelli.it as described also in [D1.2]) and activates/manages the other communication channels.

The task will promote/look for dissemination occasions and will perform them.

The task elaborates a common approach for the exploitation activities.

The task delivers the first plan for Communication, Dissemination, and Exploitation at M6 (this document, D1.3), and an update at M18 (D1.6).

5. Communication and dissemination: framework

5.1 Purpose, positioning message, content scope

Communication

Communication activities will have the **purpose** to Raise awareness about the CYBERHIMPREX project and its objectives and its link with the Digital Programme to stakeholders that might be interested in knowing how the Digital Programme works and/or may be targeted by the dissemination activities.

Communication prepares the audience for the dissemination activities and also for future exploitation, i) engaging the relevant stakeholders, including healthcare professionals, researchers, policymakers, and industry experts, ii) fostering collaboration and knowledge exchange within the cybersecurity and healthcare sectors

The **key positioning message** is that: "*we are a group of European HCOs that have decided to improve their cybersecurity capability adopting innovative solution developed by European project, making synergy and exchanging best practices: we want to share our learnings*".

The **content scope** of the communication regards information on i) CYBERHIMPREX project (e.g. goals, partners, CYBERHIMPREX partners' actions regarding the project such as participation to events as speakers, articles) ii) its results (in a non-technical format) iii) events, news, documents/videos regarding the cybersecurity applied to the health sector that can engage the target stakeholders

In the context of the purpose, positioning message and content scope, for each target group/stakeholder specific messages and contents will be defined.

Dissemination

Dissemination activities will have the **purpose** to share results, best practices and lessons learned with the relevant stakeholders.

The **key positioning message** will be "*CIBERHIMPREX is/has been an excellent opportunity for building a European success story that can be used to boost cybersecurity improvement across European Healthcare Organizations*".

With regard to the **content scope**, It is worth noting that CYBERHIMPREX's main result consist in reducing areas of cybersecurity weakness of the involved HCOs. Therefore the confidentiality level on the detailed results need to be high. That's why the dissemination activities will be *focused more on "process" and "methods" than on the "results"*. However, even if it is not a research project, it acts as "early adoption" model because adopts some new results of research projects. Public results of this adoption and the adoption process "per se" will also provide content for dissemination

In the context of the purpose, positioning message and content scope, for each target group/stakeholder specific messages and content will be defined.

5.2 Strategy to reach and engage the target stakeholders

In order to reach the communication and dissemination purposes it is necessary to engage the appropriate stakeholders and to use the appropriate channels to share information and content.

We aim to reach real people that can use information and content according to the role that they play in their organization. We name these people as “**Final Targets**”.

In order to reach them, we plan to leverage their membership to entities that are expected to find interesting the CYBERHIMPREX project and its results. We name these people as “**Intermediate Targets**”.

Once we have engaged, by a direct contact, an Intermediate Target, we can reach through them their members, i.e. the relevant “Final Targets”, and share with them the information/content using the appropriate **Channels**. Obviously, we will operate also to engage via the channels themselves the Final Targets’ people (eg. readers of on-line journals, participants to events, readers of scientific journals).

Figure 1 shows the channels, the types of Intermediate and Final Targets and their key relationships.

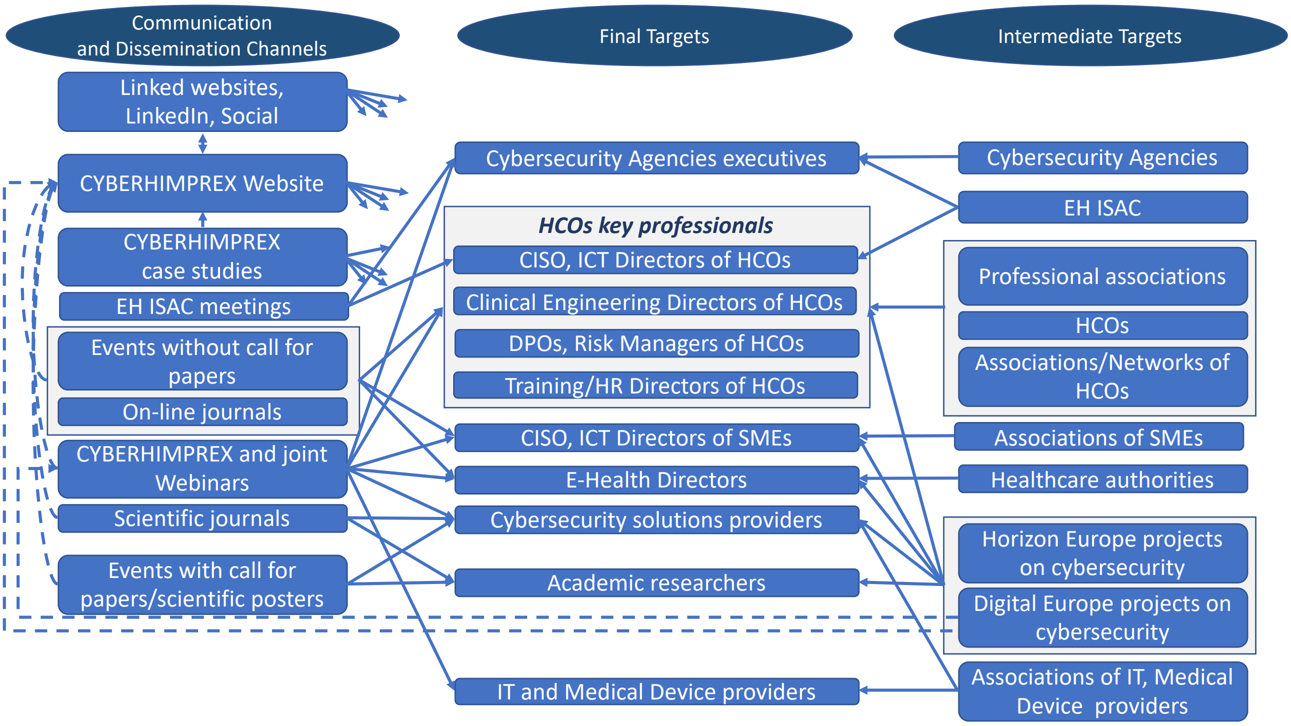

Communication and Dissemination Channels
Final Targets
Intermediate Targets
Linked websites, LinkedIn, Social
CYBERHIMPREX Website
CYBERHIMPREX case studies
EH ISAC meetings
Events without call for papers
On-line journals
CYBERHIMPREX and joint Webinars
Scientific journals
Events with call for papers/scientific posters
Cybersecurity Agencies executives
HCOs key professionals
CISO, ICT Directors of HCOs
Clinical Engineering Directors of HCOs
DPOs, Risk Managers of HCOs
Training/HR Directors of HCOs
CISO, ICT Directors of SMEs
E-Health Directors
Cybersecurity solutions providers
Academic researchers
IT and Medical Device providers
Cybersecurity Agencies
EH ISAC
Professional associations
HCOs
Associations/Networks of HCOs
Associations of SMEs
Healthcare authorities
Horizon Europe projects on cybersecurity
Digital Europe projects on cybersecurity
Associations of IT, Medical Device providers

Figure 1 Relationships between final targets, intermediate targets and communication & dissemination channels

The arrows from the *Intermediate* to the *Final Targets* indicate that the people of the *Final Targets* are members of the *Intermediate Targets*. The arrows from the *Channels* to the *Final Targets* indicate the flow of information/content from the CYBERHIMPREX project to the relevant *Final Targets* via *the Channel*. The dotted arrows from *Digital Europe peer projects* indicate that the peer projects i) make available their websites for hosting CYBERHIMPREX messages and contents and ii) collaborate with CYBERHIMPREX to deliver joint webinars. The multiple arrows from the *CYBERHIMPREX Website, Linked websites* and *CYBERHIMPREX case studies* indicate the broadcast flow towards all the Targets, both as “business card” of the CYBERHIMPREX project and as information/content vehicles.

The dotted arrows to *CYBERHIMPREX Website* from all other *Channels* indicate that the website provides visibility of all other channels and access to their content (when applicable). The double arrow between

CYBERHIMPREX Website and *Linked websites* indicate that they communicate to the users the existence of CYBERHIMPREX and vice versa.

Communication and dissemination activities belong to three threads of activity (see figure 2):
Thread 1 - Focused engagement activities aimed at engaging the intermediate stakeholders and, indirectly, their members; they have been and will be performed mainly via direct contact, leveraging the networks of UCSC, FPG, FPHAG an 7HRC
Thread 2- Communication activities aimed at i) engaging the Final stakeholders that are not reached via the Intermediate stakeholders and ii) communicating content on the project and its results (in a non-technical format); they have been and will be performed mainly via the channels that are most suitable for communication.
Thread 3- Dissemination activities towards all the Final stakeholders that will have been engaged (either via Intermediate stakeholders or "broadcast" communication channels); dissemination has not yet started because the project has not yet delivered results; when results will be available, the dissemination will be performed via the channels that are most suitable for dissemination. To be noted, the dissemination activities have also an implicit communication role and can engage new persons not previously reached via thread 1 and thread 2 activities.

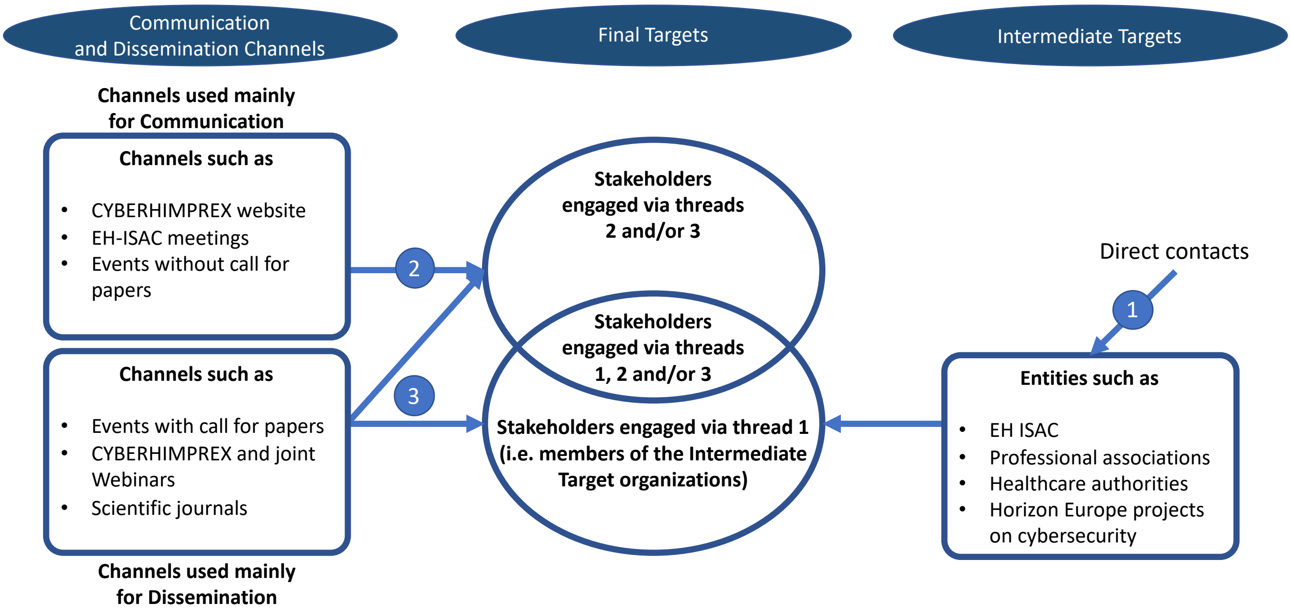

Communication and Dissemination Channels
Final Targets
Intermediate Targets
Channels used mainly for Communication
Channels such as
• CYBERHIMPREX website
• EH-ISAC meetings
• Events without call for papers
2
Channels such as
• Events with call for papers
• CYBERHIMPREX and joint Webinars
• Scientific journals
3
Channels used mainly for Dissemination
Stakeholders engaged via threads 2 and/or 3
Stakeholders engaged via threads 1, 2 and/or 3
Stakeholders engaged via thread 1 (i.e. members of the Intermediate Target organizations)
Direct contacts
1
Entities such as
• EH ISAC
• Professional associations
• Healthcare authorities
• Horizon Europe projects on cybersecurity

Figure 2 Communication and Dissemination: the three threads (1, 2, 3) of activity

The following three sections provide a description of the Intermediate and Final target groups, and of the Communication and Dissemination channels.
The activities performed by M6 and planned by M18 along the three threads are described in section 6.

5.3 Intermediate Target groups, content/messages, expected outcomes

CYBERHIMPREX project will reach the members of the Intermediate Target groups via direct contact by the partner better positioned to succeed.
Following Table 6 provides a description of each Intermediate Target group, the content/message that will be used to obtain their involvement and the outcome (behaviour/action expected by the stakeholder)

Table 6 Intermediate Target groups profiling

Intermediate Target group	Description	Content/Message	Expected outcomes
Cybersecurity Agencies	• European, National (or regional) Agencies or Authorities safeguarding security and resilience in cyberspace. and for preventing and mitigating as many cyber-attacks as possible. • ENISA, the European Union Agency for Cybersecurity, belongs to this group	• CYBERHIMPREX offers lessons learned on how to increase the cybersecurity maturity and on how the procurement of secure IT systems /services and connected medical devices	• The Top managers of the Agency facilitate the contact between CYBERHIMPREX and their relevant executives
EH ISAC	• The European Health ISAC[2] has been kicked-off with a meeting in Athens on May 25th 2023. • The participants include CISOs from healthcare organizations and representative of National/Regional Cybersecurity agencies from all over Europe. Fondazione Policlinico Gemelli is member of the EH-ISAC	• CYBERHIMPREX offers lessons learned on how to increase the cybersecurity maturity in a holistic manner and up-taking (as early adopter) innovative solutions	• The chairman of EH ISACS accepts to insert in the meetings' agenda news/results related to CYBERHIMPREX. • EH ISAC's members accept to be contacted by CYBERHIMPREX outside the strict scope of EH ISAC
Professional associations	• Associations of IT, Medical Engineering, Human Resources Management, Risk Managers from the HCOs	• CYBERHIMPREX offers practical examples of cybersecurity solutions, adopted in a Hospital, that may enrich the "toolkit" of the professionals that are members of the associations	• The President/Top representatives of the association accepts to insert in the association's meetings agenda news/results related to CYBERHIMPREX. • Association's members accept to be contacted by CYBERHIMPREX outside the association's activities.
HCOs	• Hospitals • Groups of Hospitals	• CYBERHIMPREX offers practical examples of funding mechanism that can facilitate the up-taking of innovative cybersecurity solutions, adopted in a Hospital	• The mangers of the HCO facilitate the contact between CYBERHIMPREX and their responsible of IT security, Clinical Engineering (Medical Devices), Data Protection Officer, Risk Management, Procurement, Human

[2] ISAC stands for Information Sharing and Analysis Center. ISACs can be public, private or public-private partnerships where participants mutually exchange information and experiences on cyber security. The mission of the EH-ISAC is to improve the resilience and security of European Healthcare providers

			Resources Management
Associations/Networks of HCOs	• Associations/Networks of HCOs aiming at innovate the operations via e-health and connected medical devices	• CYBERHIMPREX offers lessons learned on how to associate the cybersecurity to the technological upgrading, also via an appropriate procurement process	• The President/Top representatives of the association accepts to insert in the meetings' agenda news/results related to CYBERHIMPREX. • Association's members accept to be contacted by CYBERHIMPREX outside the association's activities.
Associations of SMEs	• Associations of SMEs aiming at innovate their operations via digitization	• CYBERHIMPREX offers lessons learned on how to associate the cybersecurity to the technological upgrading • CYBERHIMPREX offers practical examples of funding mechanism that can facilitate the up-taking of innovative cybersecurity solutions	• The President/Top representatives of the association accepts to insert in the meetings' agenda news/results related to CYBERHIMPREX. • Association's members accept to be contacted by CYBERHIMPREX outside the association's activities.
Healthcare authorities	• Authorities that have the responsibility to ensure the compliance of the HCOs of the country with the cybersecurity regulations (e.g. NIS2, GDPR) • They are National (e.g. MoH) or Regional	• CYBERHIMPREX offers lessons learned on how to associate the cybersecurity to the technological upgrading, also via an appropriate procurement process	• The Top representatives of the authority facilitate the contact between CYBERHIMPREX e-health design and/or procurement
Horizon Europe projects on cybersecurity	• Projects (RIA, IA) that develop cybersecurity solutions. They normally include, i) on the development side partners from Academy and Cybersecurity solutions providers, ii) on the end user side, Healthcare Organizations and SMEs	• CYBERHIMPREX offers a good example of post-project exploitation[3]. • CYBERHIMPREX offers to the end users practical examples of funding mechanism that can facilitate the up-taking of innovative cybersecurity solutions, adopted in a Hospital • CYBERHIMPREX offers to the cyber solutions providers an example of funding of early adoptions • CYBERHIMPREX offers to the cyber solutions providers an example of the features that IT solutions and Medical	• The partner in charge for "exploitation" take inspiration from CYBERHIMPREX • Partners accept to be contacted by CYBERHIMPREX outside the Project's activities.

[3] It must be noted that: i) CYBERHIMPREX uptakes some of the solutions developed by two H2020 projects (PANACEA, CUREX) ii) UCSC, FPG and 7HRC were partners of PANACEA; FPHAG was partner of CUREX

		Devices must embed to satisfy the procurement requirements (defined in initiative 6[4])	
Digital Europe projects on cybersecurity	• Projects funded through calls of the Cybersecurity thread of Digital Europe • They may include partners similar to those of the Horizon Europe projects	• These projects can join the forces with CYBERHIMPREX to do more effective communication and dissemination (e.g. with joint webinars)	• The Coordinator accepts to collaborate with CYBERHIMPREX • Partners accept to be contacted by CYBERHIMPREX outside the Project's activities.
Associations of IT, Medical Device providers	• Associations at National and European level that represent the member of the supply chain, i.e. providers of Medical Device, e-health solutions, ICT infrastructures and services, cybersecurity solutions	• CYBERHIMPREX offers to the suppliers an example of mechanism that the HCOs will use to procure secure IT solutions and Medical Device • CYBERHIMPREX offers to the cyber solutions providers an example of the features that IT solutions and Medical Devices must embed to satisfy the procurement requirements (defined in initiative 6)	• The President/Top representatives of the association facilitate the contact between CYBERHIMPREX and the members of the association • Members accept to be contacted by CYBERHIMPREX outside the association's activities.

5.4 Final Target groups, content/messages, expected outcomes

Following Table 7 provides for each Target group[5], the message that will be used to obtain their involvement, the content that may be interesting for them and the expected outcome, i.e. behaviour/action expected by the stakeholder.

Table 7 Final Target groups profiling

Target group	Content/Message	Expected outcomes
Cybersecurity Agencies executives	• CYBERHIMPREX offers lessons learned on how to increase the cybersecurity maturity and on how the procurement of secure IT systems /services and connected medical devices	• The executives take stock of the findings of CYBERHIMPREX - Adapting the relevant policies/guidelines (e.g. for the application of NIS2) - Promoting the diffusion of best practices (eg. for procurement) - Promoting mechanisms to fund/facilitate the early adoption of innovative solutions (e.g. creating a "sandbox" for simpler procurement of innovations)
CISO, ICT Directors of HCOs	• CYBERHIMPREX offers practical examples of cybersecurity solutions, adopted in a	• The CISO, ICT Directors decide to adopt the holistic approach of CYBERHIMPREX and

[4] Initiative 6: Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines

[5] The names of Final Target groups are quite self-explanatory and do not require a description

	Hospital, that may enrich the "toolkit" of the CISO/ICT Directors in the HCO context • CYBERHIMPREX offers to the cyber solutions providers an example of funding of early adoptions	some of its solutions (in particular those of the initiatives of type G[6]) • The CISO, ICT Directors consider to respond to calls of the Digital Europe programme (or similar programmes) • The CISO, ICT Directors support the adoption of the governance model implemented at FPG
Clinical Engineering Directors of HCOs	• CYBERHIMPREX offers practical examples of cybersecurity solutions, adopted in a Hospital, that may enrich the "toolkit" of the clinical engineer when procuring or protecting the connected medical devices	• The Clinical Engineering Directors decide to adopt the solutions of CYBERHIMPREX regarding procurement and protection of the connected medical devices • The Clinical Engineering Directors support the adoption of the governance model implemented at FPG
DPOs, Risk Managers of HCOs	• CYBERHIMPREX offers practical examples of cybersecurity solutions, adopted in a Hospital, that may reduce the risk for patient safety and confidentiality related to cyber-attacks	• The DPOs and Risk Managers decide to adopt the solutions of CYBERHIMPREX that directly or indirectly reduce the risk for patient safety and confidentiality related to cyber-attacks • The DPOs and Risk Managers support the adoption of the governance model implemented at FPG
Training/HR Directors of HCOs	• CYBERHIMPREX offers practical examples of cybersecurity solutions, adopted in a Hospital, that reduce the vulnerability of the staff and diffuse the know-how on cybersecurity	• The Training/Human Resources Directors decide to adopt the solutions of CYBERHIMPREX that reduce the vulnerability of the staff and diffuse the know-how on cybersecurity • The Training/Human Resources Directors support the adoption of the governance model implemented at FPG
CISO, ICT Directors of SMEs	• CYBERHIMPREX offers lessons learned on how to associate the cybersecurity to the technological upgrading in the SMEs • CYBERHIMPREX offers practical examples of funding mechanism that can facilitate the up-taking of innovative cybersecurity solutions	• The CISO, ICT Directors of SMEs decide to adopt the holistic approach of CYBERHIMPREX and some of its solutions (in particular those of the initiatives of type G[7]) • The CISO, ICT Directors of SMEs consider to respond to calls of the Digital Europe programme (or similar programmes)
E-Health Directors	• CYBERHIMPREX offers lessons learned on how to associate the cybersecurity to the technological upgrading, also via an appropriate procurement process	• The E-Health Directors of the Healthcare Authorities decide to promote the adoption of CYBERHIMPREX solutions (in the context that they regulate/influence) in - the design and procurement of IT systems - the cybersecurity governance
Cybersecurity solutions providers	• CYBERHIMPREX offers to the cyber solutions providers an example of funding of early adoptions • CYBERHIMPREX offers to the cyber solutions providers an example of the	• The cybersecurity solutions providers consider to be involved as providers of the HCOs/SMEs that respond to the calls of the Digital Europe programme (or similar programmes)

[6] See figure 4 and the related explanatory text
[7] See figure 4 and the related explanatory text

	features that IT solutions and Medical Devices must embed to satisfy the procurement requirements (defined in initiative 6)	• The cybersecurity solutions providers decide to propose their solutions to the developers of IT solutions and Medical Devices
Academic researchers	• CYBERHIMPREX offers a good example of post-project exploitation • CYBERHIMPREX offers to the researchers in the cybersecurity domain an example of the features that IT solutions and Medical Devices must embed to satisfy the procurement requirements (defined in initiative 6) • CYBERHIMPREX offers to the researchers on the relationship "human factor-cybersecurity" methods and knowledge on approaches to cybersecurity awareness raising	• The researchers consider to be involved as providers of the HCOs/SMEs that respond to the calls of the Digital Europe programme (or similar programmes), proposing the adoption their innovative solutions • The researchers decide to propose their solutions to the developers of IT solutions and Medical Devices • The researchers on the relationship "human factor-cybersecurity" use the knowledge on approaches to cybersecurity awareness raising
IT and Medical Device providers	• CYBERHIMPREX offers to the suppliers an example of mechanism that the HCOs will use to procure secure IT solutions and Medical Device	• IT and Medical Device providers decide to adapt their solutions/devices and technical assistance modalities to the requirements defined in Initiative 6

5.5 Communication and dissemination channels

The following Table 8 provide descriptive details of each of the nine channels that are meant to be used by the CYBERHIMPREX project to communicate and to disseminate.
For each channel it is also provided an indication of the main use planned for the channel, meaning for communication or for dissemination. The reason is that some channels are more suitable attracting and informing (communication), while others are more suitable for transferring detailed and/or technical contents (dissemination).

Table 8 Communication and dissemination channels profiling

Channel	Used mainly for		Details
	Comm	Dissemin	
CYBERHIMPREX website	x		The website https://cyberhimprex.policlinicogemelli.it has been set-up at the end of M2
Linked websites, LinkedIn/ Social/Media	x		CYBERHIMPREX Partners' websites and social channels Peer projects websites Local/National newspaper, radio, television
CYBERHIMPREX Case study		x	**CYBERHIMPREX Case Study** will be in PDF format to be easily downloaded from the CYBERHIMPREX website. The **Case Study** will summarize the "stories" lived by each HCO, and by the Consortium as a whole, during the project. The case study will be targeted to • European HCOs, to share lesson learned and provide recommendations on the implementation of investments tagged as holistic, cross-border, aimed at regulatory compliance • European and National policy makers, to provide recommendations on policies and strategies at European and National level regarding promotion/supporting/facilitation of 1) the up-take of EU projects results, 2) a holistic and governance-led approach to cybersecurity investments, 3) investments ensuring regulatory compliance 4) cross-

			border practices. • other supply chain actors to share lesson learned and provide recommendations relevant for their roles
EH-ISAC meetings	**x**		• Meetings are expected to be organized at least twice a year
Events without call for papers	**x**		• There are many conferences organized by some of the Intermediate Target stakeholders (in particular by the associations) that may host non-scientific presentations of experiences/points of view on cybersecurity
Events with call for papers		**x**	• Scientific congresses including topics related to the solutions of CYBERHIMPREX or its funding mechanism or to the innovation process (in particular to the innovation up-take)
On-line journals	**x**		• On line journals that are expected to be read by the stakeholders targeted by CYBERHIMPREX (in Italian or Spanish or Greek or English)
CYBERHIMPREX and joint Webinars		**x**	• CYBERHIMPREX will organize webinars to disseminate the non-confidential results and knowledge produced by the project • In order to attract a wider audience and offer a richer spectrum of results/knowledge CYBERHIMPREX aims to promote the organization and delivery of at least one joint webinar with peer projects[8]
Scientific journals		**x**	• Journals that publish on topics related to the solutions of CYBERHIMPREX or its funding mechanism or to the innovation process (in particular to the innovation up-take)

6. Communication and dissemination: activities

The following three Tables provide details on the three activity threads described in section 5.2 (see also fig. 2) , in terms of what has been done so far (M6) and of what is planned to be done by M18[9].

6.1 Activities to engage the Intermediate Targets

The following Table 9 describes the activities performed until M6 in the first thread activities, i.e. those to engage the Intermediate Targets. The planned activities will consist in contacting the listed entities and obtain their collaboration for accessing their members and to have the opportunity to participate to the event that they organize.

Table 9 Activities to engage the Intermediate Targets until M18

Target group	Activities	
	Performed until M6	Planned until M18
Cybersecurity Agencies	A **representative of the Italian agency (ACN)** has attended the CYBERHIMPREX kick-off meeting	**ENISA** Will be engaged, with the purpose to establish a communication line with the key persons **ACN** ACN will be constantly informed of CYBERHIMPREX progress, and relevant reference persons will be identified **Agencia de Ciberseguretat de Catalunya (CISECAT)** https://ciberseguretat.gencat.cat/en/inici/index.html FPHAG will leverage the relationship with CISECAT, the cybersecurity agency in Catalonia, to organize a joint event, webinar, or publication. Engage with their experts and

[8] Projects funded through calls of the Cybersecurity thread of Digital Europe

[9] Activities after M18 will be described in the updated version (D1.6, due at M18) of this deliverable.

		share insights from the CIBERHIMPREX project to strengthen collaboration and amplify the project's reach.
EH ISAC	FPG has become **member** and has attended the first meeting (25 June 2023)	FPG will actively attend the meetings (expected at least two per year) looking for opportunities to present CYBERHIMPREX results
Professional associations	**Associazione Italiana Ingegneri Clinici** https://www.aiic.it/aiic/associazione/governance/ FPG has contacted a key member of the Governance Council, a Director at FPG and former President of the Association	**IT, Clinical Engineering, Risk Management Associations** Will be contacted in Italy, Spain, Greece and at European level. For instance: **Hellenic Scientific Society of Health Informatics** https://www.hsshi.gr/ The Panhellenic Scientific Association of Health Informatics (P.E.P.E.PL.Y) was founded on 21/11/2018 and its members are IT professionals who work in Health Units (public or private hospitals) as well as in Health Regions.
HCOs	CYBERHIMPREX has already established a strong collaboration on cybersecurity topics relevant for CYBERHIMPREX with **Hospices Civils de Lyon**, a French group of 13 Hospitals	Other HCOs in Italy, Spain and Greece will be contacted, leveraging FPG, FPHAG and 7HRC network
Associations/Networks of HCOs	**C-17 Hospital network** https://xarxac17.cat/projectes/xarxa-assistencial-de-salut The aim is to improve health services and bring them closer to the citizens of the C-17 area. In 2015, a collaboration agreement was signed between the Hospital Clínic de Barcelona, the Consorci Hospitalari de Vic, the Fundació Sanitària Mollet, the Fundació Privada Hospital Asil de Granollers (FPHAG partner) and the Fundació Hospital de Sant Celoni with the aim of creating a strategic alliance in health care management (C-17 network), with a reference population of approximately one and a half million people.	**TIC Salut i Social** https://ticsalutsocial.cat/en/ Strive to establish collaboration with TIC Salut i Social, a leading organization in Catalonia focused on digital health and innovation. Explore opportunities for joint workshops, webinars, or publications to maximize visibility and impact.
Associations of SMEs		**Cambra de Comerç de Barcelona** https://www.cambrabcn.org/en/web/cambra-english/home The Cambra de Comerç de Barcelona, or Barcelona Chamber of Commerce, is an organization that represents and supports the business community in the Barcelona region. It provides a range of services and resources to help businesses thrive, including networking opportunities, business development programs, and advocacy on behalf of the local business community. The chamber plays a key role in promoting economic growth, entrepreneurship, and trade in the Barcelona area.

		ACCIÓ Agency of de Generalitat of Catalonia https://www.accio.gencat.cat/en/inici/index.html CCIÓ is the Catalan Agency for Business Competitiveness, a public entity that promotes the competitiveness and internationalization of Catalan companies. It provides support services, funding, and resources to facilitate business growth, innovation, and market expansion. ACCIÓ plays a vital role in fostering economic development and enhancing the global presence of Catalan businesses.
Healthcare authorities		**Regione Lazio and Regione Lombardia** Directorates with responsibility on e-health **Greek Ministry of Health.** https://www.moh.gov.gr/ The Ministry of Health coordinates the work of Healthcare Regions in Greece. The initiative of training on cybersecurity issues undertaken in CYBERHIMPREX will be disseminated via the Ministry of Health.
Horizon Europe projects on cybersecurity	FPG is Partner of **DYNAMO project** (https://horizon-dynamo.eu) which include partners that may be interested to the CYBERHIMPREX results	CYBERHIMPREX partners will contact other Horizon Europe projects that have been (will be) awarded for funding related to calls dealing with cybersecurity
Digital Europe projects on cybersecurity	CYBERHIMPREX has promoted and done a meeting with **HISC4ALL**, one of the other 6 projects (see table below) that have obtained the funding together with CYBERHIMPREX.	Remaining 5 peer projects will be contacted. It is also planned to contact the projects that will get funding from the Digital Europe call DIGITAL-2022-CYBER-03-Cybersecurity and Trust, in particularDIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS (currently in the GA finalization phase and to finalized by Oct 2023) and DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS - Uptake of Innovative Cybersecurity Solutions (to be finalized by Dec 2023)[10]

Project	Acronym	Partners	Country
CYBERsecurity of Healthcare IMPRovEd in a X-border perspective	CYBERHIMPREX	UCSC (COORDINATOR) FPG FPHAG 7HRC	Italy Italy Spain Greece
Health Information Safe and Cybersecured for All	HISC4ALL	INEM (COORDINATOR) PAHLDATA	Portugal Portugal
Integrated system to access and manage individual health data across multiple institutions	IAMHEALTH	BIOMETRID SA	Portugal
Data security strengthening measures	DSSM	UNIVERZITNA NEMOCNICA - NEMOCNICA SVATEHO MICHALA AS	Slovakia
Enhancement of Cyber Security Measures in Kardiocentrum Nitra	KCNR Cyber Security	KARDIOCENTRUM NITRA S.R.O. - KARDIOCENTRUM NITRA	Slovakia
Qualitative Cybersecurity Leap for NOU	QCLN	NARODNY ONKOLOGICKY USTAV - NATIONAL CANCER INSTITUTE	Slovakia
Romanian Cyber Care Health	RO-CCH	DIRECTORATUL NATIONAL DE SECURITATE CIBERNETICA - DNSC	Romania

Associations of IT, Medical Device		**MedTech Europe** MedTech Europe provides the voice of the medical

[10] https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2022/call-fiche_digital-eccc-2022-cyber-b-03_en.pdf

providers		technology industry in Europe, from diagnosis to cure. It represents some 34,000 business entities. MedTech Europe members come from the full range of medical technology manufacturers and representation, including: National trade associations, Pan-European product associations, Large multinational manufacturers of all types of medical technology, Start-ups and SMEs. The association currently includes Members from more than 140 multinational Corporation and more than 45 medical technology associations. https://www.medtecheurope.org **AICA** Italian Association for Information Technology and Automatic Calculation aica@aicanet.it It is the most important national association of IT professionals. Founded on 1961, AICA is a non-profit association whose main purpose is the development of knowledge pertaining to computer science in all its scientific, applicative, economic aspects and social. AICA constitutes a meeting and collaboration place between the three main voices of the information technology world: universities and scientific research centers that feed theoretical and methodological knowledge, public and private users who use information technology for their application purposes and finally the manufacturers and suppliers of IT products and services. **CLUSIT** Italian Association for Information Security https://clusit.it Clusit, born in 2000 in the Computer Science Department of the University of Milan, is the most numerous and authoritative Italian association in the field of computer security. Today it represents over 600 organizations, belonging to all industries CLUSIT Organizes events for "verticals", including the healthcare sector .

6.2 Communication activities

The following Table 10 describes the activities performed until M6 in the second thread of activities, i.e. the communication activities. The planned activities until M18 will consist in accessing and possibly activating the listed entities and use them to communicate the CYBERHIMPREX project and the results in a non-technical format to engage the target audience. The purpose is to obtain that this audience access the dissemination channels (see next section 6.3).

Table 10 Communication activities until M18

Channel	Activities		
	Performed until M6	Planned until M 18	KPIs until M18
CYBERHIMPREX	The CYBERHIMPREX Logo has been defined The website has been set-up	Continuous update	At least two pieces

website	(https://cyberhimprex.policlinicogemelli.it) on 28/02/2023 and is constantly updated 11 pieces of content have been released in the first 4 months		of new content per month
Linked websites and LinkedIn/ Social/Media	The **websites of FPG, FPHAG and 7HRC** include a reference to the project and a link to its website: • **FPG** https://www.policlinicogemelli.it/scienze-innovazione-ricerca/progetti/internazionali/ • **7HRC** https://www.hc-crete.gr (click on the logo in bottom page) • **FPHAG** https://fphag.org/comunicacio/noticies/308/lhospital-general-de-granollers-participa-a-cyberhimprex-el-nou-projecte-europeu-de-ciberseguretat **Websites of peer Digital Europe Projects** CYBERHIMPREX has agreed with one of the peer projects (**Health Information Safe and Cybersecured for All- HISC4ALL)** to cite one each other the projects on its own website **Press release (7/02/2023)** by FPHAG to announcing the participation of FPHAG to the CYBERHIMPREX project https://twitter.com/DiariSomGRN/status/1620466202110988288 **Twitter announcement of the new CYBERHIMPREX website** on 13/04/2023 by FPHAG https://twitter.com/recercafphag/status/1646484640771846144 **FPHAG has already started to leverage the C-17 network**, announcing CYBERHIMPREX through the website of the network on 20/04/2023 https://www.xiscat.cat/cyberhimprex-el-projecte-europeu-de-la-fundacio-privada-hospital-asil-de-granollers/	**Websites of peer Digital Europe Projects** Other Projects will be contacted, proposing to mutually cross-refer the links to-from CYBERHIMPREX. **LinkedIn and social channels of FPG, FPHAG and 7HRC** will be used to engage targeted groups	At least two pieces of new content per month diffused via one or more of the available channels
EH-ISAC meetings	UCSC has invited the chairman of the EH ISAC, who delivered a presentation to the CYBERHIMPREX Kick-off meeting 01/02/2023 (see https://cyberhimprex.policlinicogemelli.it/documents/ and https://cyberhimprex.policlinicogemelli.it/wp-content/uploads-shared/2023/02/CYBERHIMPREX-KOM_W.-Hafkamp_Introduction-EH-ISAC_1-Feb-2023.pdf)	FPG, which is member of the EH ISAC, will ask the chairman to insert an item agenda of the next meeting to inform all the EH ISAC members about CYBERHIMPREX.	At least one presentation by M18

Events without call for papers	**HMISS Conference, HIMSS 23** European Health Conference & Exhibition, Lisbon 7-9 June 2023 https://www.himss.org/event-himss-europe Sabina Magalini, Coordinator of CYBERHIMPREX for FPG, has acted as speaker and panelist in the *Workshop 5- Rethinking Cybersecurity for a Connected World* (https://himss1.eventsair.com/himss23-europe/programme/). Sabina has reported on PANACEA project and its evolution into and CYBERHIMPREX. Her message will be: end-user participation to EU projects will guarantee the development of the best technology in an EU perspective and will help to integrate EU funding into concrete actions. HIMSS (Healthcare Information and Management Systems Society) https://www.himss.org/who-we-are is a global advisor, thought leader and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven nonprofit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and digital health transformation to advise leaders, stakeholders and influencers across the global health ecosystem on best practices. **Learningforum** (22 June 2024) http://www.learningforum.it/2023/programma Stefano Faccioli, Head of HR development at FPG, has participated as panelist and has informed the audience about CYBERHIMPREX and the initiative on awareness raising) (see https://www.youtube.com/watch?v=WyW94nU455c) The Forum intends to shed light on some of the innovations and challenges that have recently emerged in the world of Learning, also (although not only) as a result of the global crisis and the resulting reorganization of work. One such challenge has to do with the need to move training	**Health IT conference** (nest event: expected late 2023/ beginning 2024) https://www.healthitconference.gr/ The HealthIT conference is a relevant event for Informatics and e-Health, which focuses on the strengthening of e-Governance, the e-Health strategy and the National Interoperability Framework between health service providers. It focuses on Management Informatics and Quality issues and presents constructed information projects. During the hospital & health district IT conference they present new projects that help to upgrade the digital transformation. **Panhellenic Conference on Health Economics and Policies** (next event: 4-7/12/2023) https://www.healthpolicycongress.gr/%CE%B1%CE%BD%CE%B1%CE%BA%CE%BF%CE%AF%CE%BD%CF%89%CF%83%CE%B7-%CF%80%CE%B1%CE%BD%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%AF%CE%BF%CF%85-%CF%83%CF%85%CE%BD%CE%B5%CE%B4%CF%81%CE%AF%CE%BF%CF%85-2023/ The Panhellenic Conference on Health Economics and Policies 2023 is organized by the Institute of Health Economics (i-hecon) and the Hellenic Scientific Society for Health Economics & Policy (EEEOPY). Amongst the ssues that will be discussed is the digital transformation of the national health system. **CyberHealth&Pharma Summit** (next event: 21 September 2023) https://www.cyberhealthandpharma.com/es/cyberhealthandpharma The CyberHealth&Pharma Summit is a highly relevant event that focuses on cybersecurity in the healthcare and pharmaceutical sectors. We recommend reaching out to the organizers to inquire about available spots for project communication. If possible, secure a speaking slot or exhibit space to present the CYBERHIMPREX project's objectives, activities, and preliminary results. **Cyber Security Awards 2024** (date to be announced) https://events.boussias.com/el/event/cybe	Active participations (as speaker and/or panelist) to at least two events

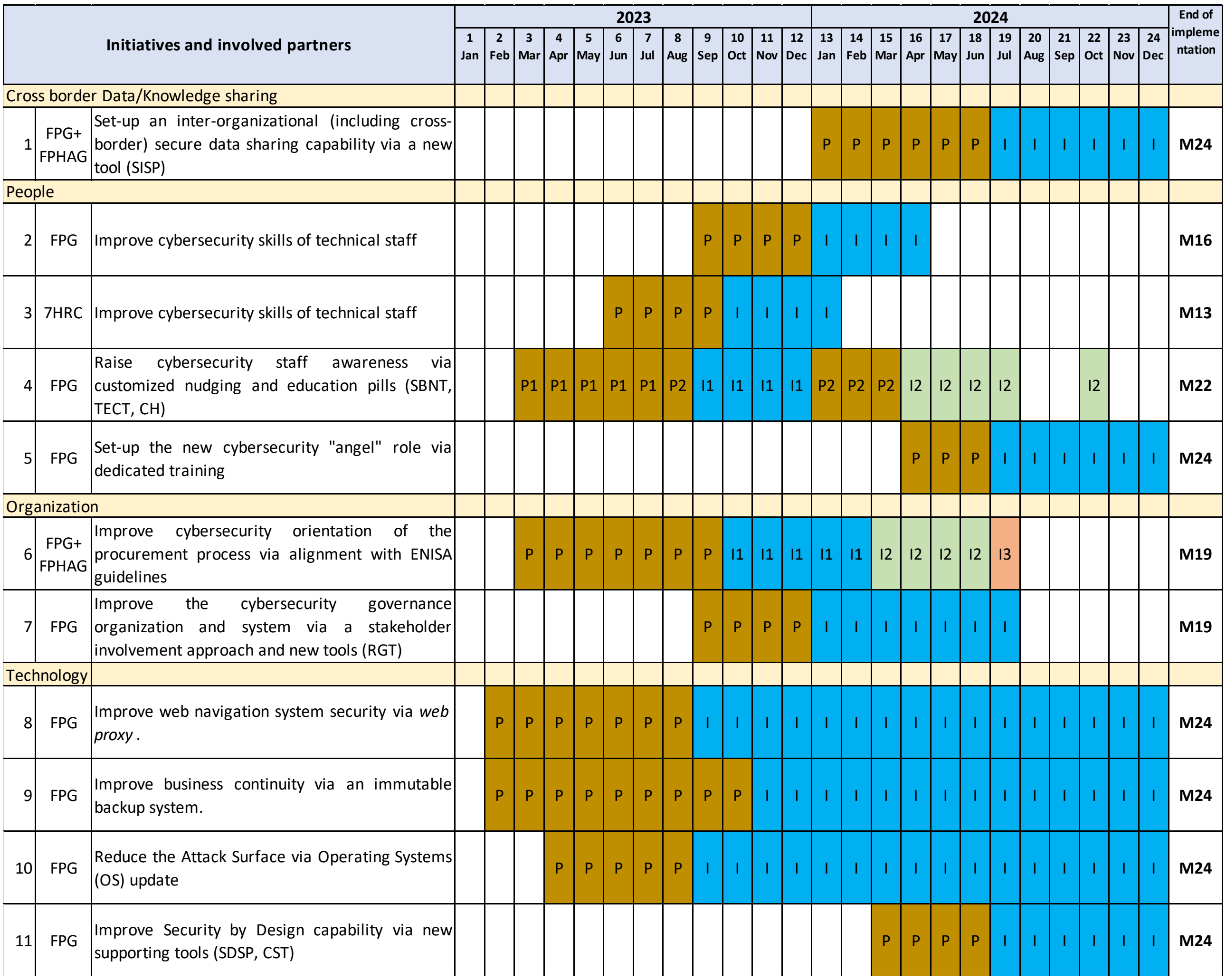
	from the classroom to digital platforms. Is it possible to take advantage of what is good in digital without giving up the advantages of face-to-face training? What opportunities does technology offer? And again, what are the new skills required by the new ways of working? What tools, reflections and strategies must the world of education come up with to keep pace with these changes? Participation of FPHAG and FPG to the **NO-FEAR project workshop "an X-Ray of GDPR and research connected issues"**, 29 March 2023, organized by UCSC (as partner of NO-FEAR) https://no-fearproject.eu/archives/2263	r-security-awards-2024/ The CyberSecurity Awards highlight and reward in an ever-changing environment, the best practices as well as the appropriate equipment/tools for the management of cyber security and digital security, in the areas of Business Critical Infrastructure and Public Infrastructure. **Cybersecurity world** (next event October 30-31 2023) https://www.cybersecurityworld.es/ The event brings together leading global cybersecurity companies to showcase their solutions in response to the rising number of cyberattacks. Companies attending the event are expected to increase their investments in cybersecurity to protect their data and operations. The event will also attract top national and international executives specializing in cybersecurity. **Forum Risk Management** (next edition: 21-24 November 2023) https://www.forumriskmanagement.it The Risk Management in Healthcare Forum was born with the presentation of the first research, carried out in partnership with ASSER (now AGENAS), Italian Ministry of Health and Regions, on what to do for the prevention and control of risks in healthcare. The Forum has increasingly established itself as the venue for the presentation and dissemination of best practices for patient safety. Thus a real "community" of health professionals, professional orders, scientific societies, experts has grown, which over the years has stimulated the growth of culture and activities for the safety of treatments. **Learningforum** (next edtition: probably June 2024) http://www.learningforum.it/2023/learning-forum-2023/ **Cyber Security 360 Summit** (next edition: October 2023) Two meetings per year (spring and fall) https://www.cybersecurity360summit.it Cyber Security 360 Summit is the in-depth	

		appointment for a comparison between the top experts on the subject and the main business representatives to outline the progress of the market in the field of information security and cyber risk, the required fulfilments, the tools and of the organization adopted and to be adopted to face today's, by now daily, challenges. In live streaming, two appointments - one in spring and one in autumn: an intense confrontation between the invited participants but also the possibility for the public to interact with the protagonists of the event with a live chat and respond to the instant polls proposed during the debate .	
On-line journals	**Cybersecurity360 (Italy)** (https://www.cybersecurity360.it) Saverio Carurso, from FPG DPO, has sent an Article (Italian language) to this journal, with planned publication by end of July 2023. The title should be (translated from Italian): CYBERHIMPREX: an EU co-funded project to improve the cybersecurity of healthcare organisations. Cybersecurity360 is a publication which explores cyber security in all its fields with analysed news, technical guides, insights and daily updates, both technical and regulatory. **Horizon, The EU Research & Innovation Magazine** https://ec.europa.eu/research-and-innovation/en/horizon-magazine Article published, with an interview to Sabina Magalini, coordinator for the Gemelli Hospital, of the CYBERHIMPEX project 24/05/2023 (see https://ec.europa.eu/research-and-innovation/en/horizon-magazine/race-make-hospitals-cybersecure)	Other articles will be sent to **Cybersecurity360** **Other on line journals** will be identified with Italian, Spanish and Greek audience (local languages) and with European audience (English language)	At least one article per country

6.3 Dissemination activities

The following Table 11 describes the third thread of activities, i.e. the activities that disseminate in a technical format the knowledge and the results of the project. No dissemination activity has been done so far because no result has already been obtained.
Based on the project plan (see figure 3[11]) only two initiatives (2 and 3) will deliver final result before M18. However Initiatives 4 and 6 are expected to deliver interesting intermediate results, respectively at M12 and M14.

[11] The procurement activities are labelled with a "P" or "Pn", while the implementation activities are labelled with a "I" or "In" . Initiatives 4 and 6 deliver interesting intermediate results at the end of their phases labelled I1



Initiatives and involved partners			2023												2024												End of implementation
			1 Jan	2 Feb	3 Mar	4 Apr	5 May	6 Jun	7 Jul	8 Aug	9 Sep	10 Oct	11 Nov	12 Dec	13 Jan	14 Feb	15 Mar	16 Apr	17 May	18 Jun	19 Jul	20 Aug	21 Sep	22 Oct	23 Nov	24 Dec	
Cross border Data/Knowledge sharing																											
1	FPG+ FPHAG	Set-up an inter-organizational (including cross-border) secure data sharing capability via a new tool (SISP)													P	P	P	P	P	P	I	I	I	I	I	I	M24
People																											
2	FPG	Improve cybersecurity skills of technical staff									P	P	P	P	I	I	I	I									M16
3	7HRC	Improve cybersecurity skills of technical staff						P	P	P	P	I	I	I	I												M13
4	FPG	Raise cybersecurity staff awareness via customized nudging and education pills (SBNT, TECT, CH)			P1	P1	P1	P1	P1	P2	I1	I1	I1	I1	P2	P2	P2	I2	I2	I2	I2			I2			M22
5	FPG	Set-up the new cybersecurity "angel" role via dedicated training																P	P	P	I	I	I	I	I	I	M24
Organization																											
6	FPG+ FPHAG	Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines			P	P	P	P	P	P	P	I1	I1	I1	I1	I1	I2	I2	I2	I2	I3						M19
7	FPG	Improve the cybersecurity governance organization and system via a stakeholder involvement approach and new tools (RGT)									P	P	P	P	I	I	I	I	I	I	I						M19
Technology																											
8	FPG	Improve web navigation system security via *web proxy* .		P	P	P	P	P	P	P	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	M24
9	FPG	Improve business continuity via an immutable backup system.		P	P	P	P	P	P	P	P	P	I	I	I	I	I	I	I	I	I	I	I	I	I	I	M24
10	FPG	Reduce the Attack Surface via Operating Systems (OS) update				P	P	P	P	P	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	M24
11	FPG	Improve Security by Design capability via new supporting tools (SDSP, CST)															P	P	P	P	I	I	I	I	I	I	M24

Figure 3 CYBERHIMPREX initiatives timeline

The activities are planned to be performed mainly using the four channels that are most suitable to disseminate the results with reasonable depth.

Table 11 Dissemination activities until M18

Channel	Activities planned until M18
CYBERHIMPREX Case study	The Case study is due to be delivered at M24, as deliverable D1.8 By M18 we plan to draft the cases regarding the initiatives that will end by M18 (initiative 2 and 3) and the intermediate results of initiatives 4 and 6
Events with call for papers	Planned submission of one paper to at least one event or journal The submission and/or the event and/or the publication may also take place after M18. Probably it will be based on Initiative 4.
Scientific journals	A Journal could be DIGITAL HEALTH (https://journals.sagepub.com/description/DHJ) a peer-reviewed open access journal, published by SAGE, which provides universally accessible and digestible content to all stakeholders involved in the digital healthcare revolution.
CYBERHIMPREX and joint Webinars	Deliver at least one webinar at M11-M12, focused on lessons learned and partial preliminary results of initiatives 3, 4 and 6 It will be checked with peer projects if it can be organized jointly

7. Exploitation: framework

The exploitation of the project's results mainly consists in the fact that the three HCO of CYBERHIMPREX will use the solutions adopted through the initiatives. In general we expect that this exploitation starts already during the life of the project; this complies also with the "first exploitation obligation" imposed by the call.

An additional thread of exploitation regards the results of initiatives that involve third parties and/or deserve to be adopted by other HCOs.

For each initiative, when it ends, a *post-initiative "exploitation process"* will be described, in order to embed the solution in the routine cybersecurity activities. This description will be part of the deliverables associated to the end of the initiatives (as sections named "Solution acceptance and exploitation report"), i.e. D3.1- Results of Implementation activities until M12, D3.2- Results of Implementation activities from M13 to M18, D3.3- Results of Implementation activities from M19 to M24.

The type of exploitation activities included in the post-initiative "exploitation process" depends on the type of initiative, that can belong to one or more of following **seven categories** (for each category it is indicated a ***possible exploitation action***):

A. Initiatives that reduce the vulnerability of the technology → *renew the licenses activated during the project*

B. Initiatives that reduce the vulnerability of the people → *periodically assess the awareness level and update/re-apply the awareness raising measures*

C. Initiatives with pilots. Some initiatives apply the solutions in pilot situations, i.e. only on parts of the HCO reality. → *expand to other situations*

D. Initiatives that require the adhesion of third parties for their success and sticking → *convince a sufficient quantity of third parties to align with the solution*

E. Initiatives that inject new know-how in the HCOs → *make sure that the know-how is re-used even after the end of the initiative*

F. Initiatives that set-up a new organization or process → *make sure that the detailed implementation actions are implemented and that the new organization/process "sticks" in the HCO*

G. Initiatives that produce results that deserve to be adopted by other HCOs across Europe → *convince relevant policy makers (e.g. ENISA, national Cybersecurity Agency) to promote the adoption of solution by other HCOs and relevant stakeholders (e.g. Medical Device manufacturers)*

8. Exploitation: activities

The project includes, as part of WP1 and WP3, activities that prepare the future actual exploitation activities. They (see table 12) will i) be performed in phase with the planned end of the implementations of the individual initiatives, ii) depend on the type of initiative (see A, B, … G above), also considering that some initiatives belong to more than one type

Table 12 Typologies of exploitation activities applicable to each initiative and related target stakeholders

		Initiatives and involved partners	End of implementation	A Tech Vuln	B People Vuln	C Pilots	D 3rd Party	E Know-how	F New org	G EU adopt	Target Stakeholder
Cross border Data/Knowledge sharing											
1	FPG+ FPHAG	Set-up an inter-organizational (including cross-border) secure data sharing capability via a new tool (SISP)	**M24**	x		x	x				FPG, FPHAG, other HCOs
People											
2	FPG	Improve cybersecurity skills of technical staff	**M16**					x			FPG
3	7HRC	Improve cybersecurity skills of technical staff	**M13**					x		x	7HRC, other HCOs, ENISA, Cybersecurity Agencie, Health authorities
4	FPG	Raise cybersecurity staff awareness via customized nudging and education pills (SBNT, TECT, CH)	**M22**		x	x		x		x	FPG, other HCOs
5	FPG	Set-up the new cybersecurity "angel" role via dedicated training	**M24**			x			x	x	FPG, other HCOs
Organization											
6	FPG+ FPHAG	Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines	**M19**			x	x		x	x	FPG, FPHAG, other HCOs, ENISA, ACN, ,other Cybersecurity Agencies
7	FPG	Improve the cybersecurity governance organization and system via a stakeholder involvement approach and new tools (RGT)	**M19**						x	x	FPG, other HCOs, ENISA, ACN, other Cybersecurity Agencies
Technology											
8	FPG	Improve web navigation system security via *web proxy* .	**M24**	x							FPG
9	FPG	Improve business continuity via an immutable backup system.	**M24**	x							FPG
10	FPG	Reduce the Attack Surface via Operating Systems (OS) update	**M24**	x							FPG
11	FPG	Improve Security by Design capability via new supporting tools (SDSP, CST)	**M24**	x		x					FPG, other HCOs

According to the approach described in previous section 7, for each initiative is applicable a set of possible exploitation activities:

1) **Initiative 1 (FPG+FPHAG)-**Set-up an inter-organizational (including cross-border) secure data sharing capability via a new tool (SISP)
    - *Convince other HCOs to adopt SISP and adhere to information sharing collaborative mechanism*
    - *Expand to other departments of FPG and FPHAG*
    - *Renew the SISP License*
2) **Initiative 2 (FPG)-**Improve cybersecurity skills of technical staff
    - *Use the trained staff in cybersecurity improvement projects*
3) **Initiative 3 (7HRC)-**Improve cybersecurity skills of technical staff
    - *Use the trained staff in cybersecurity improvement projects*
    - *Convince Healthcare authorities, ENISA, Cybersecurity agencies to promote the education method applied at 7HRC, do that it is used in other HCOs*
4) **Initiative 4 (FPG)-**Raise cybersecurity staff awareness via customized nudging and education pills (SBNT, TECT, CH)

- *Assess periodically the level of awareness*
- *Use the questionnaires on other staff members of FPG*
- *Use the questionnaires in other hospitals supported by FPG (e. g. Fatebenefratelli Isola Tiberina)*
- *Convince other hospitals to use the questionnaires and to share the results for benchmarking purposes*

5) **Initiative 5 (FPG)-**Set-up the new cybersecurity "angel" role via dedicated training

- *Use the "angels" in order to better capitalize the training and to make the new role stick and add value*
- *Expand to other departments of FPG the set-up of the "angel" role*
- *Convince other hospitals to create the role of "angels"*

6) **Initiative 6 (FPG+FPHAG)**-Improve cybersecurity orientation of the procurement process via alignment with ENISA guidelines

- *Use the new process' artifacts when procuring new IT solutions/services and medical devices*
- *Define similar artifacts for other types of items*
- *Convince and support ENISA in considering the artifacts as a good example of the implementation of the ENISA guidelines*
- *Convince and support the Italian Cybersecurity Agency (ACN) in considering the artifacts as a good example of the implementation of the requirements of the new public procurement regulation*[12]

7) **Initiative 7 (FPG)-**Improve the cybersecurity governance organization and system via a stakeholder involvement approach and new tools (RGT)

- *Implement all the components of the new cybersecurity governance organization*
- *Convince and support ENISA and the Italian Cybersecurity Agency (ACN) in considering the FPG governance model as a good example for the European HCOs*

8) **Initiative 8 (FPG)-**Improve web navigation system security via web proxy.

- *Renew the licenses*

9) **Initiative 9 (FPG)-**Improve business continuity via an immutable backup system.

- *Renew the licenses*

10) **Initiative 10 (FPG)-**Reduce the Attack Surface via Operating Systems (OS) update

- *Renew the licenses*

11) **Initiative 11 (FPG)-**Improve Security by Design capability via new supporting tools (SDSP, CST)

- *Renew the licenses*

All above activities will be updated and further detailed in the *post-initiative "exploitation process"* at the end of each initiatives. They will be performed after the end of the implementation of the initiative (the “end of implementation” Month indicated in Figures 2 and 3).

[12] *Decreto Legislativo 36/202-articolo 108 comma 4*: “In the activities of procurement of IT goods and services, the contracting authorities, including central purchasing bodies, **in the assessment of the qualitative element** for the purposes of identifying the best value for money for the award, **they always keep in consideration of the elements of cybersecurity**, attributing specific and particular relevance in cases where the **context of employment is related to the protection of strategic national interests**”. See also [CODE1] and [CODE2]

9. Ethical and Data Privacy aspects

There are no ethical or data privacy aspects relevant for the implemented and planned communication, dissemination and exploitation activities.

10. Conclusions

This deliverable has provided a conceptual and operational framework for managing effectively the **communication and dissemination** activities of the CYBERHIMPREX project.

The communication and dissemination framework is based on 10 intermediate target groups, 10 final target groups and 9 channels (5 to communicate the project and 4 to disseminate its results).

The communication and dissemination strategy consists in performing three types of activity:

- Engaging intermediate entities (e.g. associations of professionals) via direct contacts and then, through them, their members; they are the final stakeholders, i.e. the persons that can use the results of CYBERHIMPREX
- Engaging the final stakeholders also via five types of "broadcast" communication channels (e.g LinkedIn, on line journals)
- Disseminating the CYBERHIMPREX results via four types of dissemination channels (e.g. webinars)

The deliverable also reports on the activities performed so far (M6) and planned until M18, aimed to

1) Engage the intermediate entities

   - **Cybersecurity Agencies**

     Performed until M6: A representative of the Italian agency (ACN) has attended the CYBERHIMPREX kick-off meeting

     Planned until M18: contact ENISA, Agencia de Ciberseguretat de Catalunya (CISECAT)

   - **EH ISAC**

     Performed until M6: FPG has become member

     Planned until M18: propose to present CYBERHIMPREX in next EH ISAC meeting

   - **Professional associations**

     Performed until M6: contacted the Italian Association of Clinical Engineers

     Planned until M18: contact Hellenic Scientific Society of Health Informatics

   - **Associations/Networks of HCOs**

     Performed until M6: FPHAG is member of the C-17 Hospital network

     Planned until M18: contact TIC Salut i Social

   - **Associations of SMEs**

     Planned until M18: contact Cambra de Comerç de Barcelona, ACCIÓ Agency of de Generalitat of Catalonia

   - **Healthcare authorities**

     Planned until M18: contact Regione Lazio and Regione Lombardia Directorates with responsibility on e-health, Greek Ministry of Health

   - **Horizon Europe projects on cybersecurity**

     Performed until M6: FPG is Partner of DYNAMO project

     Planned until M18: contact other Horizon Europe projects on cybersecurity

   - **Digital Europe projects on cybersecurity**

     Performed until M6: A CYBERHIMPREX has promoted and done a meeting with HISC4ALL**,** *Planned until M18*: contact rremaining 5 peer projects that responded to the same CYBERHIMPREX call; .

Contact future projects, from DIGITAL-ECCC-2022-CYBER-03-UPTAKE-CYBERSOLUTIONS and DIGITAL-ECCC-2022-CYBER-B-03-UPTAKE-CYBERSOLUTIONS - Uptake of Innovative Cybersecurity Solutions

- **Associations of IT, Medical Device providers**

  Planned until M18: contact MedTech Europe, AICA, CLUSIT

2) Communicate the project and attract final stakeholders

- **CYBERHIMPREX website**

  Performed until M6: website activated

  Planned until M18: continuous update

- **Linked websites and LinkedIn/Social/Media**

  Performed until M6:

  The websites of FPG, FPHAG and 7HRC include a reference to the project
  Websites of peer Digital Europe Projects: CYBERHIMPREX has agreed with one of the peer projects (HISC4ALL) to cite one each other the projects on its own website
  Announcement of the new CYBERHIMPREX project via press release by FPHAG
  Announcement of the new CYBERHIMPREX website via twitter by FPHAG
  Announcement CYBERHIMPREX via the website of the C-17 network by FHAG

  Planned until M18: Websites of peer Digital Europe Projects, LinkedIn and social channels of FPG, FPHAG and 7HRC will be used to engage targeted groups

- **EH-ISAC meetings**

  Performed until M6: **EH ISAC** chairman delivered a presentation to the CYBERHIMPREX Kick-off meeting

  Planned until M18: FPG, which is member of the EH ISAC, will ask the chairman to insert agenda items about CYBERHIMPREX

- **Events without call for papers**

  Performed until M6: FPG attended as **speaker Learningforum, HIMSS 23**

  Planned until M18: aim at present in events such as

  Health IT conference
  Panhellenic Conference on Health Economics and Policies
  CyberHealth&Pharma Summit
  Cyber Security Awards 2024
  Cybersecurity world
  Forum Risk Management
  Learningforum
  Cyber Security 360 Summit

- **On-line journals**

  Performed until M6: FPG published Articles on Cybersecurity360 (Italy), Horizon, The EU Research & Innovation Magazine

  Planned until M18: aim at present in events such as Other articles will be sent to Cybersecurity360, Other on line journals will be identified with Italian, Spanish and Greek, European audience

3) Disseminate the results of the project in detail

No activity until M6; activities planned until M18 include

- **CYBERHIMPREX Case study:** By M18: draft of the cases regarding the initiatives that will end by M18 (2 and 3) and the intermediate results of initiatives 4 and 6

- **Events with call for papers and Scientific journals**: Planned submission of one paper to at least one event or journal (e.g. DIGITAL HEALTH)
- **CYBERHIMPREX and joint Webinars**: Deliver at least one webinar at M11-M12 on lessons learned initiatives 3, 4 and 6. Possibly joint, with a DIGITAL EUROPE peer project.

This deliverable has also provided a conceptual and operational framework for preparing the **exploitation** of the project results.

The exploitation of the project's results mainly will consists in the fact that the three HCOs of CYBERHIMPREX will use the solutions adopted through the initiatives.

An additional thread of exploitation regards the results of initiatives that involve third parties and/or deserve to be adopted by other HCOs. The analysis of the initiatives has shown that 7 of the 11 initiatives produce results that can be transferred to other HCOs.

At the end of each initiative a *post-initiative "exploitation process*" will be drafted and formally delivered in D3.1, D3.2 and D3.3., depending on when the initiative ends.

In this deliverable it is indicated, for each initiative, which possible exploitation actions could be realized. More detailed description will be provided in D1.6-2nd Communication, Dissemination, Exploitation plan, due in M18.