Project Title	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
Project Acronym	PANACEA
Project Number	826293
Type of instrument	Research and Innovation Action
Topic	SU-TDS-02-2018
Starting date of Project	01/01/2019
Duration of the project	36
Website	www.panacearesearch.eu

D1.2 PANACEA User Requirements

Work Package	WP1 User and technical requirements, and scenarios
Lead author	Andrea Mazzù (RINA-C), Federica Foti (RINA-C), Ivan Tesfai (RINA-C), Annarita Aquila (RINA-S), Omar Khan (RINA-S), Georgina Fletcher (RCD), Daisy Mundy (RCD)
Contributors	Silvia Garbin (AON), Raniero Rapone (AON) Emmanouil G. Spanakis (FORTH), Sakkalis Vangelis (FORTH), Pasquale Mari (FPG), Annette Denneby (HSE), Muireann Kelleher (HSE), Peter Daly (ICEM), Claude Bauzou (IDEMIA), Sébastien Sohier (IDEMIA), Sofoklis Kyriazakos (iSPRINT), Matteo Merialdo (RHEA), Merlin Bieze (RHEA), Matthias Pocs (STELAR), Lynne Coventry (UNAN), Elizabeth Sillence (UNAN), Dawn Branley-Bell (UNAN), Sabina Magalini (UCSC), Daniele Gui (UCSC), Saverio Caruso (UCSC), Aimilia Magkanaraki (7HRC), Kallia Anastasopoulou (7HRC)
Peer reviewers	Fabio Rizzoni (FPG), Matteo Montesi (FPG), Aimilia Magkanaraki (7HRC), Kallia Anastasopoulou (7HRC), Panagiota Alexoglou (7HRC), Nikos Karamanolakis (7HRC), Don Slyne (ICEM)
Version	V1.0
Due Date	31/07/2019
Submission Date	31/07/2019

Dissemination Level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES. Classified Information: RESTREINTUE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIELUE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRETUE (Commission Decision 2005/444/EC)

The work described in this document has been conducted within the PANACEA project. This project has received funding by the European Union's Horizon 2020 research and innovation programme under grant agreement No. 826293.

Version History

Revision	Date	Editor	Comments
0.1	11/04/2019	Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C)	First Issue: Table of Content (ToC)
0.2	04/06/2019	Pasquale Mari (FPG)	ToC review and re-structuring, extended Methodology section
0.3	18/06/2019	Ivan Tesfai (RINA-C)	Update of ToC based on specific T1.2 meeting (RINA-C, RHEA, FPG, STELAR). agreed Structure for requirements, overall methodology for D1.2, D1.3, D1.4, form for user and technical requirements, classification of scenarios
0.4	25/06/2019	Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C)	ToC review, elicitation of first requirements from different sources analysis (workshops, questionnaires)
0.5	03/07/2019	Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C)	ToC review, integration of comments on requirements
0.6	10/07/2019	Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C)	ToC review, refining of scenarios and requirements
0.7	12/07/2019	Andrea Mazzù (RINA-C), Ivan Tesfai (RINA-C)	Insertion of contribution from UNAN on security behaviours
0.8	15/07/2019	Andrea Mazzù (RINA-C)	Insertion of scenario about information sharing and update in all the sections (requirements revised from Consortium)
0.9	22/07/2019	Andrea Mazzù (RINA-C), Pasquale Mari (FPG), Dawn Branley-Bell (UNAN), Matteo Merialdo (RHEA)	Integration of last parts of the document
0.10	24/07/2019	Andrea Mazzù (RINA-C), Federica Foti (RINA-C), Ivan Tesfai (RINA-C)	Document ready for peer review
0.x	31/07/2019	Andrea Mazzù (RINA-C), Federica Foti (RINA-C), Ivan Tesfai (RINA-C)	Amendment and implementation of peer reviewers comments

List of Contributors

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

Section	Author(s)
1	Ivan Tesfai, Andrea Mazzu', Georgina Fletcher
2	All
3	All
4	Andrea Mazzu', Ivan Tesfai, Omar Khan, Annarita Aquila, Pasquale Mari, Dawn Branley-Bell, Matteo Merialdo, Georgina Fletcher
5	Andrea Mazzu', Ivan Tesfai, Dawn Branley-Bell, Matthias Pocs
6	Andrea Mazzu', Federica Foti
7	Andrea Mazzu', Dawn Branley-Bell
Annex A	Andrea Mazzu', Ivan Tesfai, Pasquale Mari, Dawn Branley-Bell
Annex B	Andrea Mazzu', Federica Foti, Pasquale Mari, Dawn Branley-Bell, Matteo Merialdo, Merlin Bieze, Georgina Fletcher, Daisy Mundy

Keywords

Healthcare Organization, Cybersecurity, requirements, end user requirements, cyber-attack driven scenarios, behaviours scenarios, regulatory

Disclaimer

Executive Summary

This document provides the description of the activities and the result of analysis performed to understand the end users needs, and carried out in order to elicit end users requirements. Requirements were categorized in two groups. General requirements are those that involve all the PANACEA tools and trace the main route where the toolkit should go towards; on the other hand, topic-specific requirements detail the needs that each singular tool should solve during its usage.

Requirements are the result of execution of several activities that involved stakeholders in order to

1 investigate about how they are performing the activities PANACEA toolkit is going to support,
2 which of these activities should be improved,
3 which are the most relevant threats and limitations identified in healthcare environment.

Regarding the first two points, consortium experts gathered stakeholders' feedbacks mainly from two kinds of communication means:

1 Face-to-face meetings;
2 Online survey.

The face-to-face approach allowed to meet directly the relevant stakeholders and have a direct approach: these kinds of meetings come with attendance to workshops where activities were scheduled in order to maximaze the available time. Furthermore, workshops permitted to have further chats with stakeholders and obtain a thorough understanding.

The 1st End-Users and Stakeholder workshop aimed at defining the actual security management state of end users, identifying functions they need to improve and what they wish from the PANACEA Toolkit.

Three workshops, with operational staff and patients, has been conducted at FPG, 7HRC and HSE, implementing the first stage of the SCENE methodology (Scenario elicitation) to capture poor security behaviours within healthcare organisations and understand more about the context for these behaviours.

Nevertheless, WP1, in close cooperation with WP8, provided online survey in order to extend the range of participants and refine the results collected during workshops. An ad hoc Requirement Collection Questionnaire based on model from task 1.1 ([D1.1]) and on the Toolkit high level architecture has been designed and submitted to all possible stakeholders by means of the PANACEA web site (https://www.panacearesearch.eu/).

In parallel and integrating with these activities, WP1 created possible risk scenarios in order to proceed with the requirements elicitation.

Consortium experts proposed several attack driven scenarios, illustred in dedicated sessions of the first stakeholders' workshop, in order to fetch stakeholders' feedback regarding the likelihood of those situations and modify them according to the stakeholders' stories.

Using information acquired by the three workshops held at FPG, 7HRC and HSE, WP1 extracted behaviour driven scenarios in order to include the behavioural aspect within the requirements generation.

In parallel, experts analysed the existing and prospective regulatory framework in order to detect regulations and directives that affect the PANACEA Toolkit. This gave birth to regulatory driven scenarios used in order to support certification activities but also conformace to the European and local regulations.

All these efforts, together with the consortium experts backgournd knowledge, led to the final results; two hundreds and two (202) requirements that represent the end users' wish list and all the constraints and regulations that PANACEA Toolkit should withstand.

Table of Contents

List of figures

List of tables

1. Introduction

1.1 Purpose

The aim of this document is to describe the results from an analysis of stakeholders' needs and provide possible security risks / user scenarios that have been used to inform development of the User Requirements Specification (URS) for the PANACEA Toolkit. The data used have been collected from workshops and interviews involving clinical, administrative, technical, IT, risk management, human resource management, device and application design, staff, etc. that shared information about their needs and expectations concerning cyber-security in healthcare their different role and organisation perspectives.

The outcome of this document is an analysis of the actual state of cybersecurity management in Healthcare Organizations (HCOs) and the needs of PANACEA toolkit end users as well as the identification of relevant functional and non-functional requirements useful to design both PANACEA solution and delivery toolkits. Such work will be used as input for the elicitation of technical requirements during task T1.3 "Definition of Solution Toolkit Technical Requirements" and, therefore, also as guideline for activities in WP3, WP4, WP5, WP6 and WP7.

1.2 Quality assurance

1.2.1 Quality criteria

The Quality Assurance (QA) in the PANACEA project relies on the assessment of a work product (i.e. deliverable) according to a list of QA checks established with the Quality Assurance Manager (QAM) - RINA, validated at a project management level and centralized in the [AD 2].

For the purpose of the QA of this deliverable, it has been assessed according to the following checklists:

- PEER REVIEW (PR) QA checklist: this deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist. The reviewers have been identified by the QAM following the criteria of robustness in terms of completeness of information, continuity and relevance of the current outcomes with the main related tasks. The peer reviewers identified are:
    1 FPG
    2 7HRC
    3 ICEM

1.2.2 Validation process

For the final validation of work products (i.e. deliverables) within the PANACEA project, a final QA review process MUST be used before the issuing of a final version. This QA validation process follows the Quality Review Procedure established with the QAM and validated at project management level in order to guarantee the high quality level of work products and to validate its adequacy according to the defined quality criteria chosen and defined for each deliverable. The Quality Review Procedure itself and the selection of the QA Review Committee are described in the [AD 2]. The QA validation process is scheduled in the QA Schedule [AD 3] managed by the QAM.

1.3 Structure of the document

The structure of the document is as follow.

Section 1 is the introduction of the document, including its purpose and the quality assurance process.

Section 2 lists all applicable and reference documents.

Section 3 provides definition of all the acronyms used in this document.

Section 4 introduces the methodology adopted to elicit the requirements: it introduces the groups of stakeholders consulted, describe the approach taken and how data were collected from the stakeholders during workshops and with questionniares.

Section 5 details the risk scenarios identified that are considered most likely for HCOs, including those that are triggered by an external attack or internal staff behaviour or foreseen by the regulations.

Section 6 reports useful considerations about end users needs in order to elicit requirements. For each topic addressed by the PANACEA toolkit, outcomes from analysis are shown supported by data extracted from the initiatives in collaboration with stakeholders.

Section 7 provides the conclusions of the document.

Annex A
Questionnaires: this annex reports the questionnaires used during the workshops with stakholders, and the material used on support of human behaviour workshops. The Questionnaire of online survey is available at https://panacearesearch.eu/questionnaire-list

Annex B
End-Users and Stakeholders Requirements: this annex reports all the requirements elicited for the design and implementation of PANACEA toolkit.

2. Applicable and Reference Documents

2.1 Applicable Documents (ADs)

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

Reference	Document Title	Document Reference	Version	Date
[AD 1]	Models of health services and of medical device lifecycle for cybersecurity	D1.1 Models of health services and of medical device lifecycle for cybersecurity	1.0	30/04/2019
[AD 2]	PANACEA Project Managment Plan		0.5	01/01/2019
[AD 3]	PANACEA QA Schedule		0.5	01/01/2019
[AD 4]	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people	SU-TDS-02-2018	6.0	24/10/2018

Table 1: Applicable Documents

2.2 Reference Documents (RDs)

The following documents have been consulted for the generation of this document:

Reference	Document Title	Document Reference	Version	Date
[RD 1]	Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams	Johnston, M. J., King, D., Arora, S., Behar, N., Athanasiou, T., Sevdalis, N., & Darzi, A. (2015). Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams. The American Journal of Surgery, 209(1), 45-51.	1.0	January 2015
[RD 2]	ENISA Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures	ENISA & Mayol, Julio & Zapparoli Manzoni, Andrea &Calcavecchia, Franck &iliev, Yordan&Kabisch, Björn&Lovis, Christian & Morgenstern, Maik& Gomes, Rui& Gerald, Götz&Glynos, Dimitrios&Antonatos, Spyridon & Fletcher, Greg & Jespersen, Pia. (2016). Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures NOVEMBER 2016 Smart Hospitals About ENISA. 10.2824/28801	1.0	November 2016
[RD 3]	2019 HIMSS Cybersecurity survey	2019 HIMSS Cybersecurity Survey (https://www.himss.org/2019-himss-cybersecurity-survey)	1.0	2019
[RD 4]	eHDSI Deployment Plans	https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Deployment+Plans		30/01/2019

Table 2: Reference Documents

3. Glossary of Acronyms

Acronym	Description
BYOD	Bring Your Own Device
CAB	Certification Accredited Body
CEO	Chief Executive Officer
CIA	Confidenciality, Integrity and availability
CSA	Cybersecurity Act
DRMP	Dynamic Risk Management Platform
DSP	Digital Service Providers
ECCG	European Cybersecurity Certification Group
EEA	European Economic Area
ENISA	European Union Agency for Network and Information Security
ESP	End-users and Stakeholders Platform
EU	European Union
FDA	Food and Drug Administration
GDPR	General Data Protection Regulation
HCO	Healthcare Organization
ICEM	Irish Centre for Emergency Management
ID	Identificator
IGT	Implementation Guidelines Tool
IMP	Identity Management Platform
IP	Internet Protocol
IT	Information Technology
MDR	Medical Device Regulation
NCCA	National Cybersecurity Certification Authority
NIS	Network and Information Security
OJEU	Official Journal of the European Union
PANACEA	Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for dAta and people
PHR	Personal Health Records
R&D	Research & Development
RGT	Resilience Governance Tool
SBNT	Secure Behaviours Nudging Tool
SCCG	Stakeholder Cybersecurity Certification Group
SDSP	Secure Design Support Platform
SISP	Secure Information Sharing Platform
TCP	Transport Control Protocol
TECT	Training & Education for Cybersecurity Tool
URS	User Requirements Specification

Acronym	Description
URWP	Union of Right-Wing Parties
USB	Universal Serial Bus
VAT	Value Assessment Tool

Table 3. Table of acronyms

4. Methodology

4.1 Overview

This section introduces the overall methodology used in the PANACEA project to develop the end user requirements for the toolkit (Annex B End-Users and Stakeholders Requirements). It gives an overview and the underlying rationale of the activities carried out in order to gather information and infer stakeholders' key needs and the related requirements.

In order to extract requirements, the starting point was the PANACEA proposal [AD 4]. In this document, it is possible to find a first description of what PANACEA toolkit (made up of nine tools) is expected to do and an initial description of all the tools involved.

This sets the "space of analysis". Inside the space, we wanted to capture, from the point of view of the different types of stakeholders and regulations and making reference to the healthcare context:

- Additional functionalities/features not clearly indentified in the proposal that could satisfy the stakehoders' needs
- The priority attached to the functionalities and to the features already identified in the proposal
- The level of satisfaction on how already existing solutions (known to the stakeholders) satisfy the stakehoders' needs
- The contextual factors (human, organizational, technological, legal) to be considered best fit the peculiarities of the healthcare provider organizations and medical device lifecycle
- A complete and credible set of applicable scenarios, capable to validate the full spectrum of the solution toolkit, which include both technological and organizational measures
- The regulatory constraints to be satisfied by the toolkit.

To reach these results, the key methodological issues are completeness and relevance.

For the last bullet point (regulatory constraints), in order to ensure completeness we performed a desktop research and leveraged STELAR and RINA (Consortium partner) expertise to identify all the applicable regulations and also got input from ENISA on regulatory trends. Relevance has been reached by performing a detailed analysis, crossing each of the nine PANACEA tools with the regulations (see matrix in Table 11).

For the remaining bullet points, the main method, to achieve both completeness and relevance, has been a face-to-face workshop that was organized by applying the following principles:

- precence of a good variety of stakehoders, which we selected from PANACEA stakeholder platform
- face-to-face interaction between the stakeholders and the PANACEA partners responsibles for the individual tools
- use of both structured (Questionnaire) and non-structured discussion
- both in the Questionnaires and in the discussion, make explicit reference to the healthcare organizations' structure and medical device/system lifecycle, using models and taxonomies provided in deliverable D1.1 ([AD 1]) of the project.

It is useful to highlight that requirements can be catalogued in two main categories:

1 General Requirements;
2 Topic Specific Requirements.

The first category collects all the requirements that involve all the tools that compose PANACEA toolkit. In these requirements we can mention the fact that PANACEA toolkit shall be composed of two main blocks (solution toolkit and delivery toolkit), that all the tools inside the toolkit should be able to operate both as stand alone tools and with some level of integration in each block and between the two blocks.

The second category are requirements specific to the following tools:

Dynamic Risk Management Platform: the Dynamic Risk Management Platform's (DRMP) aim is to proactively protect a complex IT infrastructure by quantitatively analysing the current level of risk given a multi-dimensional threat analysis and the current business impact. The computation of the risk will trigger the definition of mitigation actions with the purpose of reducing the level of risk by containing the business impact that the actions themselves may cause.

Secure Information Sharing Platform: the Secure Information Sharing Platform (SIPS) aims at delivering a security operations support tool enabling hospital personnel to coordinate and share information in near real-time. The exchange of information includes but is not limited to sensitive healthcare information.

Secure Design Support Platform: The Secure Design Support Platform (SDSP) will provide an integrated and multi-disciplinary engineering environment for system and software feasibility analyses supported by a cyber-security threat and risk assessment module and secure system and software engineering requirements database.

Identity Management Platform: The Identity Management Platform (IMP) verifies the identity and access rights of people and devices accessing to the system. Identification and authentication should be performed for both users (e.g. healthcare professionals, admin staff …) and devices (connected devices).

Training & Education for Cybersecurity Tool: Training & Education for Cybersecurity Tool (TECT) aims to train and exercise staff in order to successfully implement plans and procedures related to cybersecurity. At this scope, this tool should provide different training-education-learning packages, for different target population and on different topics for different purposes, in order to increase awareness on security or on legal and ethics issues in topics such as privacy and data usage.

Resilience Governance Tool: Resilience Governance Tool (RGT) is going to detail roles and responsibilities in terms of processes, organigrams, and job descriptions. The challenge is represented by the diversity of HCO types, the existence of different layers of governance, different IT organisation, the existence of different incident/emergency management organisations in the different countries.

Secure Behaviours Nudging Tool: Secure Behaviours Nudging Tool (SBNT) puts in place a structured methodology to design 'choice architectures' to help nudge people towards better choices without forcing certain outcomes upon anyone. This tool is based on the simple concept that awereness is never enough and that the right behaviour can be addressed ("nudged"). The approach should be interactive in order to deeply involve people.

Value Assessment Tool: Value Assessment Tool (VAT) is a methodology that will support the top management of HC organisations in selecting the most cost-effective set of solutions for cybersecurity. The solutions may include the PANACEA tools and the typical recommendations provided by the risk assessment and mitigation tools.

Implementation Guidelines Tool: Implementation Guidelines Tool (IGT) is a tool that provides all the useful information in order to adopt the PANACEA toolkit. This tool will permit managers/IT staff to assess the status

of the HCO, customize the solution, implement the solution (installing the solution or implementing mitigation actions) and support the customer during the normal operations.

This was only the first step: the need to learn from the valuable experience of the stakeholders leveraged activities of dissemination by creating a website and being active on the social media (LinkedIN, Twitter). This leads to:

1 Define and manage the End-users and Stakeholders Platform (ESP):
   a. Define platform mechanism and working guidelines;
   b. Enroll new members and regularly maintain the SP members updated;
   c. Act as a hub for receiving specific requests/feedback from partners, involving the right partners to satisfy the needs of the project.
2 Establish and maintain relationships with existing networks and knowledge communities:
   a. to expand the "stakeholder pool" supporting PANACEA, also leveraging the content the "pool" can bring;
   b. to create a destination for the dissemination activities;
3 Manage the Open Calls:
   a. Ensure relevant and varied participation of the stakeholders to the open calls;
   b. Management of the related procurement process, using the budget pre-allocated for this purpose.

End-Users and Stakeholders were engaged at different levels (Figure 1):

1 **INFORM** via newsletters, updates, etc.
   a. Supporting the dissemination of project outcomes over PANACEA community
2 **ENGAGE** through discussions, interviews, workshops, etc.
   a. User Requirements Workshop at Month 4 (M4)
   b. First round of User Feedback M7
   c. Second round of User Feedback M7
3 **PARTICIPATE** to the Open Calls
   a. Supporting stronger validation phase of project outcomes

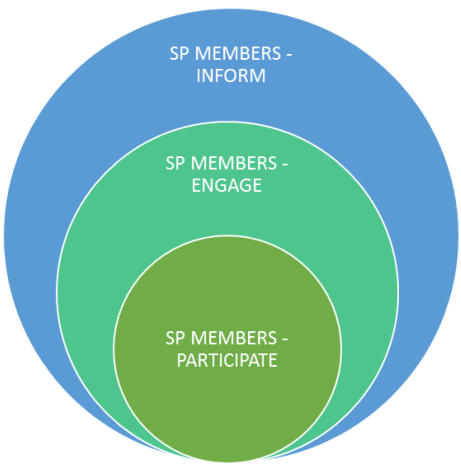


Figure 1: Stakeholders Engagement.

Description of end users and stakeholders is reported in Section 4.2

These activities have been supported by additional activities: PANACEA consortium experts formulated three preliminary different kinds of scenarios, meant to be confirmed/finetuned by the stakeholders:

1 Attack-driven scenarios;
2 Behavior-driven scenarios;
3 Regulatory-driven scenarios.

In addition, an on-line survey has been released by means of the PANACEA web site (www.panacearesearch.eu) in order to reach a higher number of stakeholders. How these activities have been conducted and how the requirements were elicited will be explained in the following sections.

From the feedback of these activities, it was possible to identify, design and review scenarios scoping, use cases definition and requirements. Outcome of these activities are the requirements reported in Annex B End-Users and Stakeholders Requirements these requirements were though in order to achieve an average TRL 5/6 that is, a system validated in simulated environment.

The work done in this task and reported in this deliverable will be the cornerstone for all the other tasks. Figure 2 shows the relationships with the other tasks.

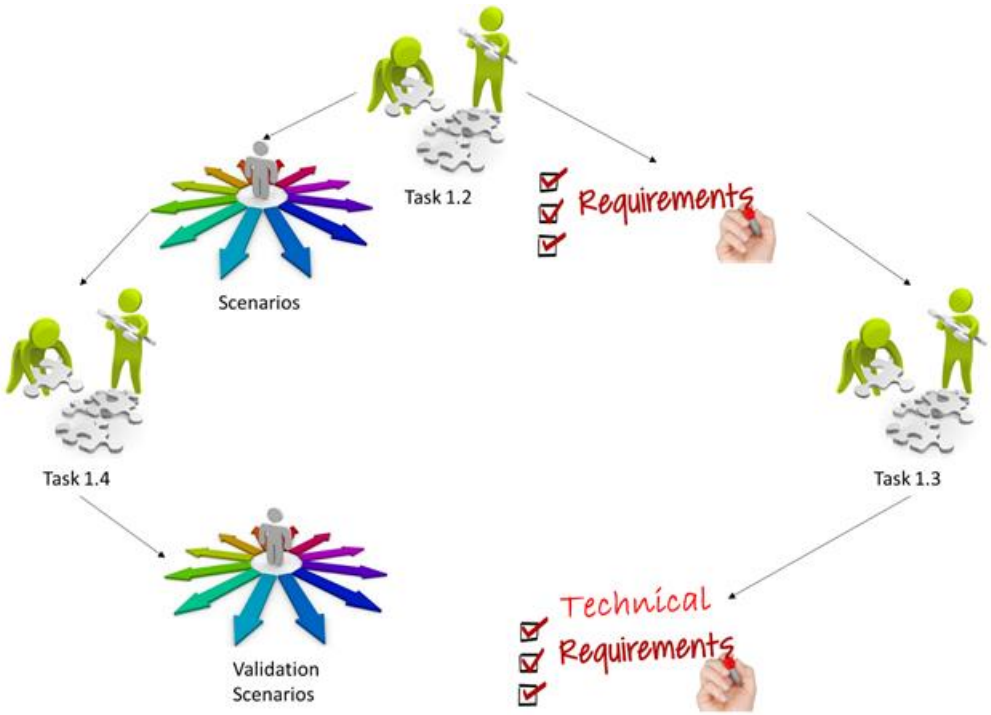


Figure 2: Relationships among the tasks of WP1.

As it is possible to see, the work in this task is fundamental for tracing the way to the technical requirements required for the PANACEA toolkit and the elaboration of the validation scenarios on which to evaluate the system.

4.2 PANACEA Stakeholders Group

During this task, and in particular in the workshop leaded in Rome on 28th – 29th May 2019, end users and stakeholders were mainly classified in the following three groups:

1 Medical device group;

2 IT Security group
3 Non technical / managerial group

These groups map all the end users and stakeholders of the following organization types:

1 Hospital, Clinic, Healthcare Facility
2 Healthcare Devices and Application Supplier
3 Healthcare Research Organisation
4 Cybersecurity & Privacy Supplier Company
5 Policy Makers and Regulators
6 Insurance Companies
7 Partner
8 Patient Association
9 Standards Organisation

4.3 End-Users and Stakeholders workshop

The first end users workshop was organized by RINA-C in collaboration with FPG in Rome at the Gemelli premesis on 28th – 29th May 2019.

Scope of the End User and Stakeholder workshop was to:

1 Introduce PANACEA project and first findings to the community (e.g. Models of health services and of medical devices lifecycle for cybersecurity)
2 Identify and discuss cybersecurity needs in healthcare ecosystem and medical device lifecycle;
3 Identify and discuss use cases from the stakeholders' experience in order to build representative scenarios.

In the following sections, the rationale with which the workshop was organized, how the needs related on cybersecurity were identified, how use cases were addressed and description of the involvement of relevant EU initiatives and H2020 R&D projects liaison for PANACEA will be explained.

4.3.1 Approach

Workshop was organized in sessions. During these sessions, the work was specified by the following topics:

1 Dynamic risk assessment,
2 Secure information sharing,
3 Security by design,
4 Identification and authentication,
5 Training,
6 Governance,
7 Nudging,
8 Value assessment and,
9 Implementation guidelines.

During the workshop, the following four partner roles were defined:
1 Facilitator: Management of the workshop sessions
2 Topic Leader and supporting partners: Representatives of the PANACEA areas of expertise
3 Observer: Collection of insights from the workshop discussions
4 End User/Stakeholder Participant: Sharing knowledge and experience

Figure 3 reports the structure and key roles of the sessions that composed the workshop.

TOPIC	GROUP 1 Medical Devices Facilitator: RINA Observer: RINA	GROUP 2 IT security Facilitator: RHEA Observer: RHEA	GROUP 3 Non technical-managerial Facilitator: RINA Observer: FPG
DYNAMIC RISK ASSESSMENT	Topic Leader: RHEA Supporting partner: UROME	Topic Leader: RHEA Supporting partner: UROME	
SECURE INFORMATION SHARING		Topic Leader: RHEA Supporting partner: FORTH	Topic Leader: RHEA
SECURITY BY DESIGN	Topic Leader: RINA Supporting partner: RHEA	Topic Leader: RHEA Supporting partner: RINA	
IDENTIFICATION AND AUTHENTICATION	Topic Leader: IDEMIA	Topic Leader: IDEMIA	
TRAINING			Topic Leader: RHEA Supporting partner: UROME
GOVERNANCE	Topic Leader: AON		Topic Leader: AON
NUDGING	Topic Leader: UNAN		Topic Leader: UNAN
ROI METHODOLOGY		Topic Leader: FPG	Topic Leader: FPG
IMPLEMENTATION GUIDELINES		Topic Leader: FPG	Topic Leader: FPG

Figure 3: Workshop structure and key roles.

Figure 4 reports the turnout related to the groups reported in Section 4.2. As it is possible to see from the chart, there was a reasonable balance between groups for the worshops, although there are clearly more IT Security staff than any other group and no Clinician group is represented. This latter group was engaged separately via interviews following the main workshop.

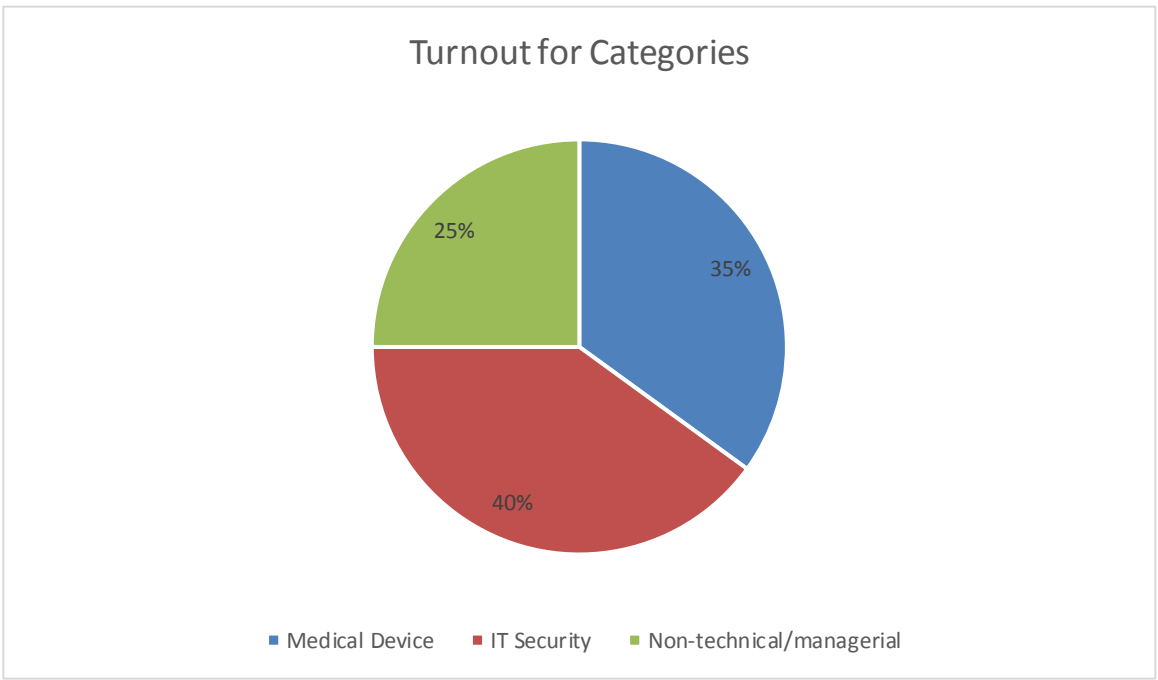


Figure 4: Turnout for Categories.

Specific PANACEA partners were in charge for each Topic (Topic Leader). The facilitator provided specific instructions to the different types of End-user/Stakeholder and introduced the Topic Leader. After a brief

introduction of the Topic Leader concerning main scope and elicitation model, the Topic Leader described the structure of the questionnaire. Each End-user/Stakeholder Participant filled questionnaires (10-15 minutes) and based on their answers, they provided clarification supported by PANACEA Partners. Some questions had open answers: in this case, the facilitator triggered discussions starting from these questions. The facilitator structured the discussion (30-35 minutes) involving all the partners while the Observers were taking notes.

4.3.2 Involvement of relevant EU initiatives and H2020 R&D projects liaison for PANACEA

In this section, a summary of the analysis carried out on other EU initiative and H2020 R&D projects, relevant to PANACEA framework is reported, showing the links/possible synergies and the additional implementations that PANACEA is going to achieve. The aim is to provide further inputs to the PANACEA identification and definition of end-users' requirements in the field of cybersecurity defence.

For this reason, we invited the coordinators of three H2020 projects regarding cybersecurity in the healthcare domain (CUREX, SPHYNX, SecureHospitals). They attended the workshop in person and delivered presentations on their projects and of their first results. They aso took part, with the role of stakeholder, to the requirement elicitation sections described in next paragraph 4.3.3.

We also invited an ENISA representative to deliver (in video-call) a presentation on the initiatives going on at European level regarding the regulatory framework on cybersecurity.

We also

The following table shows the most relevant EU initiative and H2020 R&D projects and the input for PANACEA identified during the workshop:

Title	Brief Description	Use in PANACEA
ENISA	ENISA is very active in the eHealth sector and in evolving cybersecurity within this topic: • Implementation status of the NIS Directive • Medical Devices Regulation Cybersecurity task force • Cybersecurity Act/Cybersecurity Certification Framework The NIS Directive has three parts: 1 National capabilities: EU Member States must have certain national cybersecurity capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc. 2 Cross-border collaboration: Cross-border collaboration between EU countries, e.g. the operational EU CSIRT network, the strategic NIS cooperation group, etc. 3 National supervision of critical sectors: EU Member states have to supervise	ENISA activities play a fundamental role within PANACEA project. All the activities aimed at hardening of cybersecurity in critical infrastructures. Among those, hospitals have a special focus. All these activities were taken into account in order to formulate expecially regulatory requirements.

Title	Brief Description	Use in PANACEA
	the cybersecurity of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, and finance sector), ex-post supervision for critical digital service providers (internet exchange points, domain name systems, etc). The medical device regulation foresees IT Security requirements pre-market and post-market. Among those, the needs of incident reporting for medical device security incidents. Cybersecurity act aims basically in • improve resilience against cyber attacks; • uniform the cybersecurity; • improve trust in ICT services. Cybersecurity Act is composed by two main blocks. From one side, it introduces the European system of certification of information security on network connected devices. On the other hands, it enforces the ENISA role in order to be more active in supporting the member states in the operative management.	
CUREX	The vision of CUREX is to safeguard patient privacy and increase their trust in the currently vulnerable critical healthcare information infrastructures, especially in cases where data is exchanged. The integrated CUREX Platform will rely on the following discrete layers: • The Asset Discovery layer that maps data, technical and human resources into ontological models. • The Threat Intelligence layer that discovers the vulnerabilities and identifies potential threats. • The Risk Management layer that quantifies risks considering both cybersecurity and privacy threats as well as proposing optimal safeguards and cyber hygiene enhancing techniques based on decision support systems. • The Trust Enhancing layer, which includes the deployment of a business consensus-based blockchain that will store compiled risks reports from the previous layers and will integrate the	The usage of private blockchain can be of inspiration in order to enhance trust in PANACEA Toolkit. Indeed, it includes the deployment of a business consensus-based blockchain that will store compiled risks reports. Furthermore, this platform is GDPR compliant.

Title	Brief Description	Use in PANACEA
	CUREX tools and end-user applications into a fully GDPR compliant platform. CUREX will deliver targeted measures for raising the cyber hygiene of healthcare organizations, through training and raising awareness activities, targeted towards healthcare employees. Training will involve the development of cybersecurity defending skills.	
SPHYNX	SPHINX aims to introduce a health tailored Universal Cyber Security Toolkit, thus enhancing the cyber protection of the Healthcare IT Ecosystem and ensuring patient data privacy and integrity. Aim of SPHINX is to provide a toolkit in charge of providing an automated zero touch device and service verification, providing cyber security services in a secure and easy-to-use interface and address threats to public critical infrastructure and cyber terrorism. In summary, SPHINX project will deliver an IT solution that will be tested and demonstrated in three different scenarios at different countries (Romania, Portugal and Greece) aiming to: • improve the security of Health and Care services, data and infrastructures • reduce the risk of data privacy breaches caused by cyberattacks • increase patient trust and safety	Due to the close connection between the two projects, SPHINX was considered in order to integrate attack scenarios and refine the user requirements. Furthermore, it has been usefull in order to enlarge the network behind PANACEA.
SecureHospitals	SecureHospitals project is based on two main pillars in order to prevent attacks: • Better protection measures • Awareness and training on cybersecurity-related issues Objectives of the project are: 1 Raise awareness among decision maker and IT practitionsers in hospitals and care centres across Europe 2 Aggregate existing knowledge on cybersecurity in hospitals 3 Create tailor-made training materials for trainers and IT practitioners 4 Train the trainers and practitioners all over Europe 5 Communicate training needs, development of training schemes, project training initiatives and further awareness	Due to its focus on training and raising of awareness, it is possible to achieve an integration with the tool that provides training in PANACEA by sharing materials and the online training platform. The material gathered by the SecureHospitals consortium is useful in order to integrate requirements for the human misbehaviour correction.

Table 4: Summary of most relevant projects for PANACEA.

4.3.3 Workshop Questionnaires Sessions

For the purpose of elicitation of end-user requirements, structured questionnaires on the following topics were used:

1 Dynamic Risk Assessment;
2 Secure Information Sharing;
3 Security by Design (Information Systems);
4 Security by Design (Medical Devices);
5 Identification and Authentication;
6 Training;
7 Governance;
8 Nudging;
9 ROI methodology;
10 Implementation guidelines.

For each topic, a simple model was defined and shared with the participants to support the comprehension about the topic objectives. The model made clear the broad scope of the topic and provided insights for participants to understand the context in which the questions would be deployed. The complete list of the questionnaires used is presented in Annex A Questionnaires.

Questions were organized in three different sections. Questions related to the first section focused on the following issues:

1 Do end-users already have these functionalities[1]?
2 On which of them there are issues or needs for improvement?
3 Which functionalities are the most important?
4 Are there missing functionalities?

Then, in the second section, which aims at understanding how the tool may best fit in the HCOs (Healthcare Organizations) context, questions were formulated according to the models defined in [AD 1], and the related taxonomies. We report here an extract in order to provide a flavor of the questions (e.g. for the Dynamic Risk Assessment topic):

1 On which "Technological services" should the DRA be focused?
2 On which networked Medical Devices (if with TCP/IP - Transmission Control Protocol/Internet Protocol)
3 On which processes, roles, organizational functions

Third and last section of the questionnaire builds on questions to better investigate specific issues and provide suggestion about possible improvement for each topic.

The questions were shaped in order to require a Y/N answer or a 1-5 ranking.

[1] We provided a tentative list of the functionalities that we expected could of interest for the stakeholders; we always included an open question, to collect further functionalities.

4.3.4 Cyber-attack driven scenarios elicitation

Definition of scenarios is important in order to gather as usefull as possible end user requirements. During a dedicated Plenary Session, scenarios were identified and discussed with stakeholders in order to take advantage from their experience in order to build representative scenarios.

Therefore, the scope of this Plenary Session was to:

1 Validate scenarios from both cybersecurity perspective and healthcare perspective
2 Frame the most relevant and correct impact on healthcare services
3 Identify critical issues

After the workshop, from the cyber-attack driven scenarios elicitation aspect, two distinct outcomes were expected:

1 Define reliable and representative scenarios from which to identify user needs and requirements;
2 Define validation scenarios on which to test the PANACEA Toolkit.

In order to do this, a set of scenarios were presented and questions were addressed to the audience to investigate the following aspects:

1 Credibility of attack (both in fulfilment from an attacker and in feasibility within the Healtcare context);
2 Potential consequences in terms of:
    a. Privacy;
    b. Data breaches;
    c. Patient safety;
    d. Patient trust;
    e. Business continuity;
3 Criticality of roles, processes, technology services/application and device;
4 Preventive measure to apply.

Scenarios were drafted by answering to a fixed set of questions, to collect the most comprehensive set of data. For example:

- What are the objectives of the scenario?
- What business functions does the scenario model?
- Which are the actors (person, non-person and threat agents' entities) that are involved in the scenario?
- What are the assumptions necessary for the scenario to happen? What are the system state and/or conditions that must be met before the scenario will execute? What is the system state after the described sequence of event has successfully executed?
- What is the compromise that took place in the scenario?
- What are the expected frequency of occurrence and the probability of success?
- What is the impact of the compromise? What is the loss expectancy? What are the legal, personal, physical consequences of the compromise presented in the scenario?
- What is the flow of events and resulting business impact due to the compromise?
- What information would sensors generate that indicate that the compromise has taken place?
- What would be the valid and invalid mitigation options?
- What is the flow of events during the activation of the mitigation actions?
- It this scenario a priority? Is it related to another scenario?
- Which PANACEA tool could help/mitigate the scenario?
- How do we have to configure our Emulation Environments for this scenario?

These scenarios are described in Section 5.1.

4.4 Security behaviours workshop

4.4.1 Rationale

In order to successfully address security behaviours, it is necessary to first identify the type of risk behaviours that are taking place within the target work environment (in this instance, healthcare) and the drivers behind these behaviours, i.e., why staff may find themselves more likely to engage in unsafe behaviours at work. In order to achieve this the PANACEA project incorporated in-depth interviews with end-users across three sites, and three countries. The interviews were analysed and key themes were identified. The results are discussed in detail within the following document. Recommendations for effective behaviour change interventions are also discussed.

We held focus groups across three sites: Gemelli hospital in Rome, the 7th Health Region of Crete in Heraklion, and the Irish Centre for Emergency Management (ICEM) in Cork. These sites are project partners and end-users. Ethical approval was granted by the Northumbria University ethics committee. Details of the healthcare staff groups are shown in Table 5.

Gemelli Hospital, Rome	**Lab Technicians**
	Administration Staff
	IT Team
7th Health Region of Crete (7HRC)	Biomedical Engineers
	IT Teams across 2 different hospitals
	Health Centre Staff (nurses, GPs, health workers)
	Managers
Irish Centre for Emergency Management, Cork	Lab Technicians
	Administration Staff
	Medical Consultants
	Finance Staff
	Emergency staff including paramedics and ambulance staff
	Nurses
	Doctors

Table 5: Sample demographics

Focus groups took place face-to-face at the hospital location or remotely via Skype. Each session lasted between 45-60 minutes, and included between 2-9 staff members. Opened ended questions focused upon the following areas (complete interview script included in Appendix A):

- Awareness of any previous incidents at the hospital/healthcare setting
- The type of cybersecurity risks that staff felt were of most concern within the hospital/healthcare
- The type of data and technology that staff interact with on a daily basis and the security of this technology
- Security of staff behaviour and any risky behaviours that they were aware of
- General awareness of potential cyber-risk and vulnerability to attack.

For those interviewees that could not attend the focus groups (for example, due to unforeseen patient emergencies), we collected additional survey-based responses to these questions. The results were analysed using qualitative analysis to identify key themes.

4.4.2 Behavior driven scenarios elicitation

Three workshops, with operational staff and patients, will be conducted at FPG in May, 7HRC and HSE both in June 2019, implementing the first stage of the SCENE methodology (Scenario elicitation) to capture poor security behaviors within healthcare organisations and understand more about the context for these behaviors.

The focus group results were transcribed to enable the researchers to conduct qualitative analysis to identify key themes. The aim of the analysis was to identify key risk behaviours that were reported by staff. Crucially, analysis also focused upon the identification of specific factors facilitating these behaviours (e.g., motivation for engaging in a particular risky behaviour) and potential interventions that could be effective in promoting behaviour change towards increased cybersecurity.

4.5 Regulatory requirements elicitation

4.5.1 Rationale

Analysis of current and prospective regulatory ecosystem is very important in order to incorporate regulatory inputs into the requirements of PANACEA and also to anticipate possibile future evolutions of the regulatory panorama.

The requlatory requirements elicitation task has been performed in two steps:

1. Set up of the analysis methodology
2. Execution of the analysis

4.5.2 Methodology of the analysys

The methodology of the analysis of regulatory requirements is based on the analysis of regulatory context which have been segmented into three areas (see Figure 5):

1. Cybersecurity
2. Privacy
3. Health domain

Furthermore the agreed approach has been divided into three steps (see Figure 6):

1. STEP 0: classification of regulations (identification of regulatory context with applicable and prospect regulations) and set up of regulatory scenarios
2. STEP 1: identification of relevance of regulations with respect to PANACEA key topics
3. STEP 2: bilateral call to fine tune the relevance to PANACEA main topics and elicitation of regulatory requirements

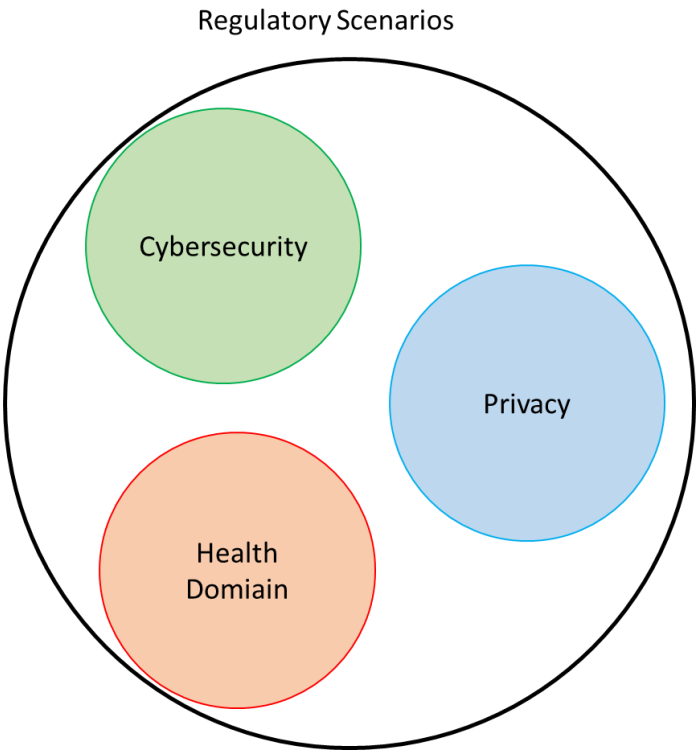


Figure 5: Regulatory context Areas

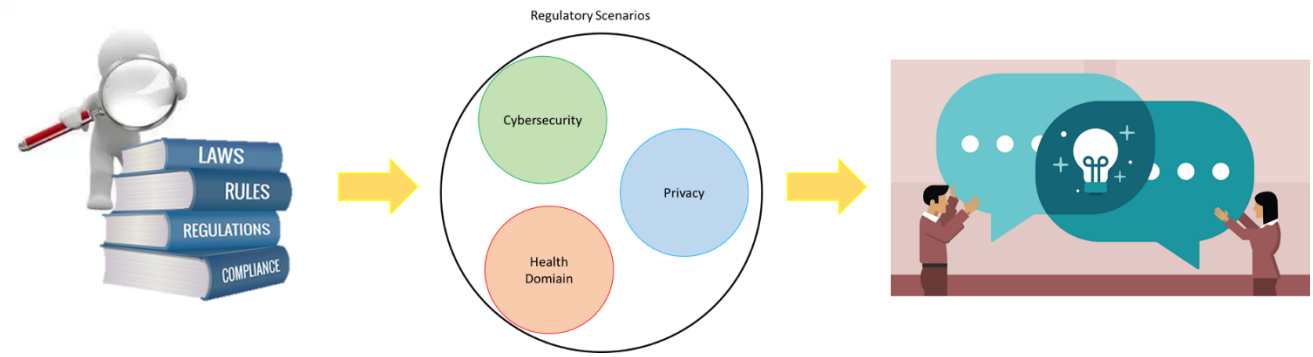


Figure 6: Process for identification of regulatory scenarios and requirements

4.6 End Users and Stakeholders requirements elicitation

4.6.1 Rationale

All the activities performed during this task had the objective of elicit the end user requirements, namely the wish list of people that is going to use the PANACEA toolkit.

For this reason, a first part of activities has been conducted in order to involve stakeholders in definition of the so-called "actual status". This is the status regarding how the cyber security is addressed inside the HCOs.

This is the starting point on which the PANACEA toolkit will operate in order to provide its services.

The other activities were carried out in order to design a status in which HCOs can operate in a reasonable secure environment ("future state") and how to reach that status.

These activities foreseen definition of questionnaires, analysis of existent regulamentations, analysis of relevant EU initiatives and security scenarios definition.

4.6.2 Stakeholders workshop questionnaires analysis

Following the Declaration of Work and based on the process, technologies and roles defined inside an HCO, the expert teams of consortium created ad-hoc focused sessions for three target groups:

1. Medical Device Manufacturer group;
2. IT Security group;
3. Non-Technical and managerial group.

All these groups are important to give their perception about all the environments PANACEA toolkit is going to operate. Indeed, while the first two groups can give tips on more technical aspects like what technologies are more sensitive during the daily activities, non-technical group drove more the aspects related to human misbehaviour and relative training and nudging. Finally, managerial group provided their needs in terms of business continuity and value assessment.

The discussions were addressed by means of ad-hoc questions that were designed with the same rationale: three sets of questions were proposed to the stakeholders. A first set of questions aimed at defining the actual situation in which the healthcare organization is operating. Second and third part were targeted at recognising elements that need an improvement and detecting the user requirements on future products.

The workshop outcome has been used to clearly identify the needs and requirements of potential PANACEA Toolkit end-users at a very early stage of the project. With the inclusion of end-users as the first step of the system development, a direct link to the needs that such system must satisfy was ensured. The objectives of the end-user workshop have been to:

1. Introduce PANACEA and the aims of the workshop
2. Obtain information about the questionnaire respondent
3. Identify critical technologies, processes and roles
4. Identify the functional requirements

All the answers were collected and averaged in order to understand the general trend in cyber security inside each group. Also, common points among the groups were analysed.

The requirements were then formulated in order to consider common and singular group expectations on PANACEA toolkit to provide cybersecurity solutions.

4.6.3 Stakeholders online surveys analysis

The purpose of the survey was to gather a volume of information concerning the group of stakeholders. The survey focused in collecting opinions or collecting real facts and was carried out at an individual level by means of a structured questionnaire published on the PANACEA web site.

Activities performed in order to carry out the survey were basically grouped in three phases:

1 Preparation: identification of the purpose, definition of the participants, preparation of the interview with reviews performed by the PANACEA consortium experts;
2 Execution: posting of the survey by means of the web channel, that is PANACEA web site;
3 Analysis: information acquiring, production of statistics, analysis of the results and assessment against the purpose defined in Preparation phase.

As in the workshop, for three target groups have been detected:

1. Medical Device Manufacturer group;
2. IT Security group;
3. Non-Technical and managerial group.

Scope of the survey was to understand the level of cyber security applied by the stakeholders and the margin of improvement. In order to accomplish this, both open and closed questions were submitted to the stakeholders that had the possibility also to specify more information in case of need.

As already introduced, questionnaires were submitted to the users by means of the PANACEA web page. An invitation to the designed stakeholders have been sent together in order to notify them about survey availability.

Once execution phase was terminated, collection of answers and creation of statistics were the two following steps. Creation of statistics permitted to create a clear framework about the current state of cyber security measures, critical roles and critical processes.

This, along an examination against the risk scenarios defined in section 5 taking into account effects on private data, data breaches, reputation and business continuity, permitted to elicit the requirements.

4.6.4 Risk scenarios analysis

Once critical technologies, processes and roles were defined in the previous activities, they were analysed against the risk scenarios proposed in Section 5.1 in order to extract further requirements.

Therefore, for each competence area of the tool, every feasible role that performs a process by means of a technology has been analysed against each scenario.

The analysis was conducted in order to evaluate indicators such as:

1 Loss in the CIA (Confidenciality, Integrity and availability) of the information;
2 Data breaches;
3 Safety and;
4 Business Continuity.

Every event that affects one of these indicators has been taken into account, the root cause has been analysed and requirements have been formulated in order to mitigate or support to the mitigation of the effects.

4.6.5 Sources from H2020 R&D projects and EU initiatives

As reported in Section 4.3.2, PANACEA project relied on different H2020 R&D projects or EU initiatives in order to carry the activities.

Activities of ENISA, especially that ones aimed at consolidating a European framework for cybersecurity in ICT services (cybersecurity Act), have been taken into account in order to extract regulatory requirements. Indeed, also PANACEA toolkit shall undergo to the regulation imposed by Cybersecurity Act. This regulation has been analysed under the point of view of each tool that composes PANACEA and requirements have been elicited if needed.

Furthermore, ENISA has been one of the sources in order to define requirements to regulate certification aspect in the Security-by-Design topic.

Curex and Sphynx are the most similar projects regarding PANACEA. Collaboration with their consortiums and attendance to workshops lead to a better definition of the attack scenarios reported in Section 5.1 and consequently to a higher quality of the requirements for PANACEA toolkit from the end users side. From these projects, points like the use of blockchain in Identification and Authentication tool and improvement in the Dynamic Risks Assessment tool have been addressed.

These two projects jointly with Securehospitals were very useful also in order to enlarge the network behind PANACEA and reach a high number of potential stakeholders. This improved the quality of PANACEA toolkit end users requirements and the dissemination of the activities.

5. Risk Scenarios

This section reports the risk scenarios designed by the PANACEA consortium experts and reviewed based on the stakeholders indication, including the workshop in Rome. Scenarios have been developed for two main reasons:

1 Analyse example of possible attacks in order to develop requirements to tackle them;
2 Refine validation scenarios that will be introduced in D1.4 "Relevant User Scenarios, use-cases and KPIs for Panacea Toolkit validation".

These scenarios were indicated by the stakeholders as the most likely to happen and they played a central role during the phase of requirements analysis, both for the functional and non-functional requirements.

Three kinds of scenarios have been developed:

- Attack driven scenarios;
- Behaviours driven scenarios;
- Regulatory driven scenarios;

Overall, 23 scenarios from these categories have been identified.

They will be further described in the following sections.

5.1 Attack driven scenarios

These scenarios encompass the description of possible attacks (both cyber and non-cyber) to the HC organization. Scenarios analysis drove the elicitation of HC organizations needs in order to improve their security posture. The following attack scenarios have been designed in combination with the PANACEA end users and are coherent with the scope defined in the proposal ([AD 4]). Please note other attack scenarios have been elicited (e.g. denial-of-service), but it has been decided to report only the most meaningful scenarios with respect to the PANACEA scope.

5.1.1 Scenario 1: Phishing attack

Phishing is the process of sending emails to a group of email addresses and making the message look legitimate enough that the recipient will click a link in the email. Once the victim clicks the link, they are typically enticed into providing information of a personal nature (including username and password).

Phishing Attack	
Description	An employee of the healthcare organization receives a fraudulent e-mail for a fake website (e.g. bank website) that instructs to click on a link in order to update some data. The employee clicks on the link and inserts sensitive data (e.g. log-in credential). While generally phishing attacks were very broad on the recipients size (fraudulent emails were sent to thousands of email addresses), the diffusion of social media allows attacker to select the targets and tailor the attack on them. Linkedin is particularly used for this reason (e.g. CEO phishing attacks).
Criticality	High – The criticality is high because of the broad range of follow-up attacks that may be possible after a successful phishing attack
Likelihood	High – People are considered a particularly weak link in an organisation's security chain ([RD 3]).
Impact	It is difficult to make a general statement about the impact. It depends on the activities of an attacker after a phishing attack has been successful.

Table 6: Phishing Attack.

5.1.2 Scenario 2: Ransomware attack

Ransomware is a relatively newer class of malware that is designed to hunt down and encrypt files on a target system. Once installed in one of the devices within the IT infrastructure, usually ransomware are able to replicate, exploit known vulnerabilities and spread in the network. When such files are found, the code will encrypt the data and then inform the victim that they must pay a certain amount to get their data back.

Ransomware Attack	
Description	An employee of the healthcare organization downloads and runs an executable that finds all available data and encrypts them in order to make them inaccessible. The program then instructs the victims to pay a ransom to unlock or unencrypt the data.
Criticality	High – The criticality is high. A ransomware infection can massively affect the operation of a hospital, meaning the availability of hospital services. While systems can usually be repaired, encrypted data may be lost forever ([RD 2]).
Likelihood	Medium – The likelihood of becoming victim of a ransomware attack is medium but increasing ([RD 2]).
Impact	Impact depends on the number of systems affected, whether or not an offline backup is available as well as the respective recovery process times (e.g. time to restore backup, system images/configuration).

Table 7: Ransomware Attack.

5.1.3 Scenario 3: Loss or Theft of Equipment or Stored Data

Data theft is one of the bigger concerns that have emerged with mobile devices increased diffusion, as criminals target them for the information they contain. With the proliferation of ever more powerful and compact

devices — including mobile devices, laptops, cell phones, and even hard drives — providing some sort of protection has become crucial. Because many devices today are easily portable, theft has become much easier. This scenario is strictly related to the low degree of cyber-security awareness and training: often portable devices are not encrypted or secured despite containing very relevant data.

Loss or Theft of Equipment or Stored Data	
Description	An employee of the healthcare organization leaves unattended a mobile device in a public space. The attacker thefts the device. This kind of attacks can be easily tailored to target specific employees, thanks to the diffusion of social media and personal and professional information in the Internet.
Criticality	Medium – Apart from the need to substitute the device, sensitive data can be at risk. This could affect the reputation of the HCO ([RD 2]).
Likelihood	Medium – The likelihood of medical equipment theft is medium. Although all kinds of equipment are stolen, laptops used by hospital staff are the most frequent target of thieves ([RD 2]).
Impact	Impact depends on the replacement promptness of the device and from the backup of data stored within the device. Any sensitive access assigned to the employee should be reviewed and updated/removed.

Table 8: Loss or Theft of Equipment or Data.

5.1.4 Scenario 4: Insider, accidental or intentional Data Loss

This scenario foresees data loss due to misbehaviour of an employee, usually accidental (related to careless personnel that loeses data), or intentional (related to personal revenge of personnel). In some cases, an attacker may pretend to be someone else, usually an employee with some specific profile in the organization. In this latter case, one of the techniques to be exploited is identity theft. Identity theft is one of the most prominent and rapidly evolving threats, which falls under the heading of social engineering. Once in possession of information, an identity thief has plenty of options available, depending on his/hers particular goals.

Insider, accidental or intentional Data Loss	
Description	An employee or someone that is pretending to work inside the HCO thieves data/equipment in order to be used for his/her own purposes.
Criticality	High – The criticality is high because of the broad range of follow-up attacks that may be possible after an intentional or unintentional data loss ([RD 2]).
Likelihood	High – Social engineering attacks are becoming more and more frequent ([RD 2]).

Impact	Impact may be devastating, in dependence with the criticality of the data stolen/loss. The HCO IT infrastructure may be compromised, identity of HCO personnel or patients may be compromised.

Table 9: Insider, accidental or intentional Data Loss

5.1.5 Scenario 5: Attacks against critical medical systems

In modern hospitals, medical systems are usually connected to the IT backbone infrastructure of the organization. While good practices should be used in order to properly protect and segregate these systems, the possibility of attacks (from inside or outside the organization) is not negligible. Vulnerabilities on the operating systems of such systems may be used in order to take control of them and potentially cause critical damage to the patients or the IT/medical infrastructure.

Attacks against critical medical systems	
Description	A cyber attacker gains access to a healthcare provider's IT infrastructure through an e-mail phishing attack and takes control of a file server to which a heart monitor is attached. While scanning the network for devices, the attacker takes control (e.g., power off, continuously reboot) of all heart monitors in the HC organization (by exploiting a vulnerability on the medical system), putting multiple patients at risk.
Criticality	High – The criticality is very high, due to the potential damage on critical systems and patient security ([RD 3]).
Likelihood	Medium – as an average, these attacks are less frequent than others, due to the relative complexity of their organization. In some hospitals, fortunately, critical medical devices are managed by separate networks, not easily accessible. Attacks on critical medical systems, however, may be caused by attacks on connected medical devices or by attacks to the corporate network, and are generally simpler to be performed ([RD 3]).
Impact	Impact may be devastating, potentially involving life losses. Due to limited possibilities with respect to securing devices themselves, hospitals have to rely on measures around the devices, as well as on the measures taken by manufacturers in line with the requirements formulated by the competent authorities. Medical systems may be not directly managed by the HCO personnel and any update or fix may require time.

Table 6: Attacks against critical medical systems

Cyber attacker gains access to healthcare provider's IT infrastructure

Attacker takes control of all heart monitors in the ICU

Multiple patients are at risk

5.1.6 Scenario 6: Attacks against connected medical device

According to Article 1 of Council Directive 93/42/EEC (amended in 2007/47/CE), 'medical device' means any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- investigation, replacement or modification of the anatomy or of a physiological process,
- control of conception,

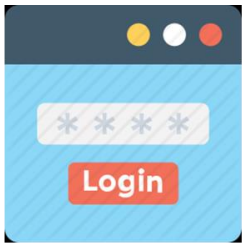
and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.

There are thousands of medical devices in every hospital, some of them capable to send and receive data through the TCP/IP network (i.e. devices for monitoring, therapeutic interventions, imaging, laboratory and pharmacy, hemodynamic monitors, ventilators and syringe pumps, among others). If connected to the IT infrastructure of the organization, these devices could potentially be used in order to access the networks (hence compromise other equipment). This attack is similar to Scenario 5: Attacks against critical medical systems (critical medical systems could be considered medical devices), with the difference that here the focus is on the new types of relatively cheap medical devices, connected via radio (with IoT protocols, potentially). These medical devices are far less observable and controllable than fixed crucial systems managing the most important business functions of the hospital (surgery room, for example). Usually, their cyber-security testing protocols are also less severe. This results in an increasing possible vulnerability surface: while the impairment of a single medical device could have limited despite potentially severe impact, the main threat is the device to be used to access the IT infrastructure and affect the critical sytems.

Attacks against connected medical device	
Description	A cyber attacker gains access to an IoT medical device by exploiting a known vulnerability. When the device connects to the HC organization IT infrastructure, the attacker gains access and infects many other similar devices (pacemakers, for example), critical medical systems or the corporate network (finance, human resources, etc..).
Criticality	High – The criticality is high because of the broad range of follow-up attacks that may be possible. Medical devices in smart hospitals are increasingly connected with clinical and enterprise information systems. The key problem is that highly vulnerable devices are brought together with highly valuable data.

Likelihood	High – Medical devices have become a key entry point/target for attacks in the healthcare context (https://securityledger.com/wp-content/uploads/2015/06/AOA_MEDJACK_LAYOUT_6-0_6-3-2015-1.pdf). The devices are considered an easy and particularly vulnerable point of entry, or an interesting target ([RD 2]).
Impact	Impact may be devastating, potentially involving life losses. Hacking is particularly critical in the hospital context as it, if successful, may allow tampering with medical devices. This can have far-reaching consequences for patient safety and privacy, and can threaten hospital operations in general. Based on access to medical devices, attackers may breach hospital records over an extended period of time.

Table 7: Attacks against connected medical device.



A cyber attacker gains access to an IoT medical device

The attacker gains access and infects many other similar devices

Network is infected

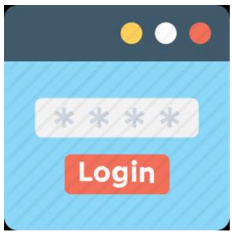
5.1.7 Scenario 7: Attacks against IT infrastructure

In modern hospitals, corporate services (finance, human resources, etc...) are usually served by the IT infrastructure. While typical hacking activities against this infrastructure and the business processes it leverages can be foreseen (not differently from any other organization), the corporate network could be used in order to access the operations networks and the critical medical systems, or connected medical devices While some hospitals correctly separates and segregates the networks, in some cases this isolation is not properly performed, leading to possible attacks on the critical systems. This attack can be related (and may be cause) to Scenario 5: Attacks against critical medical systems.

Attacks against IT infrastructure	
Description	A cyber attacker gains access to the corporate network of the HC organization by leveraging known vulnerabilities and a phishing attack against some targeted HC personnel. After exploring the corporate network and gaining access to some exploitable assets, he/she founds the possibility to access the operations network and exploit vulnerabilities on critical medical devices, generating a scenario similar to Scenario 5: Attacks against critical medical systems.
Criticality	High – The criticality is high, due to the potential damage on critical systems. Depending on the affected business functions in the corporate network, the attack may be critical even without reaching medical systems.
Likelihood	High – Corporate networks, usually connected to the Internet and accessed by not particularly cyber aware personnel, are

	generally less protected than operations network and more likely attacked ([RD 2]).
Impact	Impact may be severe, if only the corporate network is affected. If the critical systems are affected, the attack may potentially involve life losses.

Table 8: Attacks against IT infrastructure



A cyber attacker gains access to the corporate network of the HC organization

The attacker accesses to the operations network and exploit vulnerabilities on critical medical devices

Network is infected

5.1.8 Scenario 8: Lack of security-by-design good practices on medical devices

Several standards for medical devices in EU exist, including specification for the embedded software life -cycle. Among them:

- ISO 13485:2016
- IEC 62304
- IEC 60601
- ISO 14791:2012

Recently, the EU MDR (medical Device Regulation) has been issued in order to improve safety for the HC organization and the patients. In particular, the EU MDR states that, among many general requirements:

(17.2) For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation

and:

(17.4) Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended

In addition, the regulation states that each medical device should be tagged with a Unique Device Identification (UDI).

In the framework of EU regulation, the EU Cybersecurity Act introduces for the first time an EU-wide cybersecurity certification framework for ICT products, services and processes. Among the huge amount of categories, also medical devices will be involved. Within this directive, ENISA will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. At the time

being, no certification framework has been made available and adoption of this certification is not mandatory. Neverthless, PANACEA toolkit should move in this direction.

Despite these regulations, it is still possible that medical devices are affected by known or unknown vulnerabilities (zero day vulnerabiltiies). Being a complex combination of software and hardware, medical devices life cycle should be inherently secure in all its phases. Unfortunately, this may not happen. A vulnerability on a medical device may be exploited by an attacker, leading to Scenario 6: Attacks against connected medical device. In USA, the Food and Drug Administration (FDA) recently adopted (https://www.govinfo.gov/content/pkg/FR-2017-08-21/html/2017-17603.htm) the UL 2900 standard for medical devices: UL 2900 suggests good security-by-desgn practices for the manufactures. The diffusion of the standard, however, is still far from being complete even in the USA.

This scenario, despite not being directly considerable an 'attack scenario', could be one of the primary cause of attacks against medical devices.

Lack of security-by-design good practices on medical devices	
Description	During the development of a new medical device, budget constraints simplify the security assessment of the device, causing the production of software leveraging unknown vulnerabilities. Once in the market, hackers discover the vulnerabilities and are able to exploit them, leading to Scenario 6: Attacks against connected medical device.
Criticality	High – The criticality is high because of the broad range of follow-up attacks that may be possible. Medical devices in smart hospitals are increasingly connected with clinical and enterprise information systems. The key problem is that highly vulnerable devices are brought together with highly valuable data....
Likelihood	High – (Source: no specific statistics are available about lack of usage of security-by-design during the development of medical devices. Since from [RD 2] the likelihood of tampering of medical devices is classified as high due to the relative easiness of exploit, it can be assumed not many companies follow proper security-by-design processes. [RD 3] also states that incidents due to vendors are quite common) Despite several security-by-design frameworks exist (and the recent UL 2900 USA standard for medical devices is quite complete), not all medical devices are developed with rigorous cyber-security software/hardware policies.
Impact	Impact may be devastating, potentially involving life losses. Hacking is particularly critical in the hospital context as it, if successful, may allow tampering with medical devices. This can have far-reaching consequences for patient safety and privacy, and threaten hospital operations in general. Based on access to medical devices, attackers may breach hospital records over an extended period of time.

Table 9: Lack of security-by-design good practices on medical devices

Budget constraints simplify the security assessment of the device

Software is developped with unknown vulnerabilities

Hackers discover the vulnerabilities and are able to exploit them

5.1.9 Scenario 9: Spoofing attack on Biometrics for Personal Health Records and eHealth Services

Patients and doctors may use a biometric identification solution to access collaboration platforms supporting the prevention and management of a chronic condition (for example, osteoarthritis). Patients need to be able to remotely and securely report health data such as activity level, pain, etc., while general practitioners and specialists are able to access the patient journals for decision-support. If the IT department does not set correctly the context-dependent features and the requirements for the identification system in terms of access (biometrics) trade-offs, or if the biometric solution is not sufficiently robust, an attacker may potentially spoof the identification and mask himself/herself as a valid user.

Spoofing attack on Biometrics for Personal Health Records and eHealth Services	
Description	An attacker could be able (assuming too tolerant thresholds for the identification on an insufficiently robust system) to run a spoof attack on a patient or an HCO personnel and mask himself/herself as a valid user by presenting user's counterfeit biometric traits. This allows him/her to get access to the system and the Personal Health Records (PHR).
Criticality	High – Criticality could be high, depending on the attacker gaining access. In case of a spoofed medical doctor or nurse, for example, many PHRs may be accessed.
Likelihood	Low – (Source: PANACEA End Users, literature). Spoofing attack
Impact	Impact may be severe, if multiple PHRs are accessed, and it may be very complex to be detected. Reputation loss for the HC organization and identity theft are amongst the most common consequences.

Table 10: Spoofing attack on Biometrics for Personal Health Records and eHealth Services.

An attacker masks himself/herself as a valid user by presenting user's counterfeit biometric traits

An attacker runs a spoof attack

Hackers gets access to Personal Health Records

5.2 Behaviours driven scenarios

Across the three end users sites (namely FPG, 7HRC, ICEM), there is some level of awareness of cyber-incidents that have occurred or may occurred in healthcare organizations more generally. However, the sites themselves have experienced very few cyber-incidents. There have been some minor incidences of ransomware that had been successfully addressed (without payment) due to backups of the data – and no critical incidents. Many of the participants acknowledged that the hospitals had "been lucky so far".

Although some participants described having concerns that something may happen in the future, others reflected upon the lack of negative effects they have experienced despite using the internet and technology on a daily basis. This suggests that at the moment, there is a lack of learned experience across the sites – which may subsequently impact upon staffs' risk awareness and perceived vulnerability.

Eight key risk behaviours were identified from the focus group data: Computer and user account security; E-mail use; Use of USB devices; Use of own devices; Remote access and home working; Backups, updates and encryption; Connected devices; and Physical security. They lead to the development of nine scenarios, each of which is discussed in the following sections.

5.2.1 Computer and user account security

Concerns around the security of login credentials and computer access were very prevalent across all of the sites. There were three main concerns within this area: 1). Open workstations, 2). Shared login credentials, and 3). Password security.

Scenario 1: Open Workstations

Scenario 1: Open Workstations	
Description	A healthcare staff member needs to use a workstation. When she approaches the workstation, she notices it is unlocked and already logged into another staff member's account. To save time logging off and back on again using her own login details, she uses the unlocked workstation. After she has finished using the workstation, she leaves it unlocked to save time and for she assumes that, only other members of the staff will be using the workstation.

Motivation(s) for behaviour	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
		Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	High – prevalent across the sites	
Potential Impact(s)	☑	Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also inpact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
	☑	Malicious usage of hospital systems
	☑	Breach of data regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
	☑	Insider threat
	☑	Non-repudiation

Scenario 2: Shared login credentials

Scenario 2: Shared login credentials		
Description	A surgeon has just completed a day in the operating theatre and knows that she has further operations scheduled for the following day, and is on call should there be a patient emergency. While she has handwritten notes, she finds it difficult to find time to enter the information into the hospital system. To save time and ensure that the notes are entered as soon as possible and not forgotten should an emergency arise, she asks one of the administration staff to enter the patient's medical data onto the system. Admin staff does not have the access rights to the computer system containing the patient records, therefore they use the surgeon's own login credentials (i.e., username and password) so they can complete the task. This also includes making follow up appointments and issuing a prescription if required.	
Motivation for behaviour	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
	☑	Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	High – prevalent across the sites	
Potential Impact(s)		Unauthorized (or third party) access - or theft - of sensitive/personal data
		Introduction of malware to hospital systems (could potentially also impact medical devices)

		Introduction of computer virus to hospital systems (could potentially also impact medical devices)
	☑	Data input errors impacting on patient care
		Data not centrally updated on hospital systems
		Malicious usage of hospital systems
	☑	Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
	☑	Insider threat
	☑	Non-repudiation

Scenario 3: Insicure password behaviour

Scenario 3: Insecure password behaviour(s)		
Description	A nurse has received the alert that she needs to change her password for one of the hospital systems. Her current password has expired, as staff is required to change their work passwords every 2-3 months. She accesses numerous different systems at work – many of which have different rules for acceptable passwords (e.g., must contain numbers, symbols, letters etc.). The nurse has difficulty remembering all her different passwords. To help herself, she writes her password details on a note that she keeps near her computer. When prompted she also accepts the "remember password" option in order to avoid re-entering her password next time she uses the system.	
Motivation for behaviour	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
	☑	Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	High –prevalent across the sites	
Potential Impact(s)	☑	Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also impact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
	☑	Malicious usage of hospital systems
	☑	Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
	☑	Insider threat
	☑	Non-repudiation

5.2.2 E-mail use

Email usage presents two potential security risks. Firstly, the problem of opening e-mail attachments, which could lead to the introduction of malware into the system and secondly, emailing sensitive patient information to large groups or to personal emails in an insecure manner.

Scenario 4: Opening e-mail attachment

Scenario 4: Opening e-mail attachments		
Description	A doctor is waiting for a patient to e-mail a copy of their test results from an external clinic. The doctor does not know which e-mail address the patient will be using, as patients often asks a friend or family member to send the information on their behalf. The doctor sees an e-mail appearing in their inbox with the patient's name as the subject. The e-mail has a file attached, which he/she opens to access the report.	
Motivation for behaviour		
		Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
	☑	Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	Medium – prevalent across the sites but spam filters block some phishing e-mails	
Potential Impact(s)		
		Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also impact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
	☑	Malicious usage of hospital systems
		Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
		Insider threat
		Non-repudiation

Scenario 5: Emailing sensitive information, lack of encryption and home working

Scenario 5: Emailing sensitive information, lack of encryption and home working		
Description	A clinician would like the opinion of other colleagues regarding a patient she is currently treating. As the patient has been examined by multiple clinics and staff members, the clinician decides to summarize their key medical information into one e-mail – so they can easily pass this onto their colleagues, and in turn their colleagues can access this information instantly on whatever device they are currently using (even if they are currently away from the hospital, e.g., on a mobile device or a home computer). She forwards this e-mail to five colleagues and a general lab mailing list at one of the nearby clinics; she also sends a copy to her personal e-mail, so she can access the information at home. The information is not encrypted as she has not been trained how to do this, and encryption is generally not used for e-mails.	
Motivation for behaviour		
	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
		Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust

		e.g., between colleagues and/or patients
	☑	Low risk awareness
Prevalence	Low – prevalent across one site	
Potential Impact(s)	☑	Unauthorized (or third party) access - or theft - of sensitive/personal data
		Introduction of malware to hospital systems (could potentially also impact medical devices)
		Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
	☑	Data not centrally updated on hospital systems
		Malicious usage of hospital systems
	☑	Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
	☑	Insider threat
	☑	Non-repudiation

5.2.3 Use of USB devices

Scenario 6: Use of USB devices

Scenario 6a: Use of USB devices (patients)		
Description	A patient gives his doctor a USB containing his test results from an external clinic. The doctor plugs the USB into his workstation to view the report. It is common for visitors to bring their results from external clinics and hospitals in this manner, therefore the doctor regards the use of USBs as part of his daily tasks and a necessity to enable him to do his job.	
Motivation for behaviour		Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
	☑	Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	Medium – prevalent across some sites	
Potential Impact(s)		Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also impact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
	☑	Malicious usage of hospital systems
		Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
		Insider threat
		Non-repudiation
Scenario 6b: Use of USB devices (internal staff)		
Description	One of the hospital directors has a big presentation to prepare for, but he has a very busy schedule over the next week. Therefore, he asks one of the hospital residents [students] to help him prepare his presentation slides.	

	The resident prepares the slides using both the hospital workstations and his/her own personal computer. She/he provides the final slides to the director on a USB stick, so he can transfer these to his hospital workstation.	
Motivation for behaviour	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
	☑	Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	High – prevalent across the sites	
Potential Impact(s)		Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also impact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
		Malicious usage of hospital systems
		Breach of regulations (e.g., GDPR, law)
		Physical theft – or physical manipulation – of medical devices
	☑	Insider threat
	☑	Non-repudiation

5.2.4 Use of own devices

Scenario 7: Use of own devices

Scenario 7: Use of own devices		
Description	A lab technicians use their own laptop to access their work e-mail, and attachments sent to themselves, which includes an unencrypted database of patient information. This is to enable them to have quick, easy access to this information whenever and wherever they are. They only use this laptop on the public Wi-Fi, which is not connected to the main hospital network. They also access public Wi-Fi networks outside of the hospital, for example when travelling to access their e-mail at the airport. The lab tech's laptop does not have software installed to enable the staff member (or IT) to remotely wipe the drive/data if the device is stolen or misplaced. There is no clear 'Bring Your Own Device' (BYOD) policy at the hospital, and staff regularly access their work e-mail from their own devices (including smartphones) therefore the lab technician does not perceive any risk or wrongdoing related to this behaviour.	
Motivation for behaviour	☑	Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
		Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness

Prevalence	High – prevalent across the sites
Potential Impact(s)	☑ Unauthorized (or third party) access - or theft - of sensitive/personal data ☑ Introduction of malware to hospital systems (could potentially also impact medical devices) ☑ Introduction of computer virus to hospital systems (could potentially also impact medical devices) Data input errors impacting on patient care Data not centrally updated on hospital systems Malicious usage of hospital systems ☑ Breach of regulations (e.g., GDPR, law) Physical theft – or physical manipulation – of medical devices Insider threat Non-repudiation

Scenario 8: Smartphone apps for communication

Scenario 8: Smartphone apps for communication	
Description	A doctor wishes to quickly ask for another colleague's opinion on a patient's injury. She uses the smartphone application WhatsApp to send a photo directly to her colleague's phone. This enables the doctor to save time verbally explaining to a collegue or alternatively needing to upload a photo to her workstation and updating the health record to share with a colleague. Using WhatsApp also means that the doctor does not have to leave the patient. Her colleague replies via WhatsApp with some helpful information, which enables the doctor to make a decision on the patient's treatment within a matter of minutes.
Motivation for behaviour	☑ Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure* ☑ Common behaviour *i.e., social norm in the workplace* Perceived as essential *i.e., required to enable staff to do their job* ☑ Trust *e.g., between colleagues and/or patients* ☑ Low risk awareness
Prevalence	Low – prevalent across one site (although this behaviour has also been reported in the literature at other healthcare sites)
Potential Impact(s)	☑ Unauthorized (or third party) access - or theft - of sensitive/personal data Introduction of malware to hospital systems (could potentially also impact medical devices) Introduction of computer virus to hospital systems (could potentially also impact medical devices) Data input errors impacting on patient care ☑ Data not centrally updated on hospital systems Malicious usage of hospital systems ☑ Breach of regulations (e.g., GDPR, law) Physical theft – or physical manipulation – of medical devices Insider threat Non-repudiation

5.2.5 Poor physical security

Scenario 9: Poor physical security

Description	An administration assistant notes someone she/he does not recognise walking past her/his office, in a staff only area. There is little physical security to the office, i.e., staff does not need a special access key. However, the hospital is too large for staff to be able to identify all of their colleagues, therefore it is not unusual for staff to not recognise someone working in the same department. The person appears professional, confident and looks like she/he knows where she/he is heading to, i.e., she/he does not appear lost or hesitant. Therefore, the admin assistant continues with his work and does not interrupt or question the individual.	
Motivation for behaviour		
		Security as a barrier to productivity *e.g., prioritizing of timely, efficient healthcare; heavy workload/time pressure*
	☑	Common behaviour *i.e., social norm in the workplace*
		Perceived as essential *i.e., required to enable staff to do their job*
	☑	Trust *e.g., between colleagues and/or patients*
	☑	Low risk awareness
Prevalence	High – prevalent for all sites	
Potential Impact(s)		
	☑	Unauthorized (or third party) access - or theft - of sensitive/personal data
	☑	Introduction of malware to hospital systems (could potentially also impact medical devices)
	☑	Introduction of computer virus to hospital systems (could potentially also impact medical devices)
		Data input errors impacting on patient care
		Data not centrally updated on hospital systems
	☑	Malicious usage of hospital systems
	☑	Breach of regulations (e.g., GDPR, law)
	☑	Physical theft – or physical manipulation – of medical devices
		Insider threat
		Non-repudiation

5.3 Regulatory driven scenarios

This chapter presents the analysis of applicable regulations in terms of privacy and healthcare domain and prospect ones in terms of cybersecurity.

Based on these analyses and the process mentioned in Chapter 4.5, the identification of the relevance of regulations analysed led to a match with the PANACEA key topics supported also by the identification of regulatory scenarios. By these steps, regulatory requirements have been elicitated so that PANACEA can comply with regulatory constraints as mentioned in the overall Methodology in Chapter 4.1.

The following table summarises the results of the analyses performed for the study of relevant regulatory elements and match with PANACEA key topics and the new cybersecurity certification framework.

Existing applicable regulations	**Dynamic Risk Assessment**	**Secure Information Sharing**	**Security by Design**	**Identification and Authentication**	**Training**	**Governance**	**Nudging**	**Value Assessment**	**Implementation Guidelines**
GDPR 2016/679	x	x	x	x		x			
MDR/IVDR	x	x	x	x					
ISO 13485	x	x	x		x	x	x		x
ISO 27001	x	x	x	x	x	x			
EN 15224	x	x			x	x			
EN ISO 14971	x								
ISO 80002-2	x								
ISO 62304	x		x	x					
IEC 82304-1	x		x	x					x
ISO IEC 80001 -1	x					x			x
IEC/TR 80001-2-1	x								
IEC/TR 80001-2-2		x							
IEC/TR 80001-2-3		x							
IEC/TR 80001-2-4									x
Legge n. 24/2017 (Legge Gelli)	x	x				x			x

Table 11: Match between Regulations and PANACEA key topics

The new cybersecurity certification framework has been analysed by identifying the roles of the three main regulatory levels, namely the national role, the EU role (national scheme/delegates/bodies) and the EU role (European scheme). Such analysis has comprised the following points summarised in the tables below reported:

- Role of National Cybersecurity Certification Authorities and de-activation of conflict on national schemes
- New national schemes / references & preparation of candidate European schemes
- Fines / complaint / courts, guidelines & regular re-assessment
- European Cybersecurity Certification Group
- Notification of Certification Accredited Bodies
- Peer review and Stakeholder Cybersecurity Certification Group
- Issuing European certificates and ENISA website
- Adopting related legal acts
- Self-declaration
- Voluntary vs. mandatory
- Residual national role (subsidiarity)

Role of NCCAs & de-activation of conflicting national schemes	
National role	Role of NCCAs: Each Member State shall designate one or more national cybersecurity certification authorities. Each Member State shall inform the Commission of the identity of the designated NCCAs … Member States shall ensure … activities are carried out independently from each other NCCAs shall: supervise and enforce rules included in European cybersecurity certification schemes …; monitor compliance … of the manufacturers … that are established in their respective territories …; actively assist and support the national accreditation bodies in the monitoring and supervision of the activities of CABs … and … of the public bodies; authorise CABs in accordance with Article 60(3) …; handle complaints by natural or legal persons …; provide an annual summary report …; cooperate with other NCCAs or other public authorities …; monitor relevant developments Each NCCA has at least the power … to request CABs, European cybersecurity certificates' holders and issuers of EU statements of conformity to provide any information it requires …; carry out investigations, in the form of audits, …; take appropriate measures …; obtain access to the premises of any CABs or holders of European cybersecurity certificates …; withdraw … certificates …; impose penalties … and to require the immediate cessation of breaches NCCAs shall cooperate with each other and with the Commission, in particular, by exchanging information, experience and good practices as regards cybersecurity certification and technical issues concerning … cybersecurity
EU role (European scheme)	De-activation of conflicting national schemes: … national cybersecurity certification schemes, and the related procedures … that are covered by a European cybersecurity certification scheme shall cease to produce effects from the date established in the implementing act adopted pursuant to Article 49(7). … schemes and … procedures … that are not covered by a European cybersecurity certification scheme shall continue to exist. Member States shall not introduce new national cybersecurity certification schemes … already covered by a European cybersecurity certification scheme that is in force. Existing certificates that were issued under national cybersecurity certification schemes and are covered by a European cybersecurity certification scheme shall remain valid until their expiry date.

	(ENISA's) website (on the schemes/certificates) shall also indicate the national cybersecurity certification schemes that have been replaced by a European cybersecurity certification scheme.

New national schemes / references & preparation of candidate European schemes	
National role	(Information about new national schemes) With a view to avoid the fragmentation of the internal market, Member States shall inform the Commission and the ECCG of any intention to draw up new national cybersecurity certification schemes. (Reference to national standards/schemes) A European … scheme shall include … references to the international, European or national standards applied in the evaluation …; identification of national or international cybersecurity certification schemes covering the same type or categories of ICT products
EU role (national scheme/delegates/bodies)	(Preparation of candidate schemes) Inclusion of specific ICT products … in the Union rolling work programme shall be justified on the basis of … the availability and the development of national cybersecurity certification schemes … as regards the risk of fragmentation; relevant Union or Member State law or policy; request for the preparation of a specific candidate scheme by the ECCG. The Commission shall take due account of the opinions issued by the ECCG and the Stakeholder Certification Group on the draft Union rolling work programme. In duly justified cases, the Commission or the ECCG may request ENISA to prepare a candidate scheme or to review an existing European cybersecurity certification scheme which is not included in the Union rolling work programme. ENISA shall closely cooperate with the ECCG. The ECCG shall provide ENISA with assistance and expert advice in relation to the preparation of the candidate scheme … ENISA shall take utmost account of the opinion of the ECCG before transmitting the candidate scheme … to the Commission. The opinion of the ECCG shall not bind ENISA, nor shall the absence of such an opinion prevent ENISA from transmitting the candidate scheme to the Commission. In duly justified cases, … the ECCG may request ENISA to prepare a candidate scheme or to review an existing … scheme which is not included in the Union rolling work programme. Following a request from the ECCG … ENISA may (not „shall“) prepare a candidate scheme … If ENISA refuses such a request, it shall give reasons … If necessary, … the ECCG may request ENISA to start the process of developing a revised candidate scheme
EU role (European scheme)	(Preparation of candidate schemes) The Commission shall publish a Union rolling work programme … that shall identify strategic priorities for future European cybersecurity certification schemes. The Commission may request ENISA to prepare a candidate scheme or to review an existing … scheme on the basis of the URWP. In duly justified cases, the Commission … may request ENISA to prepare a candidate scheme or to review an existing … scheme which is not included in the URWP. Following a request from the Commission …, ENISA shall (not "may") prepare a candidate scheme which meets the requirements set out in Articles 51, 52 and 54. The Commission, based on the candidate scheme prepared by ENISA, may adopt implementing acts … If necessary, the Commission … may request ENISA to start the process of developing a revised candidate scheme ENISA shall consult all relevant stakeholders … For each candidate scheme, ENISA shall establish an ad hoc working group … At least every 5 years (after a Commission implementing act adoption), ENISA shall evaluate each adopted European cybersecurity certification scheme, taking into account the feedback received from interested parties. ENISA shall support and promote … by recommending appropriate technical

	specifications for use in the development of European … schemes … where standards are not available; preparing … candidate schemes; evaluating adopted European … schemes

Fines / complaint / courts, guidelines & regular re-assessment	
National role	- Fines: Member States shall lay down the rules on penalties applicable to infringements of this Title and to infringements of European cybersecurity certification schemes, and shall take all measures necessary to ensure that they are implemented. - Complaint: Natural and legal persons shall have the right to lodge a complaint with the issuer of a European cybersecurity certificate or, where the complaint relates to a European cybersecurity certificate issued by a conformity assessment body when acting in accordance with Article 56(6), with the relevant national cybersecurity certification authority. - Courts: Notwithstanding any administrative or other non-judicial remedies, natural and legal persons shall have the right to an effective judicial remedy with regard to: (a) decisions taken by the authority or body referred to in Article 63(1) including, where applicable, in relation to the improper issuing, failure to issue or recognition of a European cybersecurity certificate held by those natural and legal persons; (b) the failure to act on a complaint lodged with the authority or body referred to in Article 63(1). Proceedings pursuant to this Article shall be brought before the courts of the Member State in which the authority or body against which the judicial remedy is sought is located.
EU role (national scheme/delegates/bodies)	Elaboration of guidelines: ENISA shall compile and publish guidelines and develop good practices, concerning the cybersecurity requirements of ICT products, ICT services and ICT processes, in cooperation with national cybersecurity certification authorities and industry in a formal, structured and transparent way. ENISA shall contribute to capacity-building related to evaluation and certification processes by compiling and issuing guidelines as well as by providing support to Member States at their request.
EU role (European scheme)	Regular re-assessment of scheme: The Commission shall regularly assess the efficiency and use of the adopted European cybersecurity certification schemes and whether a specific European cybersecurity certification scheme is to be made mandatory through relevant Union law … The first such assessment shall be carried out no later than 31 December 2023, and subsequent assessments shall be carried out at least every two years thereafter. Based on the outcome of those assessments, the Commission shall identify the ICT products, ICT services and ICT processes covered by an existing certification scheme which are to be covered by a mandatory certification scheme. As a priority, the Commission shall focus on the sectors listed in Annex II of Directive (EU) 2016/1148, … When preparing the assessment the Commission shall: take into account the impact of the measures on the manufacturers … and on the users in terms of the cost of those measures and the societal or economic benefits …; the existence and implementation of relevant Member State and third country law; carry out an open, transparent and inclusive consultation process with all relevant stakeholders and Member States; take into account any implementation deadlines … with regard to the possible impact of the measure on the manufacturers… SMEs; propose the most speedy and efficient way in which the transition from a voluntary to mandatory certification schemes is to be implemented.

ECCG	
National role	The ECCG shall be composed of representatives of NCCAs or representatives of other relevant national authorities. A Member of the ECCG shall not represent more than two Member States. The ECCG shall have the task … to advise and assist the Commission in

	its work to ensure the consistent implementation and application of this Title … URWP; assist, advise and cooperate with ENISA in relation to the preparation of a candidate scheme …; adopt an opinion on candidate schemes …; request ENISA to prepare candidate schemes …; adopt opinions addressed to the Commission relating to … schemes; examine relevant developments in the field of cybersecurity certification …; facilitate the cooperation between NCCAs … by establishing methods for the efficient exchange of information …; support the implementation of peer assessment mechanisms …; facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards … by making recommendations to ENISA to engage with relevant ISOs to address … gaps in … standards. NCCAs: It is appropriate that national cybersecurity certification authorities participate in the ECCG in an active, effective, efficient and secure manner. The outcomes of peer reviews (see below) shall be examined by the ECCG … In adopting implementing acts (for methodologies on peer reviews), the Commission shall take due account of the views of the ECCG.
EU role (national scheme/delegates/bodies)	With the assistance of ENISA, the Commission shall chair the ECCG, and the Commission shall provide the ECCG with a secretariat in accordance with point (e) of Article 8(1). ENISA shall support and promote (...) by assisting the Commission in providing the secretariat of the ECCG pursuant to Article 62

Notification of CABs	
National role	- Notification of CABs: For each European cybersecurity certification scheme, the NCCAs shall notify the Commission of the CABs that have been accredited … and … of any subsequent changes … A NCCA may submit to the Commission a request to remove a CAB notified by that authority from the list - Accreditation of CABs: The CABs shall be accredited by national accreditation bodies appointed pursuant to Regulation (EC) No 765/2008 … Where a European cybersecurity certificate is issued by a NCCA … the certification body of the NCCA shall be accredited as a CAB … Where European cybersecurity certification schemes set out specific or additional requirements … only CABs that meet those requirements shall be authorised by the NCCA … The accreditation … shall be issued to the CABs for a maximum of five years … National accreditation bodies shall take all appropriate measures within a reasonable timeframe to restrict, suspend or revoke the accreditation of a CAB
EU role (national scheme/delegates/bodies)	One year after the entry into force of a European cybersecurity certification scheme, the Commission shall publish a list of the CABs notified under that scheme in the Official Journal of the European Union. If the Commission receives a notification after the expiry of the period referred to in paragraph 2, it shall publish the amendments to the list of notified conformity assessment bodies in the OJEU within two months of the date of receipt of that notification. The Commission may adopt implementing acts to establish the circumstances, formats and procedures for notifications (On nofitication by the NCCA) The Commission shall publish the corresponding amendments to that list in the OJEU within one month of the date of receipt of the national cybersecurity certification authority's request.

Peer review & SCCG	
National role	With a view to achieving equivalent standards throughout the Union in respect of European cybersecurity certificates and EU statements of conformity, NCCAs shall be subject to peer review. … Peer review shall be carried out by at least two NCCAs of other

	Member States and the Commission and shall be carried out at least once every five years. Peer review shall assess … whether the activities of the NCCAs that relate to the issuance of European cybersecurity certificates … are strictly separated from their supervisory activities …; the procedures for supervising and enforcing the rules for monitoring the compliance … with European cybersecurity certificates …; and … the obligations of manufacturers…; the procedures for monitoring, authorising and supervising the activities of the CABs; whether the staff of authorities or bodies that issue certificates for assurance level 'high' … have the appropriate expertise.
EU role (national scheme/delegates/bodies)	The Commission may adopt implementing acts establishing a plan for peer review which covers a period of at least five years, laying down the criteria concerning the composition of the peer review team, the methodology to be used in peer review, and the schedule, the frequency and other tasks related to it. ENISA may participate in the peer review. ENISA shall support and promote (...) by participating in peer reviews pursuant to Article 59(4)
EU role (European scheme)	SCCG: The Stakeholder Cybersecurity Certification Group shall be co-chaired by the representatives of the Commission and of ENISA, and its secretariat shall be provided by ENISA. ENISA shall provide the secretariat of the Stakeholder Cybersecurity Certification Group pursuant to Article 22(4).

Issuing European certificates & ENISA website	
National role	The CABs (and NCCAs) … shall issue European cybersecurity certificates … referring to assurance level 'basic' or 'substantial' (or 'high') on the basis of criteria included in the European cybersecurity certification scheme … The natural or legal person who submits ICT products, ICT services or ICT processes for certification shall make available to the … CAB … all information necessary to conduct the certification. The (certificate) holder … shall inform the NCCA or CAB of any subsequently detected vulnerabilities or irregularities concerning the security … that may have an impact on its compliance with the (certification) requirements … That CAB … shall forward that information without undue delay to the NCCA concerned.
EU role (national scheme/delegates/bodies)	… in duly justified cases a European cybersecurity certification scheme may provide that European cybersecurity certificates resulting from that scheme are to be issued only by a public body. Such body shall be one of the following: a NCCA … or a public body that is accredited as a CAB
EU role (European scheme)	ENISA shall maintain a dedicated website providing information on, and publicising, European cybersecurity certification schemes, European cybersecurity certificates and EU statements of conformity, including information with regard to European cybersecurity certification schemes which are no longer valid, to withdrawn and expired European cybersecurity certificates and EU statements of conformity, and to the repository of links to cybersecurity information provided in accordance with Article 55.

Adopting related legal acts	
National role	In the absence of harmonised Union law, Member State law may also provide that a European cybersecurity certification scheme may be used for establishing the presumption of conformity with legal requirements.

EU role (European scheme)	Where a specific Union legal act so provides, a certificate or an EU statement of conformity issued under a European cybersecurity certification scheme may be used to demonstrate the presumption of conformity with requirements of that legal act.

Self-declaration	
National role	The manufacturer … shall make the EU statement of conformity, technical documentation, and all other relevant information relating to the conformity … with the scheme available to the NCCA for the period provided for in the corresponding European cybersecurity certification scheme.
EU role (European scheme)	A copy of the EU statement of conformity shall be submitted to the national cybersecurity certification authority and to ENISA.

Voluntary vs. mandatory	
National role	The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.
EU role (European scheme)	The issuing of an EU statement of conformity is voluntary, unless otherwise specified in Union law or Member State law.

Residual national role (subsidiarity)	
National role	If in doubt national entities have a role (subsidiarity principle) if not justified otherwise by scope or objective of CSA Title III (certification framework), CSA mandate for ENISA or CSA general objective OR if it falls under exemption for public security/defence.
EU role (European scheme)	(Scope of CSA Title III) The European cybersecurity certification framework shall provide for a mechanism to establish European … schemes and to attest that the ICT products … comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services and processes throughout their life cycle. (Objective of CSA Title III) … in order to improve the conditions for the functioning of the internal market by increasing the level of cybersecurity … and enabling a harmonised approach … to European … schemes … creating a digital single market (CSA mandate) ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. … contribute to the establishment and maintenance of a … framework in accordance with Title III …, with a view to increasing the transparency of the cybersecurity of ICT products … strengthening trust in the digital internal market and its competitiveness. (CSA general objective) … for the establishment of … schemes for the purpose of ensuring an adequate level of cybersecurity Apart from the CSA, specific EU legal acts on certification (voluntary or mandatory) may apply so that EU level action is justified.

In the following, examplatory regulatory scenarios representative of the impact on PANACEA health domain are reported.

5.3.1 Scenario 1: Business Continuity and Incident Reporting for Digital Service Provider Security Incidents

NIS Directive mentions in recital 48 that many businesses in the Union rely on digital services. As they are an important resource, such services should always have alternatives available. NIS Directive continously highlights that security, continuity and reliability of the type of digital services are of the essence for the smooth functioning of many businesses. In this respect, security measures and incident reporting obligations are applicable for Digital Service Providers (DSPs) in the context of the NIS Directive.

Business Continuity and Incident Reporting for Medical Device Security Incidents	
Description	During implementation of a digital service for healthcare, functionality of incident reporting is not implemented. Whenever a fault happens nothing is communicated to the customer.
Criticality	High – The criticality is high because of the broad range of follow-up attacks that may be possible after a successful phishing attack.
Likelihood	High – Suppliers are mostly concerned that the service works correctly during the test phase and are not worried about possible other scenarios.
Impact	It is difficult to make a general statement about the impact. It depends on the activities of business continuity adopted and the criticality of the service.

No incident reporting is implemented

A fault happens

Nothing is reported

5.3.2 Scenario 2: Software Maintenance Process

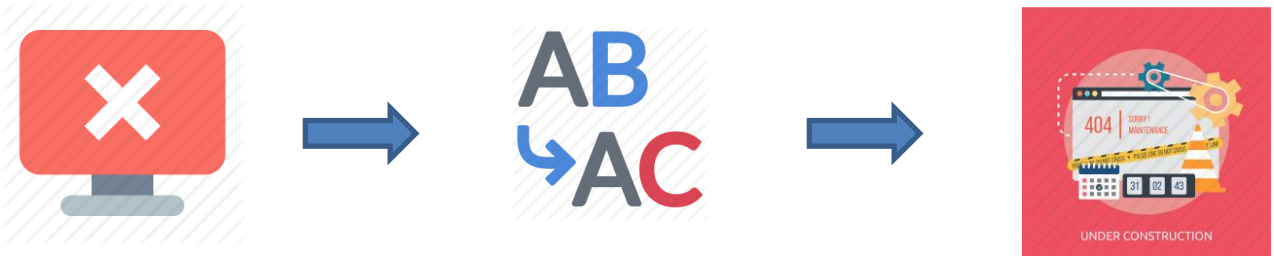
Part 6 of IEC 62304 describes processes for software maintenance. This includes:

- 6.1: Establishment of software maintenance plan.
- 6.2: Problem and modification analysis.
- 6.3: Implementation of modifications.

It's important to take user feedback and resolve issues in the maintenance phase.

Software Maintenance Process	
Description	During normal/daily operations, a systematic fault happens. A change request is raised but medical device supplier does not apply the change management process properly. Change request is lost.

Criticality	Medium – The criticality is medium because big issue should be quickly addressed.
Likelihood	Medium – Big issues are addressed as the fault happens.
Impact	Medium – During the normal operations in addressing new releases of medical device / IT services / software issue



A fault happens

A change request is forwarded

Change is not implemented

5.3.3 Scenario 3: Transfer of Information to a Third Country or International Organizations

The transfer of personal data to recipients outside the European Economic Area (EEA) is generally prohibited unless:

- the jurisdiction in which the recipient is located is deemed to provide an adequate level of data protection;
- the data exporter puts in place appropriate safeguards; or
- a derogation or exemption applies.

Understanding the application of lawful data transfer mechanisms is essential for all organisations that wish to transfer personal data to recipients located outside the EEA (including processors, such as cloud service providers).

Transfer of Information to a Third Country or International Organizations	
Description	During normal operations, data should be uploaded in cloud. Organization perform this action without in advance reviewing their existing and planned business operations identifing the circumstances in which personal data are being transferred to recipients located outside the EEA and ensuring for each such transfer a data transfer mechanism that complies with the requirements of the GDPR.
Criticality	High – Bad management of confidential data has a high impact on the organizations.
Likelihood	Low – Organisations that engage in Cross-Border Data Transfers are few. Furthermore, this scenario is intensively tested in EU widely [RD 4].
Impact	Medium – The impact of the GDPR on this issue is likely neutral for most organisations.

Operations for the GDPR compliance are not performed

Cross-Border Data Transfers is performed

GDPR violation

5.3.4 Scenario 4: Removal or Adjustment of Access Rights

According with the control A.9.2.6 of ISO27001:2013, "The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change."

Removal or adjustment of access rights	
Description	A doctor can consult the clinical situation of a patient. Patient is transferred under a new doctor but rights are not management properly and the previous doctor can still access the folder of the patient.
Criticality	High – Bad management of confidential data have a high impact on the organizations.
Likelihood	High – Access rights are not well addressed in healthcare organizations.
Impact	High – Data should be consultable only from personnel who have access right to do so.

Doctor has access to the medical folder of a patient

A new doctor has assigned to the patient

Previous doctor still has access to the medical folder of the patient

5.3.5 Scenario 5: Role of Risk Owner

The role of risk owner is important inside the Information Security Management System: it is in charge for approving the information security risk treatment plan and accepting the residual information security risk plan. Without this figure, there is the possibility that a risk is not handled properly and the organization could be unprepeared, if it shows itself or repeats again.

Role of Risk Owner	
Description	Risk Owner is not foreseen as a role within the Healthcare Organization. No one accepts the security risk treatment plan and

	no countermeasures are put in place. The risk materializes and the organization is not ready to face it.
Criticality	High – If the risk exhibits itself, the organization cannot tackle it in a proper way.
Likelihood	High – Currently no high number of organizations put in place a risk management process.
Impact	High – If the risk is not managed properly, it is possible to have a disruption experience.

6. End-Users and Stakeholders Requirements

6.1 Overview

Developing products and services that meet the expectations of users and customers is critical for success. Requirement analysis is the foundation of a user-centred approach, creating products that appeal and meet user needs at the closest level. While it is a common tendency for designers to be anxious about starting the design and implementation, discussing requirements with the customer is vital in the deployment of safety-critical systems. Activities in this first stage have significant impact on the downstream results in the system life cycle. Indeed, errors developed during the requirements and specifications stage may lead to errors in the design and implementation stage. When this error is discovered, the engineers must revisit the requirements and specifications to fix the problem. This leads not only to a large amount of wasted time but also to the possibility of other requirements and specifications errors. Many incidents are traced back to requirements flaws, incomplete implementation of specifications, or wrong assumptions about the requirements. This cannot be tolerated in safety-critical systems. Therefore, it is necessary that the requirements are specified correctly to generate clear and accurate specifications.

User requirements analysis provides precise descriptions of the content, functionality and quality demanded by prospective users. For the identification of user needs, the user perspective must be assumed and result in:

Functional Requirements: The goals that users want to reach and the tasks they intend to perform with the new product must be determined. By recognising the Functional Requirements, we understand the tasks that involve the abstraction of why the user performs certain activities, what her/his constraints and preferences are.

Non-functional requirements: Constraints on the services or functions offered by the system , such as timing constraints, constraints on the development process, standards, etc. Often apply to the system as a whole rather than individual features or services.

Non-functional requirements define system properties and constraints, e.g. reliability, response time and storage requirements. Non-functional requirements may be more critical than functional requirements. If these are not met, the system may be useless. In this scope, three classes of non-functional requirements were taken into account (Figure 7):

1. **Product requirements**: Requirements which specify that the delivered product must behave in a particular way e.g. in terms of execution speed, reliability, etc.
2. **Organizational requirements**: Requirements which are a consequence of organizational policies and procedures e.g. process standards used, implementation requirements, etc.
3. **External requirements**: Requirements which arise from factors which are external to the system and its development process e.g. interoperability requirements, legislative requirements, etc.

.

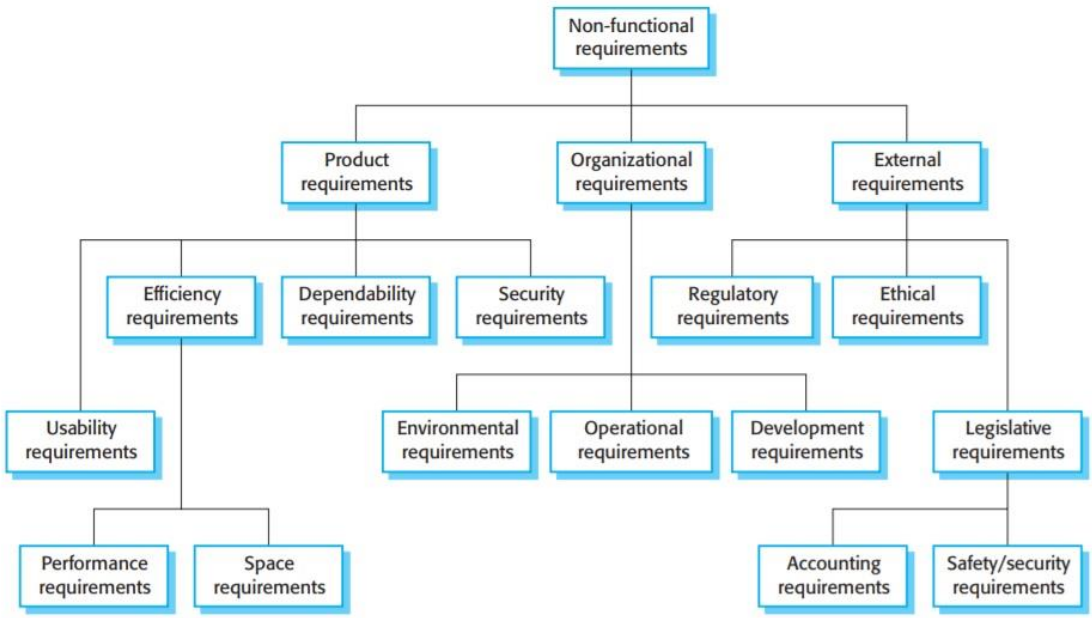


Figure 7: Organisation of PANACEA User and Stakeholders Requirements

A relevant issue is related to understanding the importance of a specific requirement as object of analysis. That is to understand which requirements have a higher priority compared to the other ones. For such reason, the level of priority has been assessed by end users for each requirement, based on both survey and internal expertise. Again, from **a technical perspective, a classification of mandatory and optional requirements will be performed**, taking into account both the users' requirements priority level (what users necessarily want to have) and the system functionalities (what the system must offer to ensure that the requirements are satisfied and the system is properly working). This second point will be presented in the chapter related to technical requirements (D1.3 "Panacea Technical Requirements").

The PANACEA User Requirements results are reported in Annex B End-Users and Stakeholders Requirements. All the requirements are reported in a table that introduces the text and also relevant information. Among other fields, the template includes:

- Source: from where information was gathered in order to formulate the requirements (e.g. workshop, risk scenario …)
- User(s) involved: type of end users involved in the requirement. The categories we took into account were:
    1 Managers;
    2 Health roles (e.g. Generalist Medical Practitioners, Specialist Medical Practitioners, Nurses, Paramedical practitioners, Medical and Pharmaceutical Technicians, Ambulance Workers, Personal care workers in Health Services);
    3 Non-Health Roles (e.g. Technical roles, Administrative back-office roles, Administrative front-office roles, Medical Secretaries, Information and Communications Technology roles);
    4 External Roles (e.g. patients, suppliers);

The defined template established is presented in the following table (Table 12).

Field	Value

ID	ID: a unique ID obeying the following naming convention: User requirements ((non)functional): <NATURE_REQUIREMENT>_<CLASS>_USER_FUN/NONFUN_<XX> where: - <NATURE_REQUIREMENT> = GEN (General), TOP (Topic-Specific) - <CLASS> = RSK (Risk Assessment and Mitigation), ISH (Information Sharing), SDC (Security-by-Design/Certification), IA (Identification and Authentication), GOV (Governance), HF (Human Factor), VAL (Value Assessment), IMP (Implementation Guidelines) - <FUN/NONFUN> = Functional Requirement or Non-Functional Requirement, respectively, - <XX> = a number over two digits, increasing for the same reference, starting from 0 for the first reference. e.g. FUNC and NONFUNC will both start at 0
Title	An intuitive short name for the requirement
Category	Class of the requirement (functional, product, organizational, external)
Description	It contains a short text describing the requirement
Justification	A short text explaining the necessity and reasons to include this requirement
Priority	It could be high, medium or low
Version	Number of update of the requirement (starting from 1.0) to help the traceability and versioning
Source	Where this user requirement was extracted from (survey, SoA, consortium expertise)
User(s) Involved	Type of user/stakeholder involved

Table 12: Template Table for PANACEA End-Users and Stakeholders Requirements definition.

6.2 General requirements

General requirements introduce the functionalities of the PANACEA toolkit in its overall. Indeed, they introduce the two main families of toolkits and the capability of working separately. Furthermore, these requirements represent common characteristics of all the tools that are going to form the PANACEA toolkit.

Their origin comes mainly from the Statement of Applicability or from consortium expertise except for the regulation requirements that come from the Cyber Security Act, a new European initiative that aims at improving resilience against cyber-attaks.

From the workshops lead with stakeholders, it emerged that staff within a very fast-paced, unique and potentially stressful environment, with a lot of time pressures and responsibilities, such as the heathcare sector, do not always facilitate/adopt secure behaviour. Many of the unsecure behaviours identified during these focus groups are driven from a need for procedures to be quick and convenient for staff – particularly when patient care (and potentially lives) can depend upon staff acting quickly. For example, in some healthcare environments, it is not possible for technology to impose certain security behaviours such as auto log-off, nor it is feasible for staff to have to follow several steps to access one system. This highlights that, for many of the platforms PANACEA will support, any interventions must be user-friendly, user transparent when possible, time-efficient and unburdensome, otherwise they will at best, be ineffective (e.g., promoting staff to find 'workarounds') or at worst, negatively affect upon patient care. This need for quick, convenient, transparent systems is also seen in the workarounds that staff have created (e.g., use of WhatsApp).

It is also vital that we understand the potential for unintended consequences of increasing security measures, for example if they influence negatively upon work and/or patient care. In order to facilitate positive and effective behaviour change, it is necessary to understand more about the factors that affect behaviour in the workplace (such as motivations and influencers).

To summarize, systems and security measures must be:

- Unburden some, user-friendly, time efficient
- Coherent – with consistent rules across systems (e.g., password rules) and updates that are easy to apply system-wide
- Understandable - with adequate education and training
- Reflective of actual daily work responsibilities, not simply those written in their job description
- Require the minimum intervention on behalf of the staff, particularly in time-pressuring health environments (like Emergency Departments)

6.3 Topic-specific End-Users Requirements

6.3.1 Risk Assessment and Mitigation

The activities in the scope of dynamic risk assessment and mitigation actions aim in continually assessing the risk inside an HCO and propose mitigation action in order to reduce the computed risk.

For this topic, Medical Device Manufacturer group and IT Security group were interviewed. At the beginning, the presence of functions in order to perform a dynamic risk assessment process have been investigated. Results are shown in Figure 8. As it is possible to see, Dynamic Security Testing, Endpoint Control/Network inventory Management and Prioritization of Mitigation Action are broadly performed by the two categories under consideration. For the Medical Device manufacturers, Data loss prevention is not covered while for IT security group in HCOs, a large sample of interviewes admitted that nothing is implemented for Business impact analysis and User behavioural analysis. Furthermore, for medical device manufacturers, 50% of interviewes have in place processes for identifing, estimating, and prioritizing risks and conducting a business impact analysis. This is the situation, although they stressed the importance of these processes. For this argument, also some part of the non-technical and managerial group highlighted the importance of all of these processes and would like to have them applied inside the HCOs.

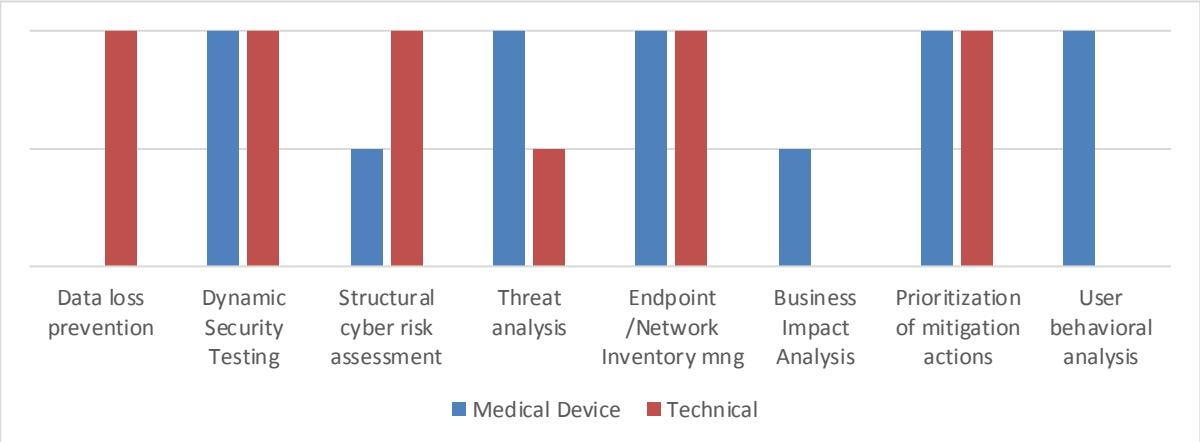


Figure 8: Dynamic risk assessment processes covered in HCO.

About the IT services that are available in HCO, the groups showed predominantly the same opinion except for facility management services and infrastructure services that are considered less important from the IT group and the medical device manufacturers respectively.

For both groups, the most of the focus in Dynamic Risk Assessment should be in the administrative and technical aspects, stressing the fact that all the roles should be kept under strictly control.

Among the various parameters to be taken into account for countermeasures formulation, two are the indexes that cannot be missed:

1 Risk reduction and,
2 Business impact.

Finally, the following aspects were considered as very important features: the provision of local view related to specific area, the full proactive risk management that interact with operators, rank countermeasures based on the above listed index, and consideration of the human factor in the risk analysis.

For this last point, what emerged by the stakeholders is that the role of manager is very critical and her/his activities should be monitored in order to prevent and detect phishing and ransomware attacks. On the other hand, regarding theft of information/devices, it could be a good practice to take into account the sudden disconnection of devices.

6.3.2 Information sharing

Secure information sharing is a fundamental tool in order to communicate in a secure way among all the PANACEA end users.

The major contribution for this group was provided by Technical group and Non-technical and managerial group. In the actual approach, weaknesses are observed especially for the lack of information sharing interoperability protocols. Managerial personnel complain also about the non-compliance of the actual means with legal requirements, the lack of active security storing and, over the others, about the procedures defined not being user-friendly.

Amongst the different examples of communication proposed to the end users, their feedback was to improve communications:

1 Between HCO and patients, and;
2 Among the tenants (e.g. laws, regulation …).

As shown in Figure 9, the Technical group has identified the need to improve the information sharing between internet accessible services, e.g. communication by corporate e-mail, and applications for both patients and staff.

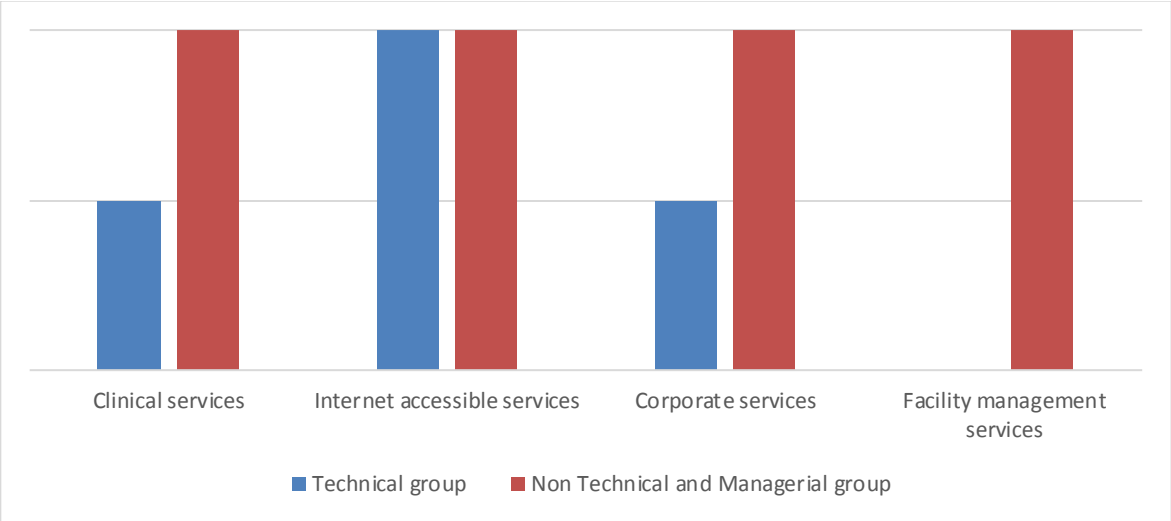


Figure 9: Applications where information sharing should be improved.

About the type of data managed, the least critical indicated by the two groups are the one related to the suppliers. All the criticality levels by type of data are reported in Figure 10

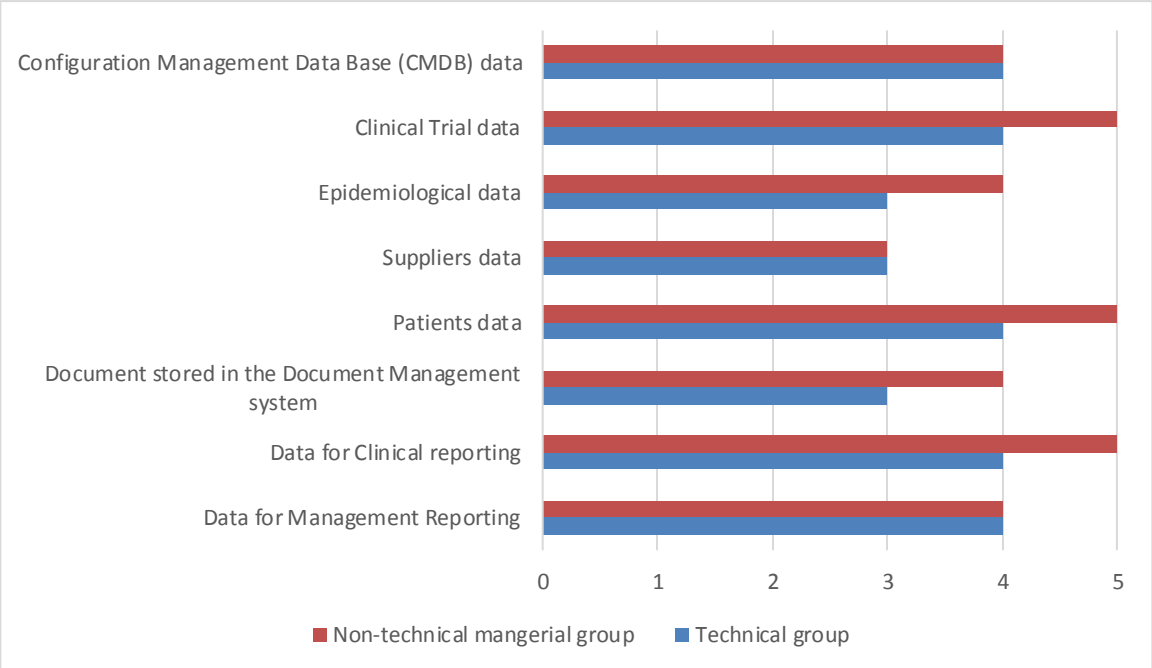


Figure 10: Criticality of data managed.

Regarding the question if blockchain could be considered as technological solution to manage access rights, the most part of technical group provide a negative feedback while non-technical group was in favour of this.

Very important is the management of the information from the GDPR point of view: the level of security may be appropriate to the importance of personal data and the communication among countries shall ensure a high protection level. On information sharing also ISO/IEC 27001, gives some regulations on how information

should be managed. Information shall be protected under the CIA (Confidentiality, Integrity and Availability) criteria perspective. Furthermore, in order to guide on how information should be treated, the level of classification of information should be well reported.

Loss of information can generate serious problems to healthcare organizations. Depending on the type of data, theft of information can lead to loss of reputation, law penalties and interruption of activities. In order to guarantee the correct working and interconnection of processes, business continuity procedures shall be defined.

6.3.3 Security-by-design and certification

Security by design is a technique that include the security aspects during the requirements and design definition phases. Since these aspects are introduced in embryonic stage, security will well fit with the architecture of the product and will reduce the vulnerabilities by hardening the product itself.

In security by design technique, three functions have been identified:

1. Static Application Security Testing System (SAST): Analyses application source code, byte code and binaries for coding and designs conditions that are indicative of security vulnerabilities.
2. Interactive Application Security Testing System (IAST): Instruments the application binary, which can enable both "application security testing"-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process, which provides significant benefits to DevOps approaches.
3. Security By Design Assessment System (SDAS): Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.

For medical device, the average of manufacturers that cover security by design functions is shown in Figure 11.

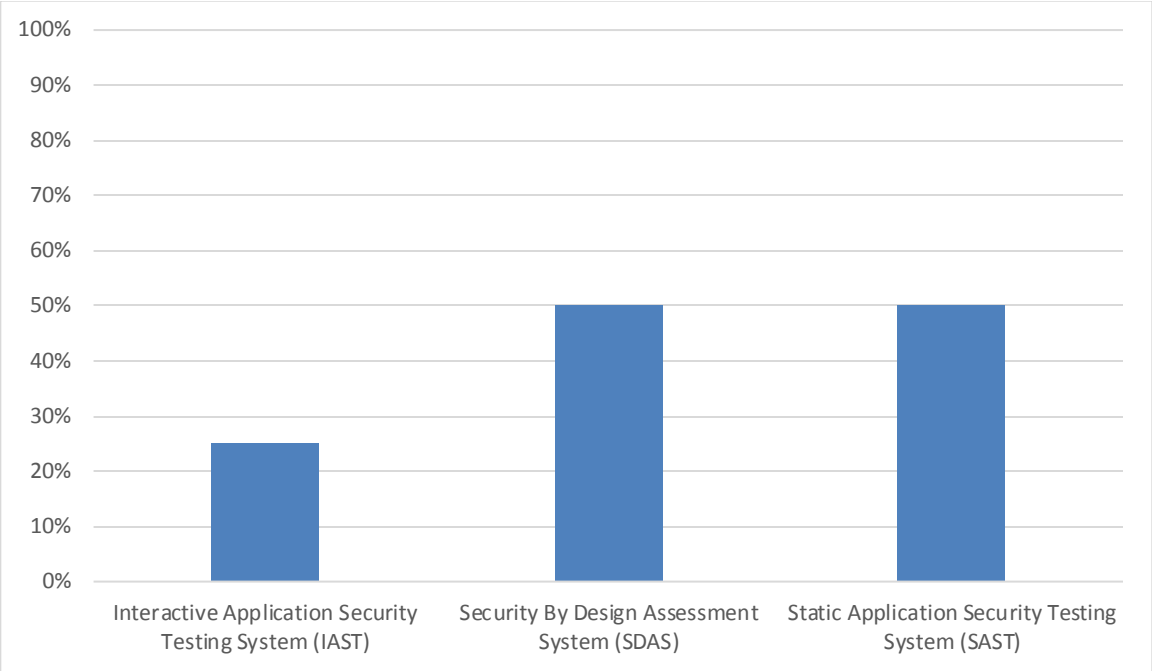


Figure 11: Security by design functions covered by medical device manufacturers.

Applied to information systems, the situation is equivalent.

Security by design should be applied to all the products and software that are involved with:

1 Mobile devices (e.g. portable ultrasound devices)
2 Wearable external devices (e.g. wireless temperature counter)
3 Implantable devices (e.g. cardiac pacemaker)
4 Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)
5 Supportive devices (e.g. assistive robot)

and to applications related to:

1 Internet Accessible Services
2 Corporate services
3 Facility Management services
4 Data services
5 Infrastructure services.

In general, there is a poor attention to new vulnerabilities tracking and management and there is not yet a dedicated team in charge of tracking and monitoring security incident related to system supporting healthcare processes, in order to implement the continuous improvement in security.

Hardening of products is one of the main issue for this topic. From what it is possible to infer from the risk scenarios, it is important that the medical devices and systems/software provided to healthcare organizations will be robust under the confidentiality point of view in order to avoid disclosure of data.

6.3.4 Identification and authentication

Identification and authentication are the first steps in order to allow access to resources. There are several situations where one needs to access the hospital system. In particular, it is possible to distinguish at first hand two categories of system interactions: people and objects (connected medical devices).

According to the technical and medical device manufacturers groups, the already covered functionalities covered in this ambit are shown in Figure 12.

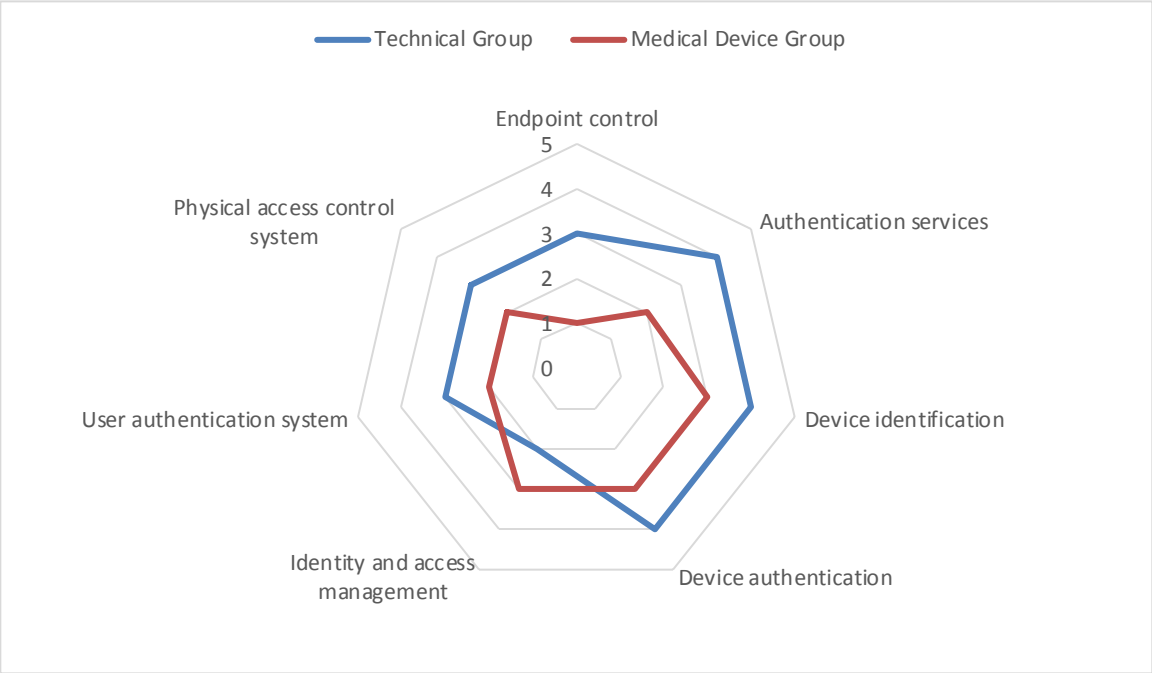


Figure 12: Functions covered in identification and Authentication process.

The result shows a low attention to all the functions related to the identification and authentication processes, even though all these functions are perceived of extreme importance from all the groups.

These functions should be improved and applied especially in tools related to Clinical services and Facility Management services and should be focused on manager's roles.

During workshop, experts of the consortium proposed different situations in order to understand how to address identification and authentication. The situations are the following:

1 The same medical device may connect to multiple hospital systems
2 Medical devices are directly talking to each other
3 Medical devices are permanently connected to the IT system
4 Medical Devices are permanently controlled during their use in hospital
5 Patients prefer more secure authentication even if authenticating is less simple
6 Patient connect to multiple hospitals
7 Patients connect from home for monitoring devices, instead of coming to the hospital

The result are shown in Figure 13.

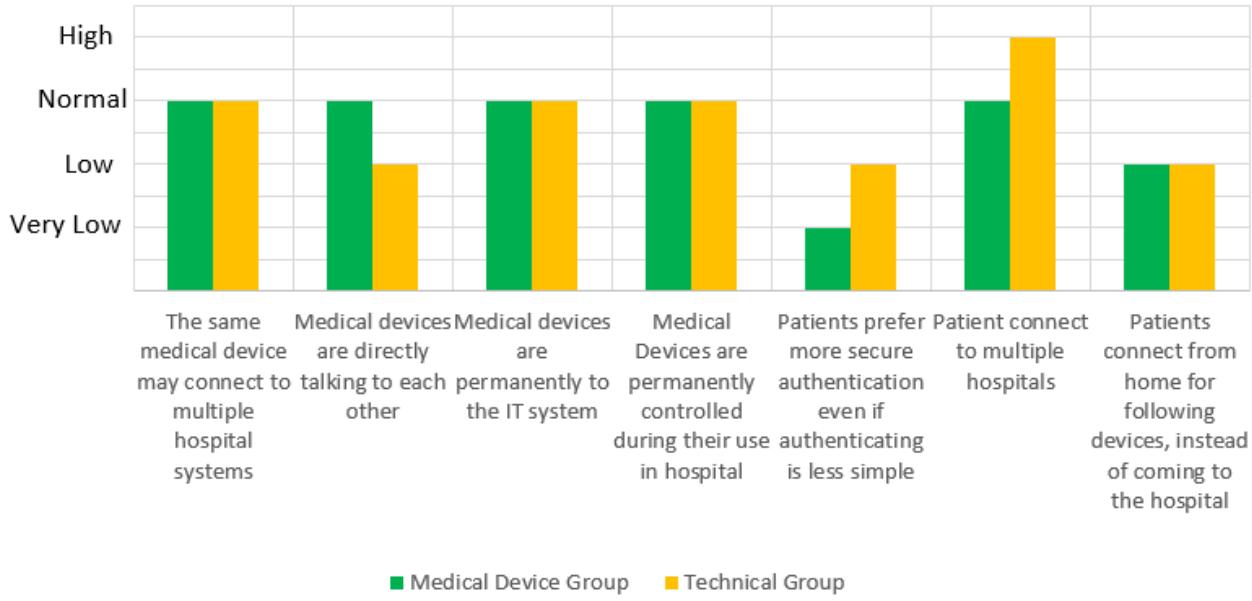


Figure 13: Frequency of happening of situations proposed by experts of consortium.

Furthermore, it is very frequent that patients connect to multiple HCOs.

Other features important for Identification and Authentication processes are:

1. Capability to manage the transfer of rights from one person to another on connected object (e.g. I am doctor Anna and I transfer the right to doctor Ahmed to operate the connected object of Ms. Alice)
2. Capability to manage the identification between hospital and the first aid services (firefighter, ambulance …)
3. It is it important that doctors/nurses who are using multiple "IT things" have different control, depending on situation

This topic is very important to satisfy the "need-to-know" principle and guarantee non-repudiation of actions. The first one is also related to GDPR, which is very strict about access to the personal data. For this reason, a revision of the access policy should be performed periodically, especially when particular events happen (e.g. termination of employment or change of duties).

Even de-registration process is very important to understand theft of devices. For this reason, a tool that permits identification and authentication shall communicate with a tool that provides dynamic risk assessment and mitigation actions.

Non-repudiation allows instead integrity and genuineness of data.

6.3.5 Governance

Governance is the system via which an organization directs and controls cyber security. In particular, governance determines who is authorized to make decisions to mitigate the risks, the accountability framework and provides surveillance to ensure risks are adequately mitigated. All these decisions are defined in order to be aligned with business objectives and consistent regulations.

According to [AD 1], the model for Cybersecurity in Healthcare Organizations foreseen five processes:

1 Identify: consists in developing an organizational understanding to manage cybersecurity risk for systems, people, assets, data, and capabilities,
2 Protect: consists in developing and implementing appropriate safeguards to ensure delivery of critical services,
3 Detect: consists in developing and implementing appropriate activities to identify the occurrence of a cybersecurity event,
4 Respond: consists in developing and implementing appropriate activities to take action in cases of a detected cybersecurity incident,
5 Recover: consists in developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Based on observations, the most qualified role responsible for these processes is the IT department, supported in Respond by a new ad-hoc function that reports to the security responsible of HCO.

For each process in cybersecurity, importance of each sub-processes was investigated. Information gathered lead to the fact that measures should be taken into account in order to direct and assess each sub-process identified.

For governance purposes, it is requested for top management to demonstrate leadership by defining:

1 security policies,
2 responsibilities and authorities for relevant roles and role segregation,
3 review champaign of security management system.

The governance has to rely on the concept that cybersecurity is a duty for everyone and it is not possible to delegate own duties to others. Of course, the level of responsibility is different for each role but shall be clear that the level of security depends on the weakest part of the process.

6.3.6 Human Behaviours

Insecure behaviours are commonplace across countries and healthcare organisations and awareness of breadth of risks associated with these behaviours is low, while awareness training is required to ensure that staff are more aware of the potential implications of their behaviour in the workplace.

The importance of training in order to decrease misbehaviour was recognized by all the stakeholders involved. Of course, of extreme importance are the:

1 Initial learning stage;
2 Refresher learning and;
3 Support of mechanisms in order to remind and guide on cyber security threats and processes daily.

Training should be focused on all type of processes in an HCO like hospital workflows, inter-hospital medical consultations and cross-border exchange of patient related data and for each roles, e.g. managers health roles, external partners …

The preferable training tools include scenario-based learning, case studies and support the transfer of learning into the workplace.

It is also vital that employees are clearly informed by their employer of what is expected from them – and why – and whom to approach if they require any further information or guidance. It is important that staff do not feel unsupported or kept "out of the loop". Many of the staff in our interviews reported feeling as if their roles were not recognised or were unimportant, and therefore they did not receive the training they required.

Therefore, one main point to be focused on is also the concept that cybersecurity is not something that can be demanded by someone else, but everyone should contribute in order to secure the environment. Some staff reported feeling that security is something that is imposed upon them, with no explanation provided. They expressed a desire to be informed about why these behaviours were important, again feeding back into the need for great guidance and training.

In order to improve knowledge and sensitivity about security, an awareness campaign plays a fundamental role. Nudges and tips should be provided to the personnel both inside and outside HCOs (e.g. system suppliers). High priority should be focused in improving awareness on how to share passwords, do not open suspicious documents attached to emails, information sharing, and about the antivirus usage.

Nudges and training can improve the misbehaviour of people. The most effective attack indeed is focused on people and is the social engineering attack. This can be carried out in different way: phishing is the most common and effective since induce internal people to provide sensitive data that can be exploited in order to carryout an attack. Other forms are for example dumpster diving or shoulder surfing. These kinds of attack exploits:

1 Familiarity: users are less suspicious of people they are familiar with;
2 Intimidation: people tend to avoid people who intimidate others around them;
3 Human curiosity: the social engineer may deliberately drop a virus infected flash disk in an area where the users can easily pick it up;
4 Human greed: the social engineer may lure the user with promises of making a lot of money.

Therefore, training and nudges shall be focused on improving these aspects.

6.3.7 Cyber-security Value Assessment

Defending against attacks is very expensive because while an attacker only has to find and exploit one vulnerability, those in charge of defending against attacks have to manage all possible vulnerabilities. For this reason, it is difficult to assess investment on cybersecurity: an organization must decide which risks to protect itself against, how subject it is to risks, and which ones it should insure itself against.

After the analysis of HCOs needs, inside the PANACEA scope it is needed to consider, in order assessing value of investment:

1 Tools of the Panacea Toolkit to be implemented (all the tools shall be able to operate as stand-alone tool)
2 Organizational scope (i.e. HCO roles/types of staff, processes, organizational functions/units)
3 Technical assets to be bought (applications, networks, medical devices)
4 Activities to be performed to do the investment
5 Activities to be performed over the time horizon, to ensure the usability of the investment
6 Existing assets to be modified/eliminated as a consequence of the investment
7 Costs related to all above elements

Furthermore, other aspects like budget, time needed in order to implement the cyber security solution, and the impact on the patients should be taken into account.

The time horizon over which cybersecurity investment should be evaluated is 5 years and the amortisation rate swings between 10% and 20%.

For this evaluation, anticipation of the future threat scenarios is fundamental. This can be done by studying new types of attack, checking frequencies of attacks, considering possibility of hybrid attack, analysing size of possible attacks and their average costs.

Return indicators are essential in order to make statistics and give the real perception about the value of investment. Indicators adapted for this task are:

1 Total differential cash flow
2 Total differential cash flow/investrment
3 Average differential recovery time
4 Average differential impact on the health of patients
5 Average differential data loss/corruption
6 Average differential impact on privacy

6.3.8 Cyber-security solutions implementation

In order to easily adopt solutions to contrast cyber attacks, guidelines and manuals about how these solutions work should be provided. This material should be on support of HCOs in order to accomplish the following steps:

1 Assessment and scoping. It consists in a preliminary assessment in terms of solutions to de implemented;
2 Customization design/Mitigation actions design. It consists in adapting the solution to the HC organisation;
3 Implementation. It consists in the actual installation of the customised solution;
4 Launch and testing. It consists in teaching the staff and in organizing pilots and for testing.

For each step, documentation should be provided that includes activities, key decision points and masterplans, templates, check-lists, examples, people involvement approaches.

In the Assessment and scoping step, particular emphasis should be put also in indentifing participants that will be involved in the solution adoption.

Difficulties in changing procedures and estimation of cost in training should be considered during the design phase. Furthermore, during the test phase, the human feedback should also be taken into account.

The guidelines and manuals are fundamental especially for risk assessment, secure information sharing, identification and authentication technologies and human behaviour corrections (Figure 14).

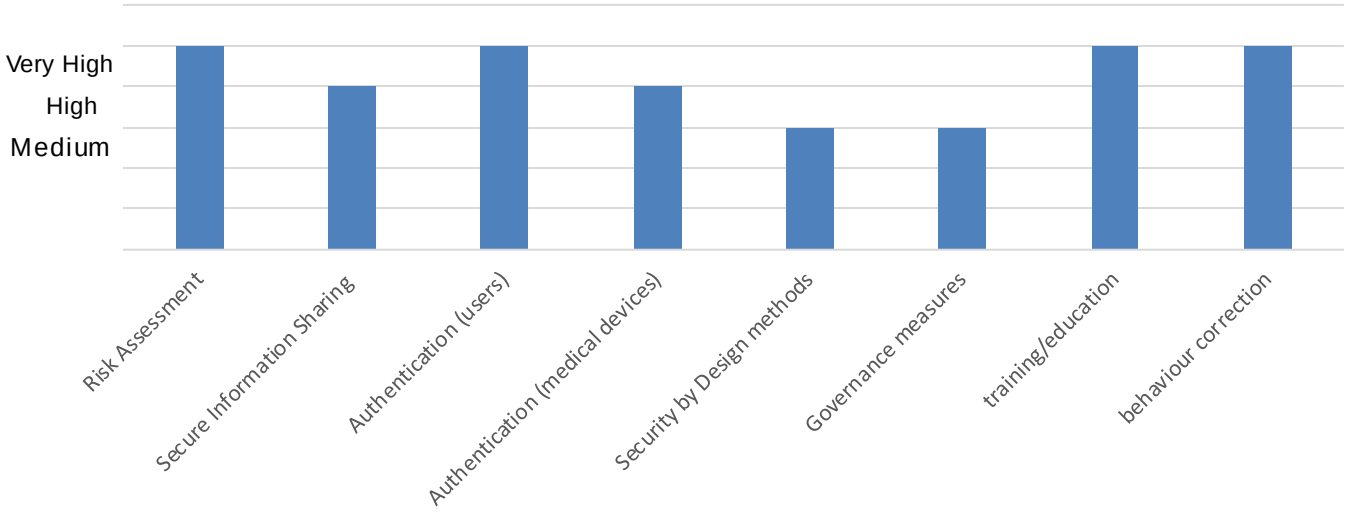


Figure 14: implementation needs against topics.

ISO 13485 addresses quality services and indicates which should be the documentation in order to provide quality services. This includes, but is not limited to:

1 a manual
2 documented procedures and records;
3 other documentation specified by applicable regulatory requirements.

7. Conclusions

Aim of this document is to collect all the stakeholders' needs and provide possible security risks / user scenarios at the end in order to perform the User Requirements Specification (URS) for the PANACEA Toolkit. Along the sections of this document:

- The methodology followed in order to interact with the stakeholders and elicit requirements has been detailed. Stakeholders groups have been introduced in order to give an idea about the profile of each interested part and which role is playing. After this, all the activities conducted in order to involve stakeholders and infer their needs have been explained: this included organization of workshop, interaction by means of web platforms and frontal interviews. Then, the process of information elaboration has been presented.
- Risk scenarios were introduced: a set of scenarios has been developed and introduced in order to understand which threats are most likely and which could be the requirements in order to contrast them. Scenarios have been introduced driven by cyber-attacks and the behaviour of stakeholders or imposed by regulations
- Results were exposed: information acquired by iteraction with stakeholders merged with knowledge of consortium experts has been reported. Information has then been used in order to write the requirements of end users.

Our overall findings suggest that lack in cybersecurity system and insecure behaviours are commonplace across countries and healthcare organisations: awareness of breadth of risks associated with these behaviours is low, and awareness of training is required to ensure that staff is more aware of the potential implications of their behaviour in the workplace.

It is also vital that employees are clearly informed by their employer of what is expected from them – and why – and whom to approach if they require any further information or guidance. It is important that staff do not feel unsupported or kept "out of the loop". Many of the staff have the feeling as if their roles were not recognised or were unimportant, and therefore they did not receive the training they required. It should be noted that these people were using others' credentials to complete a given work. These "shadow" work processes are potentially demoralising to staff, in addition to also creating a security weakness. This is a key area for improvement that requires further understanding of the organisational culture which has led to the existence of these shadow behaviours. The current behaviours are engrained habits, which coexist with a practical rationalisation that they are required to enable patient care to be efficient. Without awareness of what constitutes unsafe/risky behaviour and the potential consequences, it is not realistic to expect staff to behave securely. Furthermore, personnel have the feeling that security is something that is imposed upon them, with no explanation provided. They expressed a desire to be informed about why these behaviours were important, again feeding back into the need for great guidance and training.

As many healthcare organisations have not yet experienced a major cybersecurity breach, there is a lack of learned experience. This means that staff may not be aware of their vulnerability to be attacked, particularly as they have potentially been acting insecurely for a long period of time without any noticeable negative consequences. Therefore, staff does not necessarily understand why there is any need to change their current behaviour. This again ties to the need to raise awareness in an effective manner.

Healthcare professionals work within a very fast-paced, unique and potentially stressful environment, with a lot of time pressures and responsibilities that do not always facilitate secure behaviour. Many of the unsecure behaviours are driven by a need for procedures to be quick and convenient for staff – particularly when patient care (and potentially lives) can depend upon staff acting quickly. For example, in some healthcare environments it is not possible for technology to impose certain security behaviours, such as auto log-off, nor it is feasible for staff to have to take several steps to access one system.

In these environments, activities of dynamic risk assessment are fundamental in order to assess the status of a well-delimited environment and compute the level of risk the environment is exposed. Furthermore, this kind of control should foresee proposal of mitigation actions performed by a dedicated group in order to decrease

the risks. Parameters to be intended as indicators in order to detect the relevant countermeasures should be based on the minimum acceptable level of risk and the impact risk has on the business. On this aspect it is very important to monitor the activities related to the management, since it is detected as the most critical aspect.

Any interventions imposed must be user-friendly, user-transparent, time-efficient and unburdensome otherwise they will at best, be ineffective (e.g., promoting staff to find 'workarounds') or at worst, negatively impact upon patient care. A typical example is the sharing of information. Now, the exchange of information is inadequate to the scope: low level of protection and not intuitive communication tools push the staff to find workarounds for information sharing (e.g., use of WhatsApp). This is done both for communications that involves both HCO and patients and among tenants. About information sharing there are also limitation imposed by GDPR for the personal data management. For this reason, it is needed to generate an ad-hoc tool that can manage all these limitations and be user-friendly.

Other issues, such as the use of USB devices and sharing of attachments, may be more straightforward to - at least partially – be addressed from a technological perspective (e.g., screening of USB devices on machines that are isolated from the main hospital network). Security-by-design and identification and authentication systems are a way in order to address these issues by means of technology.

Security-by-design should drive the manifacturers along all the stages of production: requirement definition, design phase, implementation phase, testing and validation phase and maintenance phase. Hardening of products is one of the main issue for this topic. From what it is possible to infer from the risk scenarios, it is important that the medical devices and systems/softwares provided to healthcare organizations will be robust under the confidentiality point of view in order to avoid disclosure of data.

Also, identification and authentication results in limitating intrusion in HCO system. Only authenticated system/people are allowed to connect to the system, thus limiting intruders. Authentication is then to be used in order to implement the "need to know" principle: only the information needed for the normal develop of operations should be known. One of the main risk behaviours that emerged during activities was the tendency of staff to share login credentials with one another. This appeared to be largely driven by a discrepancy between the work tasks which are included within their official job description and responsibilities, and the tasks that they actually perform on a daily basis. This discrepancy should be addressed by an authentication mechanism and by appropriate training in order to minimise unsecure behaviours such as the sharing of login credentials.

Speaking about training, it is still important that staff is kept informed as to why any technological interventions are important. This will help to facilitate their adoption and continued use, and minimise perceptions of security as a barrier to productivity and another "hoop to jump through" for no perceived reward.

It is also vital that staff understands the potential for unintended consequences of increasing security measures. For example, if they impact negatively upon work and/or patient care. In order to facilitate positive and effective behaviour change, it is necessary to understand more about the factors that affect behaviour in the workplace (such as motivations and influencers).

On this principle, a cyber-security governance should be built. Cybersecurity governance should be developed by analysing the status and gaps in roles, procedures and policies and support the end users in defining these. During the work of producing this deliverable, it has been observed that, of particular importance is the definition of mapping between cyber-security roles in cyber incident management and/or general crisis management. This can be done by supporting an ad-hoc task force that reports directly to the CEO and manages processes in response to critical situations. Also, cyber-security governace should be defined within the HC organizations in order to produce continual improving of suitability, adequacy and effectiveness of information security management system.

Also methods for the value assessment of investment for cyber-security and implementation guidelines were addressed by PANACEA project. Value assessment should consider aspects, like depreciation of the investment, yearly budget allocated for cyber security, expected size of the cyberattacks, time to recover. First

of all, it is needed to point the minimum configuration on which an organization wants to operate. The adoption of cyber-security measures should then be built around this minimal configuration.

Finally, end users shall be assisted in analysis, installation and validation of the solution they choose. For this reason a tool able to assess existent security solutions already implemented by the organization and to understand how to integrate the PANACEA solution with the already existent tools is needed. This tool will provide procedures and manuals about how operate the solution and all the other documentation specified by applicable regulatory requirements. Furthermore, solution should be tested before taking effect.

Annex A
Questionnaires
1st END-USERS/STAKEHOLDERS WORKSHOP

Dynamic Risk Assessment

Definition

The protection of the IT infrastructure underlying the HCO business processes is vital nowadays.

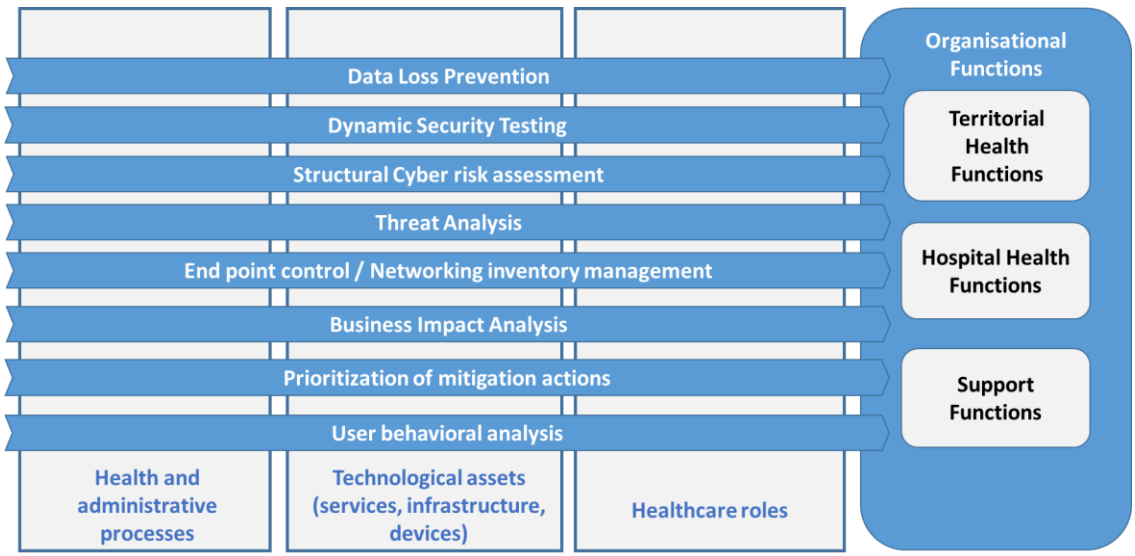
Attacks such as Wannacry could have been better managed with a dynamic risk management system monitoring the risk level on real time.

PANACEA aims at developing such a system, able to consider all possible attack path given by known vulnerabilities and suggest mitigation actions based on risk analysis.

In addition, the human factor will be taken into consideration: another layer of attack paths based on misbehaviour of HCO personnel or patients will be computed and considered during the risk analysis.

Objectives of the topic session

- Understanding the need of such a system from a stakeholder perspective
- Understanding the best scope and boundaries of such a system
- Understanding possible scenarios where such a system could be applied
- Understanding additional technical details and features of the system
- Understanding the key actors for such a functionality in HCO and information system suppliers and how it might be grouped, e.g. according to level of responsibility, role, health sector context, etc.
- Information on previous tools/knowledge/experience and any common/local policy or standards that will apply to the dynamic risk management



Question 1	**Given the following functions contributing to the Dynamic risk assessment process, which of them are covered in your organization/devices?**					
	Data loss prevention: *Detection and prevention of possible violations of corporate policies related to the usage, storage and transmission of sensitive data*	Y	N			
	Dynamic Security Testing: *Periodic identification of possible application vulnerabilities (e.g., vulnerability assessment or penetration testing over the IT infrastructure).*	Y	N			
	Structural cyber risk assessment (una tantum or regularly performed): *Risk assessment is used to identify, estimate, and prioritize risks resulting from the operation and use of information systems and possible impacting (i) organizational operations (i.e., mission, functions, image, and reputation), (ii) organizational assets, (iii) individuals, (iv) other organizations and the Nation.*	Y	N			
	Threat analysis: *Dynamic or static threat analysis where 'dynamic threat analysis' refers to the usage of tools or methodologies to dynamically evaluate the threat landscape or possible attack scenarios, while 'static threat analysis' refers to a more traditional modelling of possible threats for the organization (e.g., as it is done in the context of a cyber risk assessment).*	Y	N			
	Endpoint control/Network Inventory management: *Identification and/or management of devices in the IT infrastructure e.g., identify and list in an inventory devices connected via TCP/IP by running Network Management System tools.*	Y	N			
	Business Impact Analysis: *A Business Impact Analysis (BIA) is a systematic process aiming at determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, incident or emergency*	Y	N			
	Prioritization of mitigation actions: *Mitigation actions are usually implemented as a risk treatment measure or as response to an incident detection (e.g., patching, changing firewall rules). Mitigation actions have usually a cost and an impact over the business processes of the company which may be useful in order to prioritize them in combination with the related risk reduction.*	Y	N			
	User behavioral analysis: *Analyssis done to gain useful information to spot suspicious patterns in user access requests/usage of IT resources.*	Y	N			
Question 2	**Given the list of functions listed in Question 1, do you notice relevant functions that are missing?**	Y	N			
Question 3	**How much each funcytion needs , in your opinion, to be improved in your company? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**					
	Data loss prevention: *Detection and prevention of possible violations of corporate policies related to the usage, storage and transmission of sensitive data*	1	2	3	4	5
	Dynamic Security Testing: *Periodic identification of possible application vulnerabilities (e.g., vulnerability assessment or penetration testing over the IT infrastructure).*	1	2	3	4	5
	Structural cyber risk assessment (una tantum or regularly performed): *Risk assessment is used to identify, estimate, and prioritize risks resulting from the operation and use of information systems and possible impacting (i) organizational operations (i.e., mission, functions, image, and reputation), (ii) organizational assets, (iii) individuals, (iv) other organizations and the Nation.*	1	2	3	4	5
	Threat analysis: *Dynamic or static threat analysis where 'dynamic threat analysis' refers to the usage of tools or methodologies to dynamically evaluate the threat landscape or possible attack scenarios, while 'static threat analysis' refers to a more traditional modelling of possible threats for the organization (e.g., as it is done in the context of a cyber risk assessment).*	1	2	3	4	5
	Endpoint control/Network Inventory management: *Identification and/or management of devices in the IT infrastructure e.g., identify and list in an inventory devices connected via TCP/IP by running Network Management System tools.*	1	2	3	4	5
	Business Impact Analysis: *A Business Impact Analysis (BIA) is a systematic process aiming at determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, incident or emergency*	1	2	3	4	5
	Prioritization of mitigation actions: *Mitigation actions are usually implemented as a risk treatment measure or as response to an incident detection (e.g., patching, changing firewall rules). Mitigation actions have usually a cost and an impact over the business processes of the company which may be useful in order to prioritize them in combination with the related risk reduction.*	1	2	3	4	5
	User behavioral analysis: *Analyssis done to gain useful information to spot suspicious patterns in user access requests/usage of IT resources.*	1	2	3	4	5

Question 4	**What is your feeling of the importance of each function, in terms of its contribution to reduce the vulnerability of the organization/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Data loss prevention: *Detection and prevention of possible violations of corporate policies related to the usage, storage and transmission of sensitive data*	1	2	3	4	5
	Dynamic Security Testing: *Periodic identification of possible application vulnerabilities (e.g., vulnerability assessment or penetration testing over the IT infrastructure).*	1	2	3	4	5
	Structural cyber risk assessment (una tantum or regularly performed): *Risk assessment is used to identify, estimate, and prioritize risks resulting from the operation and use of information systems and possible impacting (i) organizational operations (i.e., mission, functions, image, and reputation), (ii) organizational assets, (iii) individuals, (iv) other organizations and the Nation.*	1	2	3	4	5
	Threat analysis: *Dynamic or static threat analysis where 'dynamic threat analysis' refers to the usage of tools or methodologies to dynamically evaluate the threat landscape or possible attack scenarios, while 'static threat analysis' refers to a more traditional modelling of possible threats for the organization (e.g., as it is done in the context of a cyber risk assessment).*	1	2	3	4	5
	Endpoint control/Network Inventory management: *Identification and/or management of devices in the IT infrastructure e.g., identify and list in an inventory devices connected via TCP/IP by running Network Management System tools.*	1	2	3	4	5
	Business Impact Analysis: *A Business Impact Analysis (BIA) is a systematic process aiming at determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, incident or emergency*	1	2	3	4	5
	Prioritization of mitigation actions: *Mitigation actions are usually implemented as a risk treatment measure or as response to an incident detection (e.g., patching, changing firewall rules). Mitigation actions have usually a cost and an impact over the business processes of the company which may be useful in order to prioritize them in combination with the related risk reduction.*	1	2	3	4	5
	User behavioral analysis: *Analyssis done to gain useful information to spot suspicious patterns in user access requests/usage of IT resources.*	1	2	3	4	5

Question 5	**On which parts of the technological assets should a dynamic risk assessment tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Applications and Data					
	Clinical services, including	1	2	3	4	5
	Radiology					
	Laboratory					
	Operating room					
	Speciality					
	Patient administration					
	Clinical trials management					
	Hospital Pharmacy Management					
	Territorial Pharmacy Management					
	Territorial medical and operational services					
	Emergency pre-hospital services					
	Remote clinical services					
	Internet accessible services, including	1	2	3	4	5
	Corporate e-mail					
	Web Portal					
	Apps for patients					
	Apps for suppliers					
	Apps for internal staff					
	Corporate services, including	1	2	3	4	5
	Staff management					
	Accounting					
	Procurement					
	Services for staff					
	Facility management services, including	1	2	3	4	5
	Domotics					
	Building and facilities management					
	Infrastructure services, including	1	2	3	4	5
	Data Centre and Networking applications (e.g. Monitoring systems, patching delivery systems, VPN)					
	Devices and Infrastructure					
	Networked medical devices, including	1	2	3	4	5
	Mobile devices					
	Wearable external devices					
	Implantable devices					
	Stationary devices					
	Supportive devices					
	Identification devices, including	1	2	3	4	5
	Patient identification devices					
	Staff identification devices					
	Access devices, including	1	2	3	4	5
	Company-owned access devices					
	Employee-owned access devices (BYOD)					
	Infrastructure, including	1	2	3	4	5
	Data Centre and Networking devices (e.g. Server, Switch, Router)					
	Networks (e.g. Wired LAN network, wireless LAN network, BLE)					

Question 6	**On which types of networked Medical Devices should a dynamic risk assessment tool be focused in a HCO (assuming that they are connected via TCP/IP-Transmission Control Protocol/Internet Protocol to the HCO IT infrastructure)? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5

Question 7	**A dynamic risk assessent tool can improve the proactive protection of the IT infrastructure underlying different processes in a HCO. Which of these processes should the tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Health Processes					
	Hospital workflows	1	2	3	4	5
	Inter-hospital medical consultations	1	2	3	4	5
	Territorial workflows	1	2	3	4	5
	Cross-border exchange of patient related data	1	2	3	4	5
	Emergency pre-hospital workflows	1	2	3	4	5
	Administrative/Technical processes					
	Patient billing	1	2	3	4	5
	Centralized processes	1	2	3	4	5
	In-Hospital processes	1	2	3	4	5

Question 8	**A dynamic risk assessent tool can improve the proactive protection of the IT infrastructure underlying different organizational functions in a HCO. Which of these organizational functions should a dynamic risk assessment tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	1. Territorial health functions					
	1.1. Prevention	1	2	3	4	5
	1.2. Diagnosis	1	2	3	4	5
	1.3. Assistance	1	2	3	4	5
	1.4. Emergency	1	2	3	4	5
	1.5. Legal and tax medicine	1	2	3	4	5
	1.6. Drug pharmaceutics	1	2	3	4	5
	1.10. Other territorial functions	1	2	3	4	5
	2. Hospital health functions					
	2.1. Emergency	1	2	3	4	5
	2.2. Anaesthesia	1	2	3	4	5
	2.3. Intensive therapy	1	2	3	4	5
	2.4. Surgery	1	2	3	4	5
	2.5. Medicine	1	2	3	4	5
	2.6. Rehabilitation	1	2	3	4	5
	2.7. Diagnostic services	1	2	3	4	5
	2.8. Histopathology	1	2	3	4	5
	2.9. Outpatient Clinics	1	2	3	4	5
	2.10 Drug pharmaceutics	1	2	3	4	5
	2.11.Blood banks	1	2	3	4	5
	2.12.Ethical Committee	1	2	3	4	5
	2.13.Other hospital functions	1	2	3	4	5
	3. Support functions					
	3.1.Operation Support functions	1	2	3	4	5
	3.2. Administrative support functions	1	2	3	4	5

Question 9	**Assuming that a dynamic risk assessment tool would be able to compute the cyber risk due to bad human behavior, which work roles should be considered in the compuation, in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	External roles					
	Patients	1	2	3	4	5
	Suppliers	1	2	3	4	5

Question 10	**Which of the following features of a Dynamic Risk Assessment tool are important for you? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Provision of local views related to specific areas (e.g., departments, sectors of the IT infrastructure) of you organization	1	2	3	4	5
	Full proactive risk management features focusing on the critical assets encompassed in the IT network (data storage, etc..) and its interaction with human operators	1	2	3	4	5
	The system proposes mitigation actions with associated information of their impact on the business continuity	1	2	3	4	5
	The system proposes a priority ranking of the mitigation actions	1	2	3	4	5
	The system considers the interaction between operators and ICT Infrastructure in the risk analysis	1	2	3	4	5
	The system recommends remediation actions also regarding people and organization	1	2	3	4	5
	Other	1	2	3	4	5

Question 11	**Consideting the following features of a Dynamic Risk Assessment tool, which is the desired level of complexity of the visual system that manage them? (1: Static overview; 2: Static detailed view; 3: Basic analytics; 4: Simple analytics environment; 5: Complex analytics environment)**					
	Provision of local views related to specific areas (e.g., departments, sectors of the IT infrastructure) of you organization	1	2	3	4	5
	Full proactive risk management features focusing on the critical assets encompassed in the IT network (data storage, etc..) and its interaction with human operators	1	2	3	4	5
	The system proposes mitigation actions with associated information of their impact on the business continuity	1	2	3	4	5
	The system proposes a priority ranking of the mitigation actions	1	2	3	4	5
	The system considers the interaction between operators and ICT Infrastructure in the risk analysis	1	2	3	4	5
	The system recommends remediation actions also regarding people and organization	1	2	3	4	5
	Other	1	2	3	4	5

Question 12	**Based on you experience, HCO context normally …**		
	Have documentation depicting the Organizational Structure of the HCOs	Y	N
	Have already performed at least one cyber threat and risk assessment	Y	N
	Currently perform Business Impact analysis	Y	N
	Have an internal IT department	Y	N
	Managein a centralized manner the Cybersecurity related aspects (e.g., installation of a new device, credentials management)	Y	N
	Manage a continuously updated Network Map of the IT infrastructure	Y	N
	Manage a continuously updated Configuration Management Data Base (CMDB)	Y	N
	Have an n IT infrastructure directly connected to the ICS/SCADA (Industrial Control System/Supervisory Control And Data Acquisition) systems managing the machinery of the hospital (if any)	Y	N
	Have an IT network connected to the the ICS infrastructure (if any)	Y	N
	Have an IT department actively monitoring the IT infrastructure with monitoring software (Assets Management Systems, Network Management Systems, IDS, IPS, SIEM, etc.)	Y	N
	Monitor fearly well the IT infrastructure with respect to cybersecurity.	Y	N
	Ensure adequate protection of the sensitive data managed in the organization	Y	N
	Use authentication features sufficiently strong to protect data	Y	N
	Are well aware about the security tools used in the organization	Y	N
	Are aware about common vulnerabilities and threats connected to the usage of your IT infrastructure	Y	N
	Have policy regulating the connection of personal devices to ICT network or infrastructure	Y	N
	Are aware about common vulnerabilities and threats arising from cybersecurity policy violations	Y	N

Question 13	**Which are the parameters that you would like to be considered in the definition of a mitigation action? (e.g., risk reduction, data properties, etc)?**		
	Risk reduction	Y	N
	Data properties	Y	N
	Cost	Y	N
	Business impact	Y	N
	Other	Y	N

Secure Information Sharing

Definition

Information sharing describes the exchange of data between various organizations, people and technologies. There are several types of information sharing:

- Information shared by individuals
- Information shared by organizations
- Information shared between firmware/software

Objectives of the topic session

- Understanding the need from the stakeholders for such of a system (which healthcare data is interesting to share and with who?)
- Understanding where it would be more useful (single organization with single premise, single organization with multiple premises, single organization with multiple premises cross border, multiple organizations with different combinations)
- Understanding the key actors for information sharing in HCO and information system suppliers and how it might be grouped, e.g. according to level of responsibility, role, health sector context, etc.
- Information on previous tools/knowledge/experience and any common/local policy or standards that will apply to the information sharing system

Question 1	Given the "Secure Information Sharing functions", which of them are covered in your organization/devices?						
	Detection and prevention of violations to corporate policies regarding the use, storage, and transmission of sensitive data	Y	N				
	Encryption of data to ensure confidentiality when stolen	Y	N				
Question 2	Do you notice missing functions when sharing information? If YES, specify	Y	N				
Question 3	Which functions need to be improved?						
	Detection and prevention of violations to corporate policies regarding the use, storage, and transmission of sensitive data	Y	N				
	Encryption of data to ensure confidentiality when stolen	Y	N				
	Other functions:	Y	N				
Question 4	What is the importance of each function, in terms of its contribution to reduce the vulnerability of the organization/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)						
	Detection and prevention of violations to corporate policies regarding the use, storage, and transmission of sensitive data	1	2	3	4	5	
	Encryption of data to ensure confidentiality when stolen	1	2	3	4	5	
Question 5	Where do you see weaknesses in current approach in your organization (or in HCOs in general) to the Secure Information Sharing?						
	non compliance with legal requirements	Y	N				
	lack of active security storing and storing method	Y	N				
	lack of information sharing interoperability protocols	Y	N				
	lack of policies	Y	N				
	lack of procedures	Y	N				
	procedures are not user-friendly	Y	N				
	access to information is not recorded	Y	N				
	there are no means to identify senders and recipients of the information	Y	N				
	Other weaknessses:	Y	N				
Question 6	On which of the following situations you feel that there is the highest need to improve Secure Information Sharing? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)						
	Healthcare information sharing of the patients (data contained within Electronic Health Records) to be shared						
	Between different departments of the same Hospital or Health territorial unit	1	2	3	4	5	
	Between different Hospitals or Health territorial units of the same organization, located in the same country	1	2	3	4	5	
	Between different Hospitals or Health territorial units belonging to different organizations, located in the same country	1	2	3	4	5	
	Between different Hospitals or Health territorial units of the same organization, located different European countries	1	2	3	4	5	
	Between different Hospitals or Health territorial units belonging to different organizations, located in different European countries	1	2	3	4	5	
	Administrative details sharing of the patients or medical personnel (contact details, financial info, etc)						
	Between different departments of the same Hospital or Health territorial unit	1	2	3	4	5	
	Between different Hospitals or Health territorial units of the same organization, located in the same country	1	2	3	4	5	
	Between different Hospitals or Health territorial units belonging to different organizations, located in the same country	1	2	3	4	5	
	Between different Hospitals or Health territorial units of the same organization, located different European countries	1	2	3	4	5	
	Between different Hospitals or Health territorial units belonging to different organizations, located in different European countries	1	2	3	4	5	
	Share a common reference library of information among the tenants (laws, regulations, other)	1	2	3	4	5	

Question 7	On which applications should a Secure Information Sharing tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Clinical services					
	Radiology	1	2	3	4	5
	Laboratory	1	2	3	4	5
	Operating room	1	2	3	4	5
	Speciality	1	2	3	4	5
	Patient administration	1	2	3	4	5
	Clinical trials management	1	2	3	4	5
	Hospital Pharmacy Management	1	2	3	4	5
	Territorial Pharmacy Management	1	2	3	4	5
	Territorial medical and operational services	1	2	3	4	5
	Emergency pre-hospital services	1	2	3	4	5
	Remote clinical services	1	2	3	4	5
	Internet accessible services	1	2	3	4	5
	Corporate e-mail	1	2	3	4	5
	Portal	1	2	3	4	5
	Apps for patients	1	2	3	4	5
	Apps for suppliers	1	2	3	4	5
	Apps for internal staff	1	2	3	4	5
	Corporate services	1	2	3	4	5
	Staff management	1	2	3	4	5
	Accounting	1	2	3	4	5
	Procurement	1	2	3	4	5
	Services for staff	1	2	3	4	5
	Facility management services	1	2	3	4	5
	Domotics	1	2	3	4	5
	Building and facilities management	1	2	3	4	5

Question 8	On which types of data should a Secure Information Sharing tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Data for Management Reporting	1	2	3	4	5
	Data for Clinical reporting	1	2	3	4	5
	Document stored in the Document Management system	1	2	3	4	5
	Patients data	1	2	3	4	5
	Suppliers data	1	2	3	4	5
	Epidemiological data	1	2	3	4	5
	Clinical Trial data	1	2	3	4	5
	Configuration Management Data Base (CMDB) data	1	2	3	4	5
	Other					

Question 9	On which types of networked Medical Devices should a Secure Information Sharing tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g. Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5

Question 10	Which users (work roles) should be considered when developing the Secure Information Sharing tool? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	External roles					
	Patients	1	2	3	4	5
	Suppliers	1	2	3	4	5
Question 11	Blockchain could be considered to manage access rights: is this of interest to you?	Y	N			

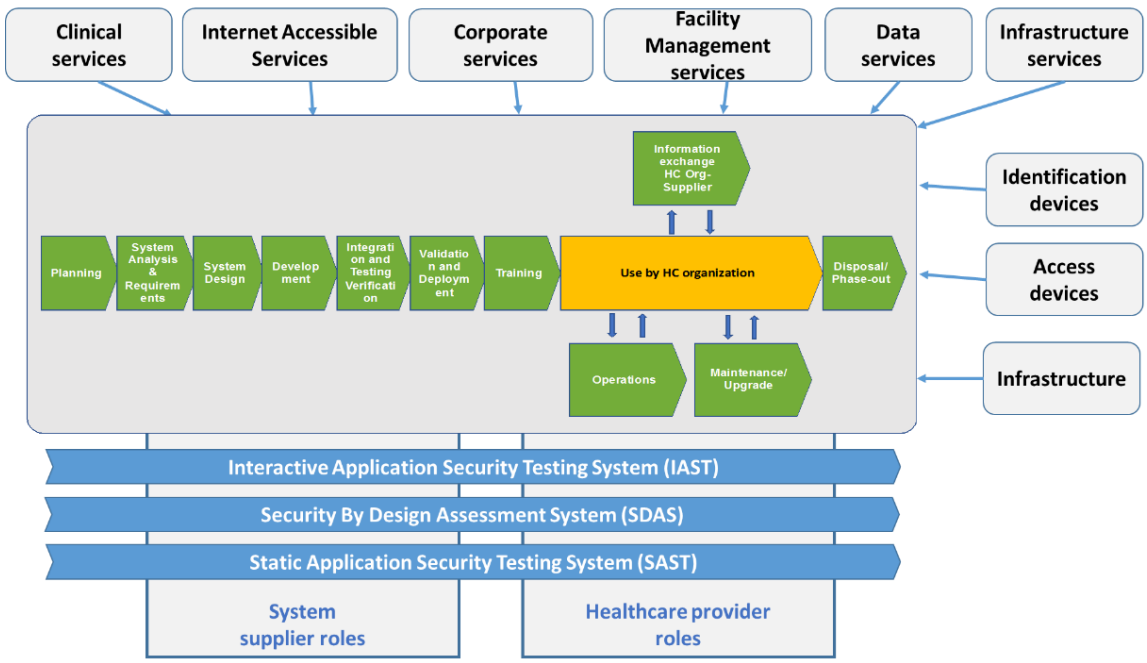
Security by Design (Information Systems)

Definition

Approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.

Objectives of the topic session

- Understanding the needs to cover cyber-security aspects during information system lifecycle
- Identification of the critical phases that are required of the information system lifecycle with regard to cyber-security
- Understanding the key actors in HCO and information system suppliers and how it might be grouped, e.g. according to level of responsibility, role, health sector context, etc.
- Information on previous knowledge/experience and any common/local policy or standards that will apply to the information system lifecycle



Question 1	**Given the "System Lifecycle Phases", which of them are covered in your organization?**						
	Planning	Y	N				
	System Analysis & Requirements	Y	N				
	System Design	Y	N				
	Development	Y	N				
	Integration and Testing verification	Y	N				
	Validation an deployment	Y	N				
	Training	Y	N				
	Operations	Y	N				
	Information Exchange HC organisation-supplier	Y	N				
	Maintenance / Upgrade	Y	N				
	Disposal /Phase Out	Y	N				
Question 2	**Considering the "Security by Design functions", which of them are covered in your organization?**						
	Interactive Application Security Testing System (IAST): *Instruments the application binary which can enable both "application security testing"-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process which provides significant benefits to DevOps approaches.*	Y	N				
	Security By Design Assessment System (SDAS): *Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.*	Y	N				
	Static Application Security Testing System (SAST): *Analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities.*	Y	N				
Question 3	**Do you notice missing functions?**	Y	N				
Question 4	Which functions need to be improved?						
	Interactive Application Security Testing System (IAST): *Instruments the application binary which can enable both "application security testing"-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process which provides significant benefits to DevOps approaches.*	Y	N				
	Security By Design Assessment System (SDAS): *Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.*	Y	N				
	Static Application Security Testing System (SAST): *Analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities.*	Y	N				
Question 5	**On which phases a security-by-design support tool should be focused?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**						
	Planning	1	2	3	4	5	
	System Analysis & Requirements	1	2	3	4	5	
	System Design	1	2	3	4	5	
	Development	1	2	3	4	5	
	Integration and Testing verification	1	2	3	4	5	
	Validation an deployment	1	2	3	4	5	
	Training	1	2	3	4	5	
	Operations	1	2	3	4	5	
	Information Exchange HC organisation-supplier	1	2	3	4	5	
	Maintenance / Upgrade	1	2	3	4	5	
	Disposal /Phase Out	1	2	3	4	5	
Question 6	**On which types of applications should a security-by-design support tool be focused in HCO?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**						
	Clinical services	1	2	3	4	5	
	Internet Accessible Services	1	2	3	4	5	
	Corporate services	1	2	3	4	5	
	Facility Management services	1	2	3	4	5	
	Data services	1	2	3	4	5	
	Infrastructure services	1	2	3	4	5	

Question 7	**On which types of Devices should a security-by-design support tool be focused in HCO?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Identification devices	1	2	3	4	5
	Access devices	1	2	3	4	5
	Infrastructure	1	2	3	4	5
Question 8	**Considering a system supplier, on which types of work roles should a security-by-design support tool be focused?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Software Developer	1	2	3	4	5
	Enterprise Architect	1	2	3	4	5
	Security Architect	1	2	3	4	5
	Research & Development Specialist	1	2	3	4	5
	Systems Requirements Planner	1	2	3	4	5
	System Testing and Evaluation Specialist	1	2	3	4	5
	Systems Developer	1	2	3	4	5
	Data Analyst	1	2	3	4	5
	Technical Support Specialist	1	2	3	4	5
	Network Operations Specialist	1	2	3	4	5
	Legal Advisor	1	2	3	4	5
	Privacy Officer/Privacy Compliance Manager	1	2	3	4	5
	Program Manager	1	2	3	4	5
	IT Project Manager	1	2	3	4	5
	Product Support Manager	1	2	3	4	5
	Product Instructor	1	2	3	4	5
	Product Instructional Curriculum Developer	1	2	3	4	5
Question 9	**Considering a HC organisation, on which types of work roles should a security-by-design support tool be focused?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Other Health roles					
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	Other non-health roles					
	External roles					
	Patients	1	2	3	4	5
Question 10	**Based on you experience, to ensure Security-by-design normally …**					
	is there a specific focus on security, during the life-cycle (dedicated reviews/milestones)?	Y	N			
	do you have specific tools to track and monitor security aspects related to systems supporting healthcare processes?	Y	N			
	do you track new vulnerabilities potentially affecting your systems supporting healthcare processes?	Y	N			
	do you assess new vulnerabilities potentially affecting your systems supporting healthcare processes?	Y	N			
	do you manage new vulnerabilities potentially affecting your medical devices or systems supporting healthcare processes?	Y	N			
	do you have a team dedicated to track and monitor security incidents related to systems supporting healthcare processes?	Y	N			

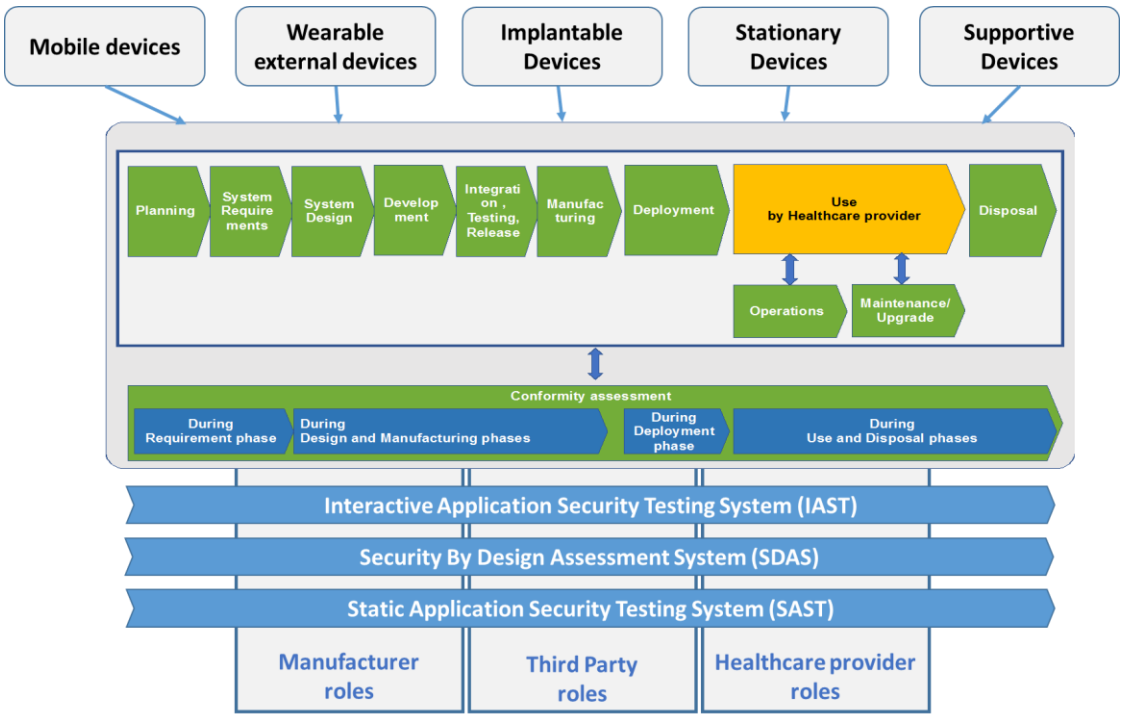
Security by Design (Medical Devices)

Definition

Approach to software and hardware development that seeks to make systems as free of vulnerabilities and impervious to attack as possible through such measures as continuous testing, authentication safeguards and adherence to best programming practices.

Objectives of the topic session

- Understanding the needs to cover cyber-security aspects during medical devices lifecycle
- Identification of the critical phases that are required of the medical devices lifecycle with regard to cyber-security
- Understanding the key actors in HCO and medical devices suppliers and how it might be grouped, e.g. according to level of responsibility, role, health sector context, etc.
- Information on previous knowledge/experience and any common/local policy or standards that will apply to the medical devices lifecycle



Question 1	**Given the "Device Lifecycle Phases" below, which of them are part of your device lifecycle?**						
	Conformity Assessment	Y	N				
	Planning	Y	N				
	System Analysis & Requirements	Y	N				
	System Design	Y	N				
	Development	Y	N				
	Integration, Testing, Release	Y	N				
	Manufacturing	Y	N				
	Deployment	Y	N				
	Operations	Y	N				
	Maintenance / Upgrade	Y	N				
	Disposal	Y	N				
Question 2	**Considering the "Security by Design functions", which of them are covered in your organization?**						
	Interactive Application Security Testing System (IAST): *Instruments the application binary which can enable both "application security testing"-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process which provides significant benefits to DevOps approaches.*	Y	N				
	Security By Design Assessment System (SDAS): *Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.*	Y	N				
	Static Application Security Testing System (SAST): *Analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities.*	Y	N				
Question 3	**Do you notice missing functions?**	**Y**	**N**				
Question 4	**Which functions need to be improved?**						
	Interactive Application Security Testing System (IAST): *Instruments the application binary which can enable both "application security testing"-like confirmation of exploit success and SAST-like coverage of the application code. In some cases, IAST allows security testing as part of general application testing process which provides significant benefits to DevOps approaches.*	Y	N				
	Security By Design Assessment System (SDAS): *Tool to support security engineering by assessing the applicability of security requirements on a software system that is still under development or already deployed.*	Y	N				
	Static Application Security Testing System (SAST): *Analyse application source code, byte code and binaries for coding and design conditions that are indicative of security vulnerabilities.*	Y	N				
Question 5	**On which phases a security-by-design support tool should be focused?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**						
	Conformity Assessment	1	2	3	4	5	
	Planning	1	2	3	4	5	
	System Analysis & Requirements	1	2	3	4	5	
	System Design	1	2	3	4	5	
	Development	1	2	3	4	5	
	Integration, Testing, Release	1	2	3	4	5	
	Manufacturing	1	2	3	4	5	
	Deployment	1	2	3	4	5	
	Operations	1	2	3	4	5	
	Maintenance / Upgrade	1	2	3	4	5	
	Disposal	1	2	3	4	5	
Question 6	**On which types of networked Medical Devices should a security-by-design support tool be focused in HCO?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**						
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5	
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5	
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5	
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5	
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5	

Question 7	**On which types of work roles should a security-by-design support tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Manufacturer					
	System architect	1	2	3	4	5
	Research & Development Specialist	1	2	3	4	5
	Hardware architect	1	2	3	4	5
	Software developer	1	2	3	4	5
	Legal advisor	1	2	3	4	5
	Maintenance staff	1	2	3	4	5
	Data analyst	1	2	3	4	5
	Conformity Responsible Person	1	2	3	4	5
	Third Party					
	Trust Service Provider	1	2	3	4	5
	Notified Body	1	2	3	4	5
	Healthcare provider					
	Specialist Medical Practitioners (e.g. Radiologist)	1	2	3	4	5
	Medical and Pharmaceutical Technicians (e.g. Medical Imaging Technicians)	1	2	3	4	5
	Nurses	1	2	3	4	5
	Patients	1	2	3	4	5
	Technical Roles (Device Dept. Engineer/Technician)	1	2	3	4	5
	Technical Roles (Medical Devices Surveillance Responsible Person)	1	2	3	4	5
Question 8	**Based on you experience, to ensure Security-by-design normally …**					
	is there a specific focus on security, during the life-cycle (dedicated reviews/milestones)?	Y	N			
	do you have specific tools to track and monitor security aspects related to medical devices?	Y	N			
	do you track new vulnerabilities potentially affecting your medical devices?	Y	N			
	do you assess new vulnerabilities potentially affecting your medical devices?	Y	N			
	do you manage new vulnerabilities potentially affecting your medical devices?	Y	N			
	do you have a team dedicated to track and monitor security incidents related to medical devices?	Y	N			

Identification and Authentication

Definition

Authentication ,also called "verification" is the capability to answer the following question:

- is this person who he or she claims to be ?
- Is this object what it claims to be ?

Authentication and identification functions refers to…

- Authenticating a user or object upon connection to a system (that can be complex)
- Making sure that during the whole time if his her or its connection it is still the same person or object
- Limiting and checking the rights of this user or object within the system she / he / it is connected to, and between users / objects (e.g. this doctor can enable the update of the firmware of this device type for these patients...)
- optionally securing the transactions and data exchanged between the connected user or object, and the system it is connected to.

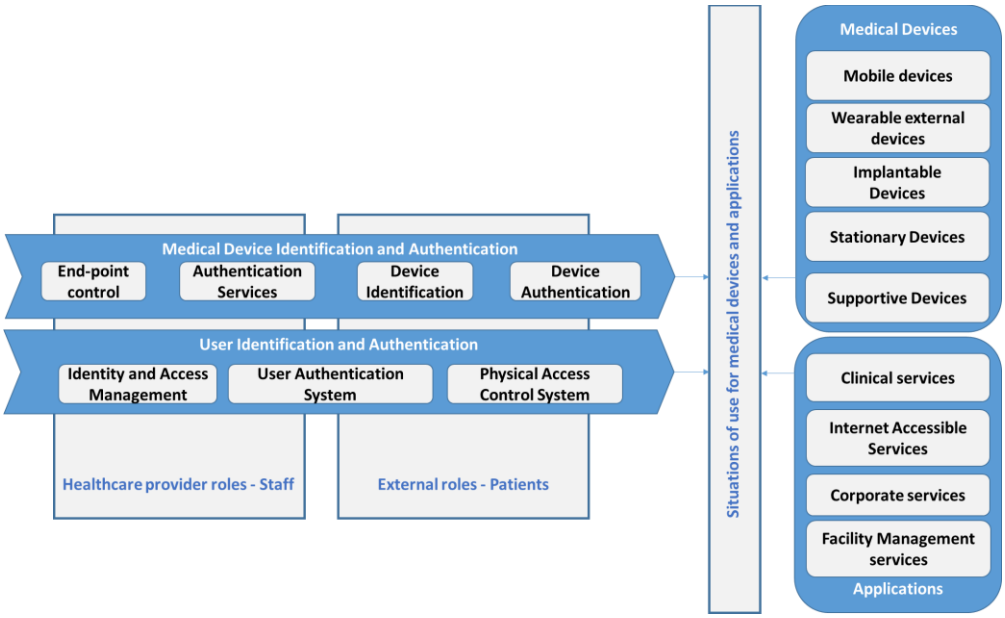
Also, the Identity and authentication management shall take care of defining which users and objects can connect to the system (e.g. add or delete user, recognize an object that is trying to connect...) and modify his, her or its rights (this can be done by administrator but also by other users)

Objectives of the topic session

In order to collect the requirements, we go through a matrix crossing **seven Identification and Authentication functions** with the two broad types of "objects" to be identified and authenticated: Medical Devices and Users.

We also consider that different solutions may be required depending on

- the work role of the user
- the type of application a user interacts
- the type of medical device a user interacts
- the situation related to how a medical device is used (e.g. the same medical device may connect to multiple hospital systems, medical devices are directly talking to each other).


Medical Device Identification and Authentication
End-point control
Authentication Services
Device Identification
Device Authentication
User Identification and Authentication
Identity and Access Management
User Authentication System
Physical Access Control System
Healthcare provider roles - Staff
External roles - Patients
Situations of use for medical devices and applications
Medical Devices
Mobile devices
Wearable external devices
Implantable Devices
Stationary Devices
Supportive Devices
Clinical services
Internet Accessible Services
Corporate services
Facility Management services
Applications

Question 1	Given the "Identification and Authentication functions", applied to a systm which is the IT system of the hospital, which of them are covered in your organization/devices?					
	Medical Device Identification and Authentication					
	Endpoint control *Detection of devices at the point of connection, e.g. USB devices, network plugin*	Y	N			
	Authentication services *Provision authentication for connected devices*	Y	N			
	Device identification *Provision the identification of devices as they are connecting to the network, Multiple levels of trust can apply*	Y	N			
	Device authentication *After device identification, the device authentication applies trust rules to provide authentication levels that govern device accessibility within the cyber-infrastructure*	Y	N			
	User Identification and Authentication for all types of users, but comment as necessary in case of restriction.	Y	N			
	Identity and access management (IAM) *IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.*	Y	N			
	User authentication system *System that authenticates users based on e.g. identiy card, physical attributes or pin code*	Y	N			
	Physical access control system *System that relies on the user authentication system to accept or deny physical access requests (e.g. door, gate, etc)*	Y	N			
Question 2	Do you notice missing functions?	Y	N			
Question 3	Which functions need to be improved?					
	Medical Device Identification and Authentication	Y	N			
	Endpoint control *Detection of devices at the point of connection, e.g. USB devices, network plugin*	Y	N			
	Authentication services *Provision authentication for connected devices*	Y	N			
	Device identification *Provision the identification of devices as they are connecting to the network, Multiple levels as trust can apply*	Y	N			
	Device authentication *After device identification, the device authentication applies trust rules to provide authentication levels that govern device accessibility within the cyber-infrastructure*	Y	N			
	User Identification and Authentication for all types of users.	Y	N			
	Identity and access management (IAM) *IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.*	Y	N			
	User authentication system *System that authenticates users based on e.g. identiy card, physical attributes or pin code*	Y	N			
	Physical access control system *System that relies on the user authentication system to accept or deny physical access requests (e.g. door, gate, etc)*	Y	N			
Question 4	What is the importance of each function, in terms of its contribution to reduce the vulnerability of the organization/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)					
	Medical Device Identification and Authentication					
	Endpoint control *Detection of devices at the point of connection, e.g. USB devices, network plugin*	1	2	3	4	5
	Authentication services *Provision authentication for connected devices*	1	2	3	4	5
	Device identification *Provision the identification of devices as they are connecting to the network, Multiple levels as trust can apply*	1	2	3	4	5
	Device authentication *After device identification, the device authentication applies trust rules to provide authentication levels that govern device accessibility within the cyber-infrastructure*	1	2	3	4	5
	User Identification and Authentication for all types of users, but comment as necessary in case of restriction.					
	Identity and access management (IAM) *IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments, and to meet increasingly rigorous compliance requirements.*	1	2	3	4	5
	User authentication system *System that authenticates users based on e.g. identiy card, physical attributes or pin code*	1	2	3	4	5
	Physical access control system *System that relies on the user authentication system to accept or deny physical access requests (e.g. door, gate, etc)*	1	2	3	4	5

Question 5	On which applications should a user Identification and Authentification tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority) (the tool would be generic, aplicable to any kind of user: please comment if you would like to see restrictions)					
	Clinical services					
	Radiology	1	2	3	4	5
	Laboratory	1	2	3	4	5
	Operating room	1	2	3	4	5
	Speciality	1	2	3	4	5
	Patient administration	1	2	3	4	5
	Clinical trials management	1	2	3	4	5
	Hospital Pharmacy Management	1	2	3	4	5
	Territorial Pharmacy Management	1	2	3	4	5
	Territorial medical and operational services	1	2	3	4	5
	Emergency pre-hospital services	1	2	3	4	5
	Remote clinical services	1	2	3	4	5
	Internet accessible services	1	2	3	4	5
	Corporate e-mail	1	2	3	4	5
	Portal	1	2	3	4	5
	Apps for patients	1	2	3	4	5
	Apps for suppliers	1	2	3	4	5
	Apps for internal staff	1	2	3	4	5
	Corporate services	1	2	3	4	5
	Staff management	1	2	3	4	5
	Accounting	1	2	3	4	5
	Procurement	1	2	3	4	5
	Services for staff	1	2	3	4	5
	Facility management services	1	2	3	4	5
	Domotics	1	2	3	4	5
	Building and facilities management	1	2	3	4	5
Question 6	On which types of networked Medical Devices should a Medical Device Identification and Authentication tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
Question 7	On which types of work roles should a user Identification and Authentication tool be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	External roles					
	Patients	1	2	3	4	5
	Suppliers	1	2	3	4	5

Question 8	What is the frequency of following situations? (1: Very low frequency; 2: Low frequency; 3: Medium frequency; 4: High frequency; 5: Very High frequency)					
	The same medical device may connect to multiple hospital systems					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
	Medical devices are directly talking to each other					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
	Medical devices are permanently to the IT system					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
	Medical Devices are permanently controlled during their use in hospital					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
Question 9	What is the frequency of following situations? (1: Very low frequency; 2: Low frequency; 3: Medium frequency; 4: High frequency; 5: Very High frequency)					
	Patients prefer more secure authentication even if authenticating is less simple	1	2	3	4	5
	Patient connect to multiple hospitals	1	2	3	4	5
	Patients connect from home for following devices, instead of coming to the hospital					
	Mobile devices (e.g. Portable ultrasound devices)	1	2	3	4	5
	Wearable external devices (e.g. Wireless temperature counter)	1	2	3	4	5
	Implantable devices (e.g.Cardiac pacemaker)	1	2	3	4	5
	Supportive devices (e.g. Assistive robot)	1	2	3	4	5
Question 10	What is the frequency of following situations? (1: Very low frequency; 2: Low frequency; 3: Medium frequency; 4: High frequency; 5: Very High frequency)					
	Staff working in emergency situation, in the tradeoff between cybersecurity and operational convenience prefer operational convenience					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5

Question 11	Which of the following features of an Identification and Authentication tool are important for you? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)					
	Capability to manage the transfer of rights from one person to another on connected object (e.g. I am doctor Anna and I transfer to right to doctor Ahmed to operate the connected object of Ms. Alice)	1	2	3	4	5
	Capability to managed the identification between hospital and the first aid services (firefighter, ambulance …)	1	2	3	4	5
	Is it important that doctors / nurses who are using multiple "IT things" have different control, depending on situation. (If I am a nurse and I have to use the patient health record and the pharmacy system and access to the scanner output and send messages to other nurses and doctors, I do this in different ways (e.g. with a badge for one, a password for the second one, a retinal scan for the 3rd etc.)	1	2	3	4	5
	Other					
Question 12	Are networked Medical Devices always associated clearly and without error to the patient they are taking care of ?					
	Mobile devices (e.g. Portable ultrasound devices)	Y	N			
	Wearable external devices (e.g. Wireless temperature counter)	Y	N			
	Implantable devices (e.g.Cardiac pacemaker)	Y	N			
	Stationary (e.g. High Automation Laboratory System, Computer Tomography scanner, Chemotherapy dispensing station)	Y	N			
	Supportive devices (e.g. Assistive robot)	Y	N			

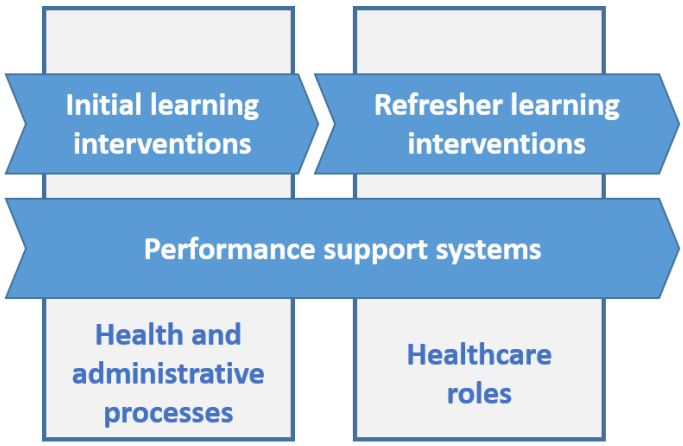
Training

Definition

Organized activity aimed at imparting information and/or instructions to improve the recipient's performance or to help him or her attain a required level of knowledge or skill.

Objectives of the topic session

- Understanding the scope, methods and tools for training in cybersecurity
- Understanding the target group in HCO and how it might be grouped, e.g. according to level of responsibility, role, health sector context, etc.
- Identification of the critical behaviours that are required of the target audience with regard to cyber-security
- Information on previous knowledge/experience and any common/local policy or standards that will apply to the training content



Question 1	**Given "Training and/or education packages for cybersecurity" measures, which of them are covered in your organization?**					
	Initial learning interventions: *Learning content, assessments and delivery methods designed specifically for each target audience (may include online learning)*	Y	N			
	Refresher learning interventions: *Delivered periodically, based on analysis of knowledge and skill fade, following initial learning intervention (likely to include online learning)*	Y	N			
	Performance support systems: *Support mechanisms in the workplace which routinely remind and guide on cyber-security threats and processes*	Y	N			
Question 2	**Do you notice missing measures?**	Y	N			
Question 3	**Which measures need to be improved in your organisation?**					
	Initial learning interventions: *Learning content, assessments and delivery methods designed specifically for each target audience (may include online learning)*	Y	N			
	Refresher learning interventions: *Delivered periodically, based on analysis of knowledge and skill fade, following initial learning intervention (likely to include online learning)*	Y	N			
	Performance support systems: *Support mechanisms in the workplace which routinely remind and guide on cyber-security threats and processes*	Y	N			
Question 4	**What is the importance of each function, in terms of its contribution to the development and maintenance of effective cyber-security behaviours in your organization?** **(1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Initial learning interventions: *Learning content, assessments and delivery methods designed specifically for each target audience (may include online learning)*	1	2	3	4	5
	Refresher learning interventions: *Delivered periodically, based on analysis of knowledge and skill fade, following initial learning intervention (likely to include online learning)*	1	2	3	4	5
	Performance support systems: *Support mechanisms in the workplace which routinely remind and guide on cyber-security threats and processes*	1	2	3	4	5
Question 5	**On which Health processes should a "Training and/or education packages for cybersecurity" be focused in a HCO?** **(1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Hospital workflows					
	Emergency department workflow	1	2	3	4	5
	Hospital admission	1	2	3	4	5
	Outpatient	1	2	3	4	5
	Clinical trial management	1	2	3	4	5
	Pharmaceutical workflows	1	2	3	4	5
	Medical management of wearable and implantable medical devices	1	2	3	4	5
	Inter-hospital medical consultations	1	2	3	4	5
	Territorial workflows					
	General Practitioner visit	1	2	3	4	5
	Centralized laboratory service	1	2	3	4	5
	Home care services	1	2	3	4	5
	Cross-border exchange of patient related data	1	2	3	4	5
	Emergency pre-hospital workflows					
	Emergency call and ambulance transportation	1	2	3	4	5

Question 6	**On which Administrative/Technical processes should a "Training and/or education packages for cybersecurity" be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Patient billing	1	2	3	4	5
	Human resources (not payroll)	1	2	3	4	5
	Human resources (payroll)	1	2	3	4	5
	Procurement	1	2	3	4	5
	Accounting	1	2	3	4	5
	Information and Communication Technology	1	2	3	4	5
	Facility management	1	2	3	4	5
	Critical infrastructure Incident management	1	2	3	4	5
Question 7	**On which types of work roles should a "Training and/or education packages for cybersecurity" be focused in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Other Health Roles					
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	Other Non-Health Roles					
	External roles					
	Patients	1	2	3	4	5
	Suppliers	1	2	3	4	5
Question 9	**Which of the following features of a "Training and/or education packages for cybersecurity" are important for you? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Traditional 'teaching'	1	2	3	4	5
	Hands-on	1	2	3	4	5
	Scenario-based learning / case studies	1	2	3	4	5
	Use of learning technologies (i.e. E-learning, performance support systems, virtual learning assistance, etc.)	1	2	3	4	5
	Support the transfer of learning into the workplace	1	2	3	4	5
	Training materials accessible before, during and after any training workshop	1	2	3	4	5
	Learning Management System	1	2	3	4	5
	Digital training materials to support learning, including gamification	1	2	3	4	5
Question 10	**What are the relevant standards applied in your organisation?**					
	common cyber-security policies/standards which relate to all European healthcare settings or specific groups of healthcare	Y	N			
	local/regional cyber-security policy standards	Y	N			
	cyber-security included in your staff competence framework, job descriptions or other role specification documents	Y	N			
Question 11	**Based on your personal experience, related to cybersecurity topics...**					
	do you have an internal team dedicated to perform training and learning?	Y	N			
	do you have external support for training and learning?	Y	N			

Governance

Definition

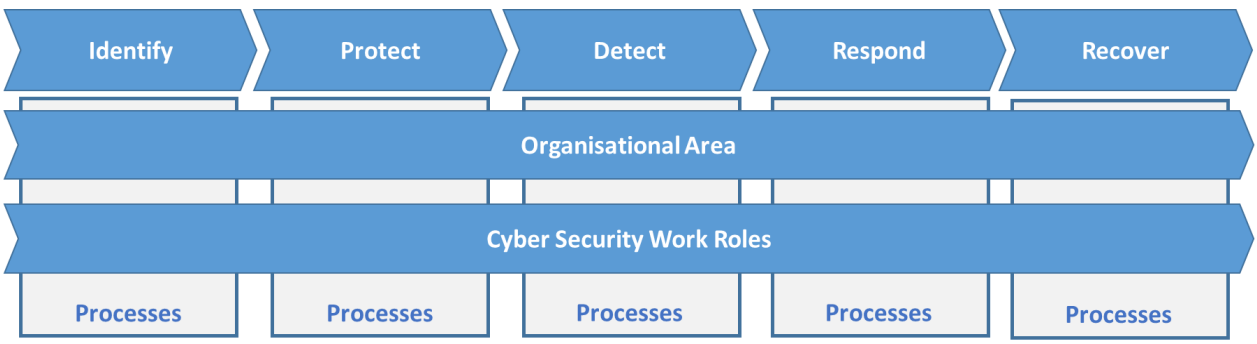
Governance is the set of organizational arrangements ensuring the capability to identify cyber risk, prevent cyber-attacks and detect cyber-attacks, recover after a cyber-attack.

The Governance arrangements can be described along two dimensions:

- the **five types of Cybersecurity processes**, corresponding to the five NIST Functions: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER
- the **key organizational elements allowing the governance**, i.e. allocation of responsibilities in the HCO structure, policies/procedures/plans, work roles.

Objectives of the topic session

- Understanding how much the Cybersecurity processes are mature in the HCOs and which of the are felt to be the most important in the in HCOs
- Understanding where the Cybersecurity responsibilities could fit in the HCO organization structures
- Understanding how much the work roles required by the Cybersecurity processes are present in the HCOs and which ones are felt to be the most important in the in HCOs



Question 1a	**IDENTIFY** processes consist in developing an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities: inventorying assets and vulnerabilities, measuring attack surface, risk profiling **In a HCO …**					
	Which organizational area should be the main responsible (R) for the Identification processes and which ones should contribute (C)					
	IT Department	R	C			
	Clinical direction	R	C			
	Clinical Engineering	R	C			
	Risk management fuction	R	C			
	Data Privacy Officer	R	C			
	A new ad-hoc function, reporting to the head of the HCO	R	C			
	Other					
Question 1b	**How much following processes need to be improved in the HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**	1	2	3	4	5
	Asset Management: The data, personnel, devices and systems and facilities required by the organisation are identified and managed in accordance with the organisation's business objectives and risk strategy	1	2	3	4	5
	Business Environment Assessment: The organisation's mission, objectives, activities and actors involved are understood and evaluated in terms of priorities. This information influences cybersecurity roles, responsibilities and cyber risk management.	1	2	3	4	5
	Governance: Cybersecurity policies and procedures shall be identified.	1	2	3	4	5
	Risk Assessment: The organisation understands the cyber risk inherent in the operations (including mission, functions, image or reputation), assets and individuals, including risks associated to the supply chain	1	2	3	4	5
	Risk Management Strategy definition: The organization's priorities and requirements and risk tolerance are defined and used to support cyber risk decisions. The scope of the strategy also include the supply chain	1	2	3	4	5
Question 1c	**What is your feeling of the importance of each process in terms of its contribution to reduce the vulnerability of the organization/systems/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Asset Management: The data, personnel, devices and systems and facilities required by the organisation are identified and managed in accordance with the organisation's business objectives and risk strategy	1	2	3	4	5
	Business Environment Assessment: The organisation's mission, objectives, activities and actors involved are understood and evaluated in terms of priorities. This information influences cybersecurity roles, responsibilities and cyber risk management.	1	2	3	4	5
	Governance: Cybersecurity policies and procedures shall be identified.	1	2	3	4	5
	Risk Assessment: The organisation understands the cyber risk inherent in the operations (including mission, functions, image or reputation), assets and individuals, including risks associated to the supply chain	1	2	3	4	5
	Risk Management Strategy definition: The organization's priorities and requirements and risk tolerance are defined and used to support cyber risk decisions. The scope of the strategy also include the supply chain	1	2	3	4	5

Question 2a	**PROTECT** processees consist in developing and implementin appropriate safeguards to ensure delivery of critical services: preventing or limiting impact, patching, containing, isolating, hardening, managing access, vulnerability remediation **In a HCO …**					
	Which organizational area should be the main responsible (R) for the Identification processes and which ones should contribute (C)					
	IT Department	R	C			
	Clinical direction	R	C			
	Clinical Engineering	R	C			
	Risk management fuction	R	C			
	Data Privacy Officer	R	C			
	A new ad-hoc function, reporting to the head of the HCO	R	C			
	Other					
Question 2b	**How much following processes need to be improved in the HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**	1	2	3	4	5
	Access Control: Access to cybersecurity assets and related resources is limited to personnel, processes, devices, activities and transactions actually authorized	1	2	3	4	5
	Awareness of cybercrime impact and Training: Personnel and third parties are educated and trained on cybersecurity and receive adequate preparation, consistent with policies, procedures and agreements.	1	2	3	4	5
	Data Security management and ensurance: Data is stored and managed in accordance with the organisation's cyber risk management strategy to ensure the integrity, confidentiality and availability of the information.	1	2	3	4	5
	Information Protection Processes and Procedures implementation: Cybersecurity policies are implemented and adapted over time (which address the purpose, scope, roles and responsibilities, commitment on the part of the management and coordination between the different parties)	1	2	3	4	5
	Maintenance of information control systems: Maintenance of information systems is carried out in accordance with existing policies and procedures	1	2	3	4	5
	Management of technical cybersecurity solutions: Technical cybersecurity solutions are managed to ensure the security and resilience of systems and assets, in accordance with the relevant policies, procedures and agreements.	1	2	3	4	5
Question 2c	**What is your feeling of the importance of each process in terms of its contribution to reduce the vulnerability of the organization/systems/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Access Control: Access to cybersecurity assets and related resources is limited to personnel, processes, devices, activities and transactions actually authorized	1	2	3	4	5
	Awareness of cybercrime impact and Training: Personnel and third parties are educated and trained on cybersecurity and receive adequate preparation, consistent with policies, procedures and agreements.	1	2	3	4	5
	Data Security management and ensurance: Data is stored and managed in accordance with the organisation's cyber risk management strategy to ensure the integrity, confidentiality and availability of the information.	1	2	3	4	5
	Information Protection Processes and Procedures implementation: Cybersecurity policies are implemented and adapted over time (which address the purpose, scope, roles and responsibilities, commitment on the part of the management and coordination between the different parties)	1	2	3	4	5
	Maintenance of information control systems: Maintenance of information systems is carried out in accordance with existing policies and procedures	1	2	3	4	5
	Management of technical cybersecurity solutions: Technical cybersecurity solutions are managed to ensure the security and resilience of systems and assets, in accordance with the relevant policies, procedures and agreements.	1	2	3	4	5

Question 3a	**DETECT** processes consist in developing and implementing appropriate activities to identify the occurrence of a cybersecurity event: discovering events, triggering on anomalies, hunting for intrusions, security analytics						
	Which organizational area should be the main responsible (R) for the Identification processes and which ones should contribute (C)						
	IT Department	R	C				
	Clinical direction	R	C				
	Clinical Engineering	R	C				
	Risk management fuction	R	C				
	Data Privacy Officer	R	C				
	A new ad-hoc function, reporting to the head of the HCO	R	C				
	Other						
Question 3b	**How much following processes need to be improved in the HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**	1	2	3	4	5	
	Anomalies and Events: Unexpected cyber activities are detected in a timely manner and their potential impact is analysed	1	2	3	4	5	
	Security Continuous Monitoring: Information systems and assets are periodically monitored to identify cybersecurity events and to verify the effectiveness of protection measures.	1	2	3	4	5	
	Detection Processes: Monitoring processes and procedures shall be adopted, maintained and verified over time to ensure a timely and adequate understanding of security events.	1	2	3	4	5	
Question 3c	**What is your feeling of the importance of each process in terms of its contribution to reduce the vulnerability of the organization/systems/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**						
	Anomalies and Events: Unexpected cyber activities are detected in a timely manner and their potential impact is analysed	1	2	3	4	5	
	Security Continuous Monitoring: Information systems and assets are periodically monitored to identify cybersecurity events and to verify the effectiveness of protection measures.	1	2	3	4	5	
	Detection Processes: Monitoring processes and procedures shall be adopted, maintained and verified over time to ensure a timely and adequate understanding of security events.	1	2	3	4	5	
Question 4a	**RESPOND** processes consist in developing and implementin appropriate activities to take action regarding a detected cybersecurity incident: acting on events, eradicating intrusion footholds, assessing damage, coordinating, reconstructing events forensically . **In a HCO …**						
	Which organizational area should be the main responsible (R) for the Identification processes and which ones should contribute (C)						
	IT Department	R	C				
	Clinical direction	R	C				
	Clinical Engineering	R	C				
	Risk management fuction	R	C				
	Data Privacy Officer	R	C				
	A new ad-hoc function, reporting to the head of the HCO	R	C				
	Other						
Question 4b	**How much following processes need to be improved in the HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**	1	2	3	4	5	
	Response Planning: Response procedures and processes are executed and maintained to ensure timely response to detected cybersecurity events.	1	2	3	4	5	
	Communications: Response procedures and processes are executed and maintained to ensure timely response to detected cybersecurity events.	1	2	3	4	5	
	Analysis: Analysis are conducted to ensure adequate response and support for recovery activities	1	2	3	4	5	
	Mitigation: Response activities are improved by incorporating lesson learned from previous monitoring and response activities	1	2	3	4	5	
	Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	1	2	3	4	5	
Question 4c	**What is your feeling of the importance of each process in terms of its contribution to reduce the vulnerability of the organization/systems/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**						
	Response Planning: Response procedures and processes are executed and maintained to ensure timely response to detected cybersecurity events.	1	2	3	4	5	
	Communications: Response procedures and processes are executed and maintained to ensure timely response to detected cybersecurity events.	1	2	3	4	5	
	Analysis: Analysis are conducted to ensure adequate response and support for recovery activities	1	2	3	4	5	
	Mitigation: Response activities are improved by incorporating lesson learned from previous monitoring and response activities	1	2	3	4	5	
	Improvements: Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	1	2	3	4	5	

Question 5a	**RECOVER** processees consist in developing and implementing appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident: returning to normal operations, restoring services, documenting lessons learned **In a HCO …**					
	which organizational area should be the main responsible (R) for the Identification processes and which ones should contribute (C)					
	IT Department	R	C			
	Clinical direction	R	C			
	Clinical Engineering	R	C			
	Risk management fuction	R	C			
	Data Privacy Officer	R	C			
	A new ad-hoc function, reporting to the head of the HCO	R	C			
	Other					
Question 5b	**How much following processes need to be improved in the HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very High need)**	1	2	3	4	5
	Recovery Planning: Restoration processes and procedures are executed and maintained to ensure timely recovery of systems or assets involved in a cybersecurity event	1	2	3	4	5
	Improvements: Organizational response activities, restoration plans and related processes have been improved taking into account lessons learned for future activities	1	2	3	4	5
	Communications: Incident recovery activities are coordinated with internal and external parties, such as victims, Internet Service Providers (ISPs), owners of attacked systems, vendors, Computer Emergency Response Team (CERT)/CSIRTs, etc	1	2	3	4	5
Question 5c	**What is your feeling of the importance of each process in terms of its contribution to reduce the vulnerability of the organization/systems/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Recovery Planning: Restoration processes and procedures are executed and maintained to ensure timely recovery of systems or assets involved in a cybersecurity event	1	2	3	4	5
	Improvements: Organizational response activities, restoration plans and related processes have been improved taking into account lessons learned for future activities	1	2	3	4	5
	Communications: Incident recovery activities are coordinated with internal and external parties, such as victims, Internet Service Providers (ISPs), owners of attacked systems, vendors, Computer Emergency Response Team (CERT)/CSIRTs, etc	1	2	3	4	5
Question 6	**How much following cybersecurity roles are, covered in the HCOs? (1: Very low coverage; 2: Low coverage; 3: Medium coverage; 4: High coverage; 5: Very High coverage)**					
	Security Provision (e.g. Security Architect, Information Systems Security Developer, Secure Software Assessor)	1	2	3	4	5
	Operate and Maintain (e.g. Systems Security Analyst, Network Operations Specialist, Data Analyst)	1	2	3	4	5
	Oversee and Govern (e.g. Privacy Compliance Manager, Cyber Training/Education/Awareness officer, Cyber Policy and Strategy Planner)	1	2	3	4	5
	Protect and Defend (e.g. Vulnerability Assessment Analyst, Cyber Defense Incident Responder)	1	2	3	4	5
	Analyze (e.g. Threat/Warning Analyst)	1	2	3	4	5
	Investigate (e.g. Cyber Crime Investigator)	1	2	3	4	5
Question 7	**How much following cybersecurity roles are, in your opinion, important in the HCOs, in terms of its contribution to reduce the vulnerability of the organization/devices? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**					
	Security Provision (e.g. Security Architect, Information Systems Security Developer, Secure Software Assessor)	1	2	3	4	5
	Operate and Maintain (e.g. Systems Security Analyst, Network Operations Specialist, Data Analyst)	1	2	3	4	5
	Oversee and Govern (e.g. Privacy Compliance Manager, Cyber Training/Education/Awareness officer, Cyber Policy and Strategy Planner)	1	2	3	4	5
	Protect and Defend (e.g. Vulnerability Assessment Analyst, Cyber Defense Incident Responder)	1	2	3	4	5
	Analyze (e.g. Threat/Warning Analyst)	1	2	3	4	5
	Investigate (e.g. Cyber Crime Investigator)	1	2	3	4	5

Nudging

Definition

Nudging is the set of interventions, in addition to the training, aimed at influencing the behaviours of the HCO staff and patients and other staff involved in the medical device and information systems lifecycle

Objectives of the topic session

In order to contextualize the nudging interventions, we aim at understanding:

- Which work roles In a HCO and along the Medical Device Lifecycle are more in need for nudging may depend
- Which of the typical situations where non-secure behaviours may happen (e.g. password sharing, clicking on links) apply to the healthcare environment
- Which of the typical influencing mechanisms (e.g. doing what a reputed person says) more apply to the healthcare environment
- Which are the barriers to secure behaviours
- How HCOs and Manufacturers organizations currently manage non-secure behaviours

Question 1	**On which types of work roles do we need to improve security behaviours along the Medical Device Lifecycle development? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	SYSTEM SUPPLIER SIDE					
	Software Developer	1	2	3	4	5
	Enterprise Architect	1	2	3	4	5
	Security Architect	1	2	3	4	5
	Research & Development Specialist	1	2	3	4	5
	Systems Requirements Planner	1	2	3	4	5
	System Testing and Evaluation Specialist	1	2	3	4	5
	Systems Developer	1	2	3	4	5
	Data Analyst	1	2	3	4	5
	Technical Support Specialist	1	2	3	4	5
	Network Operations Specialist	1	2	3	4	5
	Legal Advisor	1	2	3	4	5
	Privacy Officer/Privacy Compliance Manager	1	2	3	4	5
	Program Manager	1	2	3	4	5
	IT Project Manager	1	2	3	4	5
	Product Support Manager	1	2	3	4	5
	Product Instructor	1	2	3	4	5
	Product Instructional Curriculum Developer	1	2	3	4	5
	HCO SIDE					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Other Health roles	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	Other non-health roles	1	2	3	4	5
	External roles					
	Patients	1	2	3	4	5

Question 2	**On which types of work roles do we need to improve security behaviours in a HCO? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Managers					
	Health services Managers	1	2	3	4	5
	Health Roles					
	Generalist Medical Practitioners	1	2	3	4	5
	Specialist Medical Practitioners	1	2	3	4	5
	Nurses	1	2	3	4	5
	Paramedical practitioners	1	2	3	4	5
	Medical and Pharmaceutical Technicians	1	2	3	4	5
	Ambulance Workers	1	2	3	4	5
	Personal care workers in Health Services	1	2	3	4	5
	Non-health Roles					
	Technical roles	1	2	3	4	5
	Administrative back-office roles	1	2	3	4	5
	Administrative front-office roles	1	2	3	4	5
	Medical Secretaries	1	2	3	4	5
	Information and Communications Technology roles	1	2	3	4	5
	External roles					
	Patients	1	2	3	4	5
	Suppliers	1	2	3	4	5
Question 3	**Which of the following behaviours should be focussed on? (1: Very low priority; 2: Low priority; 3: Medium priority; 4: High priority; 5: Very High priority)**					
	Password creation	1	2	3	4	5
	Password sharing	1	2	3	4	5
	Phishing: Clicking on links in email	1	2	3	4	5
	Phishing: Opening document attachments from email	1	2	3	4	5
	Use of facebook or other social media in the workplace	1	2	3	4	5
	Use of USB devices	1	2	3	4	5
	Copying files to personal devices	1	2	3	4	5
	Sharing online files or information about patients between staff members	1	2	3	4	5
	Encryption of information on computers, when sending between people/organisations	1	2	3	4	5
	Logging out of shared workstations when you are not using it	1	2	3	4	5
	Backup of files	1	2	3	4	5
	Update of software up to date	1	2	3	4	5
	Ensure that antivirus and firewalls are active	1	2	3	4	5
	Oher					

Question 4	**Which types of infuencing mechanisms, in your opinion, are expected to have more impact on behaviours of staff in HCOs? (1: Very low imoact; 2: Low impact; 3: Medium impact; 4: High impact; 5: Very High impact)**					
	Messenger *We are influenced by the reputation of the person and/or method by which the message is delivered. What would be the impact of an influential person delivering the security message?*	1	2	3	4	5
	Do you have such a person in your organisation?	yes	no			
	Incentives *We are influenced by the rewards and punishments (losses) we receive. This includes our evaluation of the cost of behaving appropriately and the cost of the consequences if we do not. How impactful would appropriate rewards and punishments be?*	1	2	3	4	5
	Do you have rewards for security behaviours?	yes	no			
	Are sanctions in place if people do not follow your security policies?	yes	no			
	Relationships *We are influenced by the behaviors demonstrated by influencial others, such as senior managers, colleagues and family. How influential would the behaviours of other members of staff be?*	1	2	3	4	5
	Do senior staff lead by example with secure behaviours in your organisations	yes	no			
	In general do the majority of staff behave securely	yes	no			
	Defaults *We go with the flow of preset options. The default option will be chosen more often. Would it be impactful for the default options in your systems to be the most secure?*	1	2	3	4	5
	Affect *Our emotional associations influence our behavior. For example, initial emotions formed when visiting a new and unfamiliar shopping websites can influence whether or not a visitor to these sites will disclose information. Would it be impactful to ensure that staff have a positive attitude towards the hospital?*	1	2	3	4	5
	Commitments *We seek to be consistent with our public statements and reciprocate the acts of others. How impactful would it be to sign a public statement that you will always behave securely within the hospital?*	1	2	3	4	5
	Do staff currently sign an agreement to behave securely?	yes	no			
Question 5a (HCO)	**How much do you agree on following sentences? (1=I fully disagree, 5=I fully agree)**					
	The staff in HCOs believe that their behaviour can affect the security of the hospital systems and information	1	2	3	4	5
	The staff in HCOs behave and want to behave in a way that maximises cybersecurity	1	2	3	4	5
	There are behaviours, which are not in a policy, but staff in HCOs believe are needed for security (Eg workarounds they believe are secure)	1	2	3	4	5
Question 5b (HCO)	**What non-secure behaviours would you most like to see changed?**					
Question 5c (HCO)	**What do you think are the barriers to secure behaviours?**					
Question 5d (HCO)	**What do you think are the incentives to secure behaviours?**					
Question 5e (HCO)	**How do you ensure that staff are aware of how they should behave to maximise cybersecurity?**					
Question 5f (HCO)	**How do you measure if staff are behaving securely?**					
Question 6a (MD Lifecycle)	**How much do you agree on following sentences? (1=I fully disagree, 5=I fully agree)**					
	The staff involved in MD Lifecycle believe that their behaviour can affect the security of the hospital systems and information	1	2	3	4	5
	The staff involved in MD Lifecycle behave and want to behave in a way that maximises cybersecurity	1	2	3	4	5
	There are behaviours, which are not in a policy, but staff involved in MD Lifecycle believe are needed for security (Eg workarounds they believe are secure)	1	2	3	4	5
Question 6b (MD Lifecycle)	**What non-secure behaviours would you most like to see changed?**					
Question 6c (MD Lifecycle)	**What do you think are the barriers to secure behaviours?**					
Question 6d (MD Lifecycle)	**What do you think are the incentives to secure behaviours?**					
Question 6e (MD Lifecycle)	**How do you ensure that staff are aware of how they should behave to maximise cybersecurity?**					
Question 6f (MD Lifecycle)	**How do you measure if staff are behaving securely?**					

ROI methodology

Definition

ROI Methodology is a structured process for evaluating the return of investing in cybersecurity solutions (such as the PANACEA toolkit or parts of it). Its purpose is to support the HCO decision makers in taking the investment decision.

It considers both economic and non-economic returns.

Returns are evaluated in terms of **difference between two situations**:

- the investment is not done: this is named "WITHOUT case" and is the baseline situation
- the investment is done: this is named "WITH case".

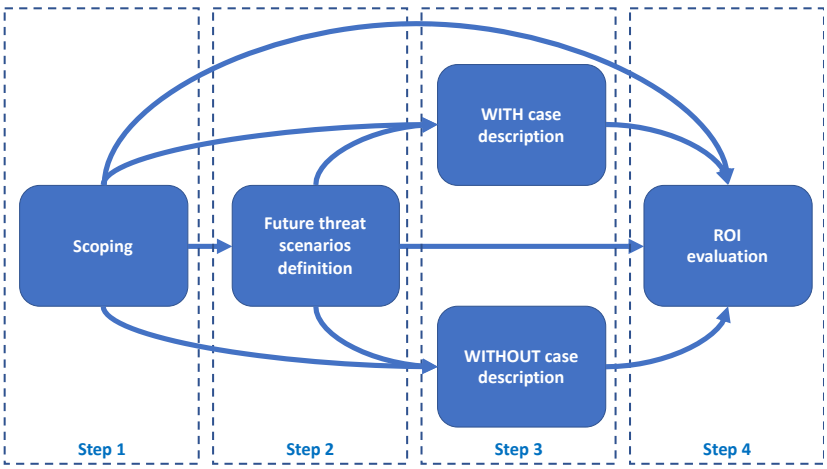
For instance, if we consider only the economic evaluation, the process builds two cashflows (WITH and WITHOUT) and makes the difference between them, building the differential cashflow. Then calculates indicators, such as the net present value.

Objectives of the topic session

In order to contextualize the nudging interventions, we have structured the process in four steps and we aim at understanding how to contextualize each one of them

The process may be articulated in **four steps**:

1) **Scoping**, to describe the investment and to state the time horizon, i.e. the number of years over which the investment is evaluated
2) **Future threat scenarios definition**, to make reasonable assumptions on the future possible attacks
3) **WITH and WITHOUT cases description**, to describe what happens in case of attack (and between attacks) in case the investment is done (WITH case) and in case investment is not done (WTHOUT case)
4) **ROI evaluation**, to elaborate indicators of the differences between the WITH and the WITHOUT cases.



Question 1	**Which elemets should be defined in the Scoping step? ?**						
	Tools of the Panacea Toolkit to be implemented	Y	N				
	Organizational scope (i.e. HCO roles/types of staff, processes, organizational functions/units)	Y	N				
	Technical assets (applications, networks, medical devices)	Y	N				
	Activities to be performed to do the investment	Y	N				
	Activities to be performed over the time horizon, to ensure the usabilty of the investment	Y	N				
	Existing assets to be modified/eliminated as a consequence of the investment	Y	N				
	Costs related to all above elemenents	Y	N				
	Other						
Question 2	**What is the typical time horizon over which cybersecurity investments are evaluated in your organization? (years)**						
Question 3	**What is the typical discount rate used to evaluate the investments in your organization? (%)**						
Question 4	**Which elemets should be defined in the Future threat scenarios definition step?**						
	Types of attacks	Y	N				
	Frequency of attacks per type (per year)	Y	N				
	Other						
Question 5	**Which elemets should be defined in the WITH and WITHOUT cases description steps?**						
	Activities done in non-attack situations (e.g. remediation activities)	Y	N				
	Response activities done when the attack happens	Y	N				
	Recovery activities done when the attack happens	Y	N				
	Probability of successful attack	Y	N				
	Impact on HCO operations	Y	N				
	Amount of tghe ransom	Y	N				
	Costs related to above activities	Y	N				
	Other related quantities, to estimate the return indicators (see Question 6)	Y	N				
	Other elements						
Question 6	**In the ROI evaluation step, which return indicators (i.e. which types of difference between WITH and WITHOUT cases) do you think are more important? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)**						
	Total differential cash flow	1	2	3	4	5	
	Total differential cash flow/investrment	1	2	3	4	5	
	Average differential response time	1	2	3	4	5	
	Average differential recovery time	1	2	3	4	5	
	Average differential impact on the health of patients	1	2	3	4	5	
	Average differential data loss/corruption	1	2	3	4	5	
	Average differential impact on privacy	1	2	3	4	5	
	Average differential impact on patients' trust	1	2	3	4	5	
	Average differential impact on patients' trust	1	2	3	4	5	
	Other indicators						
Question 7	**Given the ROI evaluation process above, do you have a similar one to evaluate IT investments?**	Y	N				
	if NOT, how much do you think it is important to use this type of methodology? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)	1	2	3	4	5	
	If YES, are you satisfied with it?	Y	N				
	If not, why?						
Question 8	**Do you notice some missing steps in the ROI evaluation process above ?**	Y	N				
	If YES, specify						

Implementation guidelines

Definition

The Implementation guidelines are meant to support the HCO in the adoption of cybersecurity solutions, either technical or non-technical. Their purpose is to ensure that the solutions

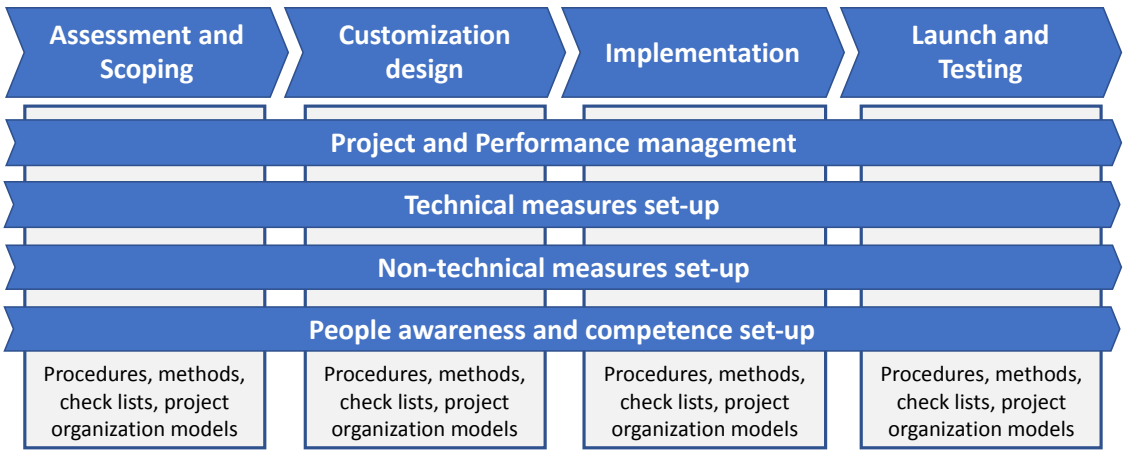
- fits with the needs and the context of the HCO
- are implemented effectively and efficiently
- produce the expected results.

The guidelines consist in procedures, check-lists, methods, project organization models do be used during the implementation process.

Objectives of the topic session

In order to contextualize the implementation guidelines, we have structured the adoption process in four phases and four streams and we aim at understanding how to contextualize each one of and them: on which ones the Panacea project should focus, for which measures the guidelines are more needed, which contextual factors should be taken into consideration in the adoption process

The adoption process may be structured in four phases and four streams of activity.



The four phases include:

- **Assessment and scoping**: consists in preliminary assessment of the initial security level of the HCO considering different aspects such as governance, past risk incidents, current policies and procedures, company business profile, data management, etc.; it identifies the areas of intervention
- **Customization design**: consists in adapting to the HCO the cybersecurity solution (e.g. the Panacea Solution Toolkit). Options may emerge, and a choice is needed. The ROI tool is used in this phase
- **Implementation**: consists in the actual customization and installation of the selected solutions
- **Launch and testing**: consists in teaching the staff and in organizing a validation demo or a pilot.

The four streams include:

- **Project and performance management:** consists in activities, activities to set up and track the project and the key performance indicators, and activities to adjust the initial plan and design in order to reach the expected results; it includes the ROI evaluation

- **Technical measures set up**: consists in the actual design, implementation and testing of the technical measures; in the Panacea case, it includes the set-up of an environment emulator
- **Non-Technical measures set up**: consists in the actual design, implementation and testing of the non-technical measures
- **People awareness and competence set-up**: consists in organizational change management activities, such as communication and training on the implemented solution.

Question 1	Given this implementation process above, do you have a similar one?	Y	N				
Question 2	Do you notice some missing phase?	Y	N				
Question 3	Do you notice some missing stream?	Y	N				
Question 4	Which are the issues/improvement for phase: Assessment and scoping?						
	Vision/Strategy	Y	N				
	Decision making process	Y	N				
	Skills	Y	N				
	Documentation/Asset inventory	Y	N				
	Resistance to change						
	Other						
Question 5	Which are the issues/improvement for phase: Customised Design?						
	Decision making process	Y	N				
	Skills	Y	N				
	Documentation/Asset inventory	Y	N				
	Resistance to change						
	Other						
Question 6	Which are the issues/improvement for phase: Implementation?						
	Decision making process	Y	N				
	Skills	Y	N				
	Documentation/Asset inventory	Y	N				
	Resistance to change	Y	N				
	Other	Specify					
Question 7	Which are the issues/improvement for phase: Testing and launching?						
	Decision making process	Y	N				
	Skills	Y	N				
	Documentation/Asset inventory	Y	N				
	Resistance to change	Y	N				
	Other	Specify					
Question 8	Which types of cybersecurity measures are more in need of implementartion guidelines, in HCOs? (1: Very low need; 2: Low need; 3: Medium need; 4: High need; 5: Very high need)						
	Adoption of Risk Assessment technologies and methods	1	2	3	4	5	
	Adoption of Secure Information Sharing technologies and methods	1	2	3	4	5	
	Adoption of Identity and Authentication technologies and methods for users	1	2	3	4	5	
	Adoption of Identity and Authentication technologies and methods for medical devices	1	2	3	4	5	
	Adoption of Security by Design technologies and methods	1	2	3	4	5	
	Adoption of Risk Governance measures (organization, plans, periodical controls, standard ooperating procedures, insurance schemes)	1	2	3	4	5	
	Adoption of new training/education packages	1	2	3	4	5	
	Adoption of measures to change the behaviours in the daily operations	1	2	3	4	5	
Question 9	Which of the following aspects should be taken into account in the implementation guidelines? (1: Very low importance; 2: Low importance; 3: Medium Importance; 4: High Importance; 5: Very High importance)						
	Adoption level of information technology in the HCO in scope	1	2	3	4	5	
	Existance of a process for the integration of a new system within the HCO in scope	1	2	3	4	5	
	Existance of specific health safety rules/processes for the integration of new system within the HCO in scope	1	2	3	4	5	
	Existance of Guidelines to perform the evaluation of new cybersecurity solutions within a HCO	1	2	3	4	5	
	The actual IT architecture of the HCO in scope	1	2	3	4	5	
	Actual types of medical devices in the HCO in scope	1	2	3	4	5	
	Level of cyber-security awareness within the HCO in scope	1	2	3	4	5	
	Other						

Focus Group Script

Aim: set the scene

Thank you for joining us today and giving up your valuable time.

My name is Lynne and this is Dawn and we are researchers at the University of Northumbria in the UK.

I would like to remind you that nothing that you say today will be shared with your employers. The purpose of this session is to ensure we understand what is really going on in your place of work and whether or not there are any issues that may need to be fixed. This is not about identifying individual people who might be doing something wrong, or placing blame with anyone, but simply understanding why things might be going wrong – and what can potentially be done to improve things.

As healthcare locations and equipment are increasingly more connected with the internet, and more and more of the processes are being computerised, we need to understand if these locations are secure. By this I mean that patient records cannot be stolen, devices cannot be tampered with from outside, and hackers cannot block the system and stop it working. To do this we need the right combination of technology, processes and staff behaviour.

I will be using the term cybersecurity today, and wonder what does this term mean to you? [Have definition available should anyone say they do not understand the term]

CURRENT EXPERIENCE

Aim: Explore previous experiences which may be driving attitude

Firstly, let me ask if anyone has any experience of something going wrong in the workplace, which they believe was a result of poor cybersecurity?

For each one probe: How do you think that happened, what do you think caused that to happen? How was the incident handled? (e.g., were any improved security measures put into place, how was ransomware dealt with etc).

If not, is there anything you worry about, that could go wrong and that the hospital could have some sort of cyberattack?

BEHAVIOURS

Aim: Explore if there is a policy in place, including: what behaviours it covers, whether staff think it is excessive or missing anything, and what they think influences the associated behaviours. Review expected secure behaviours, whether or not they actually carry them out and how their behaviour is influenced.

I would now like to explore specific behaviours related to cybersecurity and understand what behaviours you think are necessary and how your behaviour is influenced at work.

Firstly what behaviours do you think help keep your workplace secure?

Do you always behave securely?

If not, in what circumstances would you not behave securely?

How did you learn about these behaviours?

Is there training in place? What sort of training?

Do you have any sort of policy at work that tells you what is expected of you?

What behaviours does this cover?

Do you sign anything that says you will follow the policy/behave securely?

Are there any other behaviours that you think are needed at work that people don't currently do?

Do you see any messages around the workplace relating to how to behave securely?

What are the rewards/incentives for behaving securely?

What are the sanctions/disincentives to not behaving securely?

Lastly, I would just like to go over some behaviours more specifically.

For each behaviour (that has not been explored in the conversation so far) explore how important it is, whether or not they do it (and if applicable, how they do it), if they could avoid it, and whether they think it is necessary (e.g., whether any behaviours are seen as a burden or a barrier to productivity).

1 Password creation – how do you create a password and understand its strength?
2 Passwords security and sharing
3 Clicking on links in email
4 Opening documents/attachments from email
5 Using Facebook or other social media in the workplace
6 Using USB devices
7 Copying files to personal devices
8 Sharing online files or information about patients between each other
9 Do you encrypt information on computers, and/or when sending between people/organisations?
10 Do you log out of shared workstations when you are not using them?
11 Do you physically secure your devices, e.g. locked room?
12 Who is responsible for backing up files, keeping software up to date, ensuring antivirus and firewalls are active?

Is there anything else we have not covered today, that you feel is important to discuss in relation to cybersecurity in your workplace?

THANK YOU

I would just like to thank you all again for your honesty and taking part in this discussion.

Annex B
End-Users and Stakeholders Requirements

This Annex B complements the information provided in Section 6 and reports the tables for the entire Users' requirements of the PANACEA toolkit for each case study.

General Requirements

Field	Value
ID	GEN_USER_FUN-1
Title	Awareness in HCOs
Category	Functional
Description	Awareness about cyber security shall be provided to HCO.
Justification	HC organizations are a critical target of cyber-attacks. HC personall must be aware of possible risks compromising their critical business processes and how to mitigate them
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_FUN-2
Title	Cybersecurity and risk management in HCOs
Category	Functional
Description	Cyber security risk management process shall be provided to HCO.
Justification	HC organizations are a critical target of cyber-attacks. HC personall must be aware of possible risks compromising their critical business processes and how to mitigate them
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-1
Title	Solution
Category	Product
Description	PANACEA toolkit shall support cyber security risk assessment and awareness tools and methods for HC organizations (in the following solution aspect)
Justification	The aspects are required to provide support both in technical and economical perspectives
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-2

Title	Delivery
Category	Product
Description	PANACEA toolkit shall support economical evaluation of the deployment of the parts reported in GEN_USER_NONFUN-1 (in the following delivery aspect).
Justification	The aspects are required to provide support both in technical and economical perspectives
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-3
Title	Independence of tools
Category	Product
Description	Independent solutions/tool shall compose the PANACEA toolkit
Justification	Depending on the HC organization, some solutions of the PANACEA toolkit may not be needed. The deployment approach must hence be tailored to each HC organization.
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-4
Title	
Category	Product
Description	The solution aspect shall support cybersecurity both on system and organisational/human components of the Healthcare centre.
Justification	Determine which is the scope of solution aspect
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-5
Title	Integration of toolkits
Category	Product
Description	The delivery aspect shall integrate the use of the solution aspect under the economic efficiency and the implementation points of view.
Justification	Determine which is the scope of delivery aspect
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-6
Title	Ufficial language
Category	Product
Description	The PANACEA Toolkit shall be localized in English
Justification	International language
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-7
Title	Other languages
Category	Product
Description	The PANACEA Toolkit (or some of its components) may be localized in other languages.
Justification	Not all HC personnel has a good command of English
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-8
Title	Integration with existant solution in HCO
Category	Organizational
Description	All the tools composing PANACEA toolkit shall be able to integrate with the existing technical and organizational infrastructure of the HC organization, when applicable.
Justification	The solution toolkit (or a subset of it) may need to be integrated with other existing technical tools and policies. For example, the HC organization may leverage existing network and vulnerability management systems.
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Field	Value
ID	GEN_USER_NONFUN-9
Title	Type of data management
Category	Organizational
Description	The solution aspect shall be able to properly handle confidential data about patients, HC personnel and the IT infrastructure of the HC organization in accordance with European and local regulatories
Justification	Some components of the PANACEA toolkit handle confidential data. Appropriate security measures must be put in place in order to ensure their protection.
Priority	HIGH
Version	1.0

Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Risk Assessment and Mitigation Requirements

ID	TOP_RSK_USER_FUN_1
Title	Risk evaluation
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall provide an evaluation of the risks related to possible path of attacks within the IT infrastructure of the HC organization.
Justification	The IT infrastructure (including connected medical devices) of an HC organization leverages most of the HC business processes and is a possible target of cyber attacks
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Non-health Roles

ID	TOP_RSK_USER_FUN_2
Title	Determination of model
Category	Functional
Description	In order to perform Dynamic risk assessment and mitigation activities, a threat reference model of the IT infrastructure (including medical devices connected via IP protocol) shall be taken into consideration as an input for the dynamic risk assessment and mitigation platform.
Justification	This will allow characterization of various attack strategies leveraged by a threat agent within the TRM without reference to the details of the IT infrastructure
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Non-health Roles

ID	TOP_RSK_USER_FUN_3
Title	Determination of network topology
Category	Functional
Description	In order to perform Dynamic risk assessment and mitigation activities, the network topology (ISO/OSI layer 3 and 4) of the IT infrastructure (including medical devices connected via IP protocol) shall be an input for the dynamic risk assessment and mitigation platform.
Justification	This will allow characterization of various attack strategies based on the network topoogy
Priority	HIGH

Version	1.0
Source	Workshop
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_4**
Title	Model updating
Category	Functional
Description	Within the context of dynamic risk assessment and mitigation activities, It shall be possible to update the threat reference model of the IT infrastructure.
Justification	This will allow characterization of various attack strategies leveraged by a threat agent within the TRM without reference to the details of the IT infrastructure
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_5**
Title	Medical devices
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall take into consideration every device connected to the IT infrastructure in scope via the IP protocol.
Justification	Every device connected via IP protocol to the IT infrastructure in scope for the risk analysis could be part of a possible attack path.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_6**
Title	Devices monitoring
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall consider changes in the network topology of the IT infrastructure (new devices connected, devices disconnected, etc...)
Justification	Changes in the network topology may trigger new possible attack paths and raise the level of risk.
Priority	HIGH

Version	1.0
Source	SoA
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_7**
Title	Considering human behavior in risk evaluation
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall consider the human behavior of the HC personnel for the computation of the risk and the suggested mitigation actions.
Justification	Humans misbehaviors in cyber-security are among the major causes of incidents. As part of the risk evaluation, this factor must be taken into consideration.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles, External Roles

ID	**TOP_RSK_USER_FUN_8**
Title	Actions proposal
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall propose mitigation actions to reduce the level of risk.
Justification	Mitigation actions are computed in relationship to the risk assessment evaluation of the IT infrastructure. Proper mitigation action will cut existing possible paths of attack in order to lower the risk levels.
Priority	HIGH
Version	1.0
Source	Experts, SoA
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_9**
Title	Risk reduction effectiveness classification
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall automatically rank the suggested mitigation actions (for example, by the potential risk reduction).
Justification	Different mitigation actions may have different impact in the reduction of the risk
Priority	HIGH
Version	1.0
Source	Experts, SoA

User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_10**
Title	Graphical reconstrucion
Category	Functional
Description	Dynamic risk assessment and mitigation platform shall provide a graphical reconstruction of the IT infrastructure under protection, with additional information about HC personnel accessing it (e.g., roles, accessed resources)
Justification	A graphical representation of the IT infrastructure in scope improves the awareness of the users (the IT and security departments) on possible cyber threats.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_11**
Title	Graphical summary
Category	Functional
Description	Dynamic risk assessment and mitigation platform shall provide a graphical summary of evaluated risks of the IT infrastructure under protection, with additional information about HC personnel accessing it (e.g., roles, accessed resources)
Justification	A graphical representation of the risk evaluation improves the cyber awareness of the users (the IT and security departments).
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_12**
Title	Graphical summary
Category	Functional
Description	Dynamic risk assessment and mitigation platform shall provide a graphical summary of the suggested mitigation actions to reduce the level of risks of the IT infrastructure under protection, with additional information about HC personnel accessing it (e.g., roles, accessed resources)
Justification	A graphical representation of the suggested mitigation actions improves the cyber awareness of the users (the IT or security departments).
Priority	HIGH
Version	1.0
Source	Workshop

User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_13**
Title	IT infrastructure protection
Category	Functional
Description	The dynamic risk assessment and mitigation platform should be able to protect distributed IT infrastructure (not limited to a single physical site but belonging to the same organization)
Justification	While some HC organization are concentrated on a single premise, other are distributed in the territory, but still connected by the same network. Paths of attack may start from one site and involve another site: it is then important to potentially consider multiple sites when computing the risk.
Priority	HIGH
Version	1.0
Source	Risk Scenarios
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_14**
Title	List of mitigation actions
Category	Functional
Description	Mitigation actions suggested by the dynamic risk and mitigation activities shall be selected from a pre-defined list of mitigation actions.
Justification	Mitigation actions may be possibly invasive for the organization ad at the same time, not all mitigation actions are applicable in all organizations. It is hence important for the users to pre-define a list of possible mitigation actions for the risk treatment.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_15**
Title	IT infrastructure vulnerabilities
Category	Functional
Description	Dynamic risk assessment and mitigation activities shall take into account the vulnerability surface of the IT infrastructure including those due by HC personnel interactions.
Justification	Awareness of the technical vulnerabilities of the IT infrastructure is a necessary element of the risk evaluation

Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_16**
Title	Existing technical risk mitigation measures
Category	Functional
Description	Dynamic risk assessment and mitigation action shall take into account existing technical risk mitigation measures (firewalls, IPS, IDS, etc..) within the evaluation of the risks
Justification	Existing mitigation measures need to be evaluated during risk computation, sicne they may be able to (partially) reduce the possible paths of attack
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_17**
Title	Mitigation actions against ramsomware
Category	Functional
Description	The predefined list of mitigation actions shall encompass measures to mitigate the risk of ransomware attacks.
Justification	Ransomware prevent the daily operations of the hospital
Priority	HIGH
Version	1.0
Source	Risk Scenarios
User Involved	Non-health Roles

ID	**TOP_RSK_USER_FUN_18**
Title	Learning functionality
Category	Functional
Description	Dynamic Risk assessment computation may be based on past experience
Justification	Past experience can improve the service of dynamic risk assessment
Priority	LOW
Version	1.0
Source	Risk Scenarios
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	TOP_RSK_USER_NONFUN_1
Title	Human behaviour
Category	Product
Description	Dynamic risk assessment and mitigation activities shall take into consideration the human behavior of the healthcare personnel interacting with the IT infrastructure (including medical devices)
Justification	Human misbehavior is one of the most important source of cyber risks.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	TOP_RSK_USER_NONFUN_2
Title	Security policies and guidelines
Category	Product
Description	Existing security policies and guidelines shall be considered in the risk assessment and mitigation processes.
Justification	Human behavior may be affected by strong security policies, resulting in risk reduction.
Priority	HIGH
Version	1.0
Source	Experts, Workshop
User Involved	Managers, Non-health roles

ID	TOP_RSK_USER_NONFUN_3
Title	Risk assessment and mitigation activities tool
Category	Organizational
Description	Dynamic risk assessment and mitigation activities shall be leveraged by dynamic risk assessment and mitigation software platform developed as part of the PANACEA toolkit.
Justification	While many COTS products for incident detection and response exist, dynamic risk assessment platforms for proactively improve the security posture of an IT infrastructure are still very scarce in the market. In addition, usually the human behavior is not taken into consideration in the risk analysis.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Non-health roles

ID	TOP_RSK_USER_NONFUN_4
Title	IT infrastructure compromission
Category	Organizational
Description	Dynamic risk assessment and mitigation activities shall take into account the impact on the business activities of the organization due to the compromission of the IT infrastructure
Justification	Risk is function of likelihood of an attack and impact over the organization. Business processes must hence be analysed and traced to the supporting IT infrastructure in order to properly compute the risk.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Non-health roles

ID	TOP_RSK_USER_NONFUN_5
Title	Impact on business activities
Category	Organizational
Description	Dynamic risk assessment and mitigation activities shall compute the impact of the suggested mitigation actions over the business activities of the organization
Justification	Mitigation actions may be possibly invasive for the organization, in particular within critical systems. It is hence important to evaluate their impact on order to allow a proper prioritization and selection.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Non-health roles

ID	TOP_RSK_USER_NONFUN_6
Title	Authentication control for devices of IT infrastructure under protection
Category	Organizational
Description	Dynamic risk assessment and mitigation activities shall take into account how users are authenticated to devices of the IT infrastructure under protection.
Justification	User authentication is a critical process and may lead to cyber attacks. It is hence important for the risk analysis to evaluate the strenght of the user authentication mechanisms.
Priority	HIGH

Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	**TOP_RSK_USER_NONFUN_7**
Title	Results protection
Category	Organizational
Description	All results of the dynamic risk assessment and mitigation activity shall be protected in terms of availability, confidentiality and integrity.
Justification	Any attacker could greately benefit from these information.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	**TOP_RSK_USER_NONFUN_8**
Title	Data protection
Category	Product
Description	All data collected during the dynamic risk assessment and mitigation activities shall be protected in terms of availability, confidentiality and integrity
Justification	Any attacker could greately benefit from these information.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	**TOP_RSK_USER_NONFUN_9**
Title	Anonymous access not allowed
Category	Product
Description	The dynamic risk assessment and mitigation platform shall not allow anonymous access
Justification	In order to allow no repudiation it is needed that all the activities could be reconducted to only one person
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Non-health Roles

ID	TOP_RSK_USER_NONFUN_10
Title	Secure password management
Category	Product
Description	The dynamic risk assessment and mitigation platform shall ensure a secure password management
Justification	Password is one of the sensitive information
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Non-health Roles

ID	TOP_RSK_USER_NONFUN_11
Title	Security of transmitted data
Category	Product
Description	The end to end transmission of data within the dynamic risk assessment and mitigation platform shall guarantee integrity and confidentiality.
Justification	Information should be protected in all its treatments
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	TOP_RSK_USER_NONFUN_12
Title	Authentication mechanism
Category	Product
Description	An authentication mechanism shall be put in place in order to access to the dynamic risk assessment and mitigation platform.
Justification	Authentication is needed in order to guarantee confidentiality of information
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-health Roles

ID	TOP_RSK_USER_NONFUN_13
Title	Data sources
Category	Product
Description	When a minimum baseline of needed information is available (e.g. Configuration Management Database ...), the dynamic risk assessment platform shall interact with network/asset information gathering tools already installed in the HC organization and, in case, update records of information.

Justification	The platform should be able to abstract the data sources (assuming they are reachable and they provide sufficient information), in order to be adaptable (may be using different plug-ins) to existing network/assets management tools. Furthermore, NIS Directive imposes the usage of assets manager tools (e.g. CMDB) in order to manage the status of available assets within the critical infrastructures. For this reason, cooperation with this kind of tools is important in order to be compliant with the Derective.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health Roles, External Roles

ID	**TOP_RSK_USER_NONFUN_14**
Title	Documented criteria
Category	External
Description	The information security risk criteria, including acceptance criteria and how to perform security risk assessment shall be documented
Justification	Documentation is required in order to have all the criterias clear and to manage all kinds of inconvenience
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_15**
Title	Results features
Category	External
Description	The results provided during the dynamic risk assessment and mitigation action shall be measurable, consistent and comparable
Justification	This permits to monitor the performance of the activities and put in place eventual modification in the processes to implement continual improving
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_16**
Title	Risk owner
Category	External

Description	Each risk identified during the dynamic risk assessment shall have assigned a risk owner
Justification	Risk owner is a figure that knows the risk and decide how to manage with it
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_17**
Title	Analisys of results
Category	External
Description	The results of the dynamic risk assessment shall be analysed in accordance with the risk criteria reported in TOP_RSK_USER_NONFUN_14
Justification	Evaluation of the processes based on the criterias organizations give themselves is important for the continual improvement
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_18**
Title	Results as documented information
Category	External
Description	The result of the dynamic risk assessment shall be retained as a documented information
Justification	Evaluation of the processes based on the criterias organizations give themselves is important for the continual improvement
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_19**
Title	Status of risk treatment plan assessment
Category	External
Description	All the results provided by the dynamic risk assessment and mitigation activities shall be used in order to assess a risk treatment plan composed by one or more mitigation actions.

Justification	Evaluation of the processes based on the criterias organizations give themselves is important for the continual improvement
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-health Roles

ID	**TOP_RSK_USER_NONFUN_20**
Title	Process of impact assessment
Category	External
Description	Dynamic risk assessment and mitigation activities shall take into account the privacy impact on the organization due to data leaks of personal data
Justification	Security of personal data should be ensured
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-health Roles, External Roles

Information Sharing Requirements

ID	**TOP_ISH_USER_FUN_1**
Title	Information sharing system HL7 support
Category	Functional
Description	The information sharing system should provide support for HL7 (Health Level Seven)
Justification	The HL7 standard is used in the healthcare domain for interoperability between system
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_2**
Title	Secure information sharing mechanism
Category	Functional
Description	The information sharing system shall have customizable role-based access controls to align with the organizational needs, i.e. health, non-health, manager, external
Justification	Not all the user have the same need to know

Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_3**
Title	Secure information sharing mechanism
Category	Functional
Description	The information sharing system shall allow healthcare information to be shared with users across HCO organizational or territorial borders
Justification	The main purpose of this topic is share information among all the stakeholders
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_4**
Title	Secure share of information
Category	Functional
Description	Health personnel in HCO shall be able to share information in a secure way for the below services: Service user healthcare records Emergency department, birth, theatre, minor operations and other related registers. X-ray and imaging reports Photographs, slides, and other images. Computerised records. Scanned records.
Justification	This will allow to avoid disclosure of data
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Health Roles

ID	**TOP_ISH_USER_FUN_5**

Title	Secure information sharing mechanism
Category	Functional
Description	The information sharing system may get identification information on its users from an external identification management platform
Justification	Identify the user is the first step to authenticate it
Priority	LOW
Version	1.0
Source	Experts
User Involved	Non-Health Roles

ID	**TOP_ISH_USER_FUN_6**
Title	Clinical and management reporting security
Category	Functional
Description	Health personnel in HCO shall share data for management reporting and for clinical reporting in a secure way
Justification	This will allow to avoid disclosure of data
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles

ID	**TOP_ISH_USER_FUN_7**
Title	Suppliers data
Category	Functional
Description	Health personnel in HCO should share suppliers data in a secure way
Justification	This will allow to avoid disclosure of data
Priority	MEDIUM
Version	1.0
Source	Workshop
User Involved	Managers, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_8**
Title	Web client user interface
Category	Functional
Description	The information sharing system shall feature a web client user interface
Justification	Web client is used by its simplicity of usage.

Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_9**
Title	Notifications
Category	Functional
Description	The information sharing system should provide tailored email and UI notifications to users of the system after a system event occurs.
Justification	This permit to be updated about all information
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_10**
Title	Health taxonomy
Category	Functional
Description	The information sharing system shall capture healthcare data using a health domain specific taxonomy
Justification	N.A.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_FUN_11**
Title	Information sharing system
Category	Functional
Description	Data which is not shared in the information sharing system shall never be distributed to other installations or be made accessible outside of the information sharing system
Justification	This allows to avoid information disclosure
Priority	HIGH

Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_1**
Title	Authentication mechanism
Category	Product
Description	An authentication mechanism shall be put in place in order to access to the information sharing platform
Justification	This permits to realize confidentiality
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_2**
Title	Non repudiation mechanism
Category	Product
Description	A non repudiation mechanism shall be put in place for the communication
Justification	This permits to identify who performed actions
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_3**
Title	Backup
Category	Product
Description	The information sharing system should be able to recover from data loss.
Justification	This in order to mitigate information theft and IT systems attacks
Priority	HIGH
Version	1.0
Source	Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_4
Title	Inactivity
Category	Product
Description	Communication among parties shall implement an automatic closing mechanism in case of inactivity.
Justification	Usually, personnel forget to lock logout from the system. This is done automatically in order to avoid disclosure of information
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_5
Title	Audit trails
Category	Product
Description	Data manipulation and data sharing within the information sharing system shall have audit trails to trace successful and unsuccesful events
Justification	Permits to take trace about all the actions performed in the information sharing system for both prevention and analysis phases.
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_6
Title	Secure password management
Category	Product
Description	The information sharing system shall ensure a secure password management
Justification	Password is a sensitive information and shall be protected
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_7
Title	Security of transmitted data
Category	Product
Description	The end to end transmission of data within the information sharing system shall guarantee integrity and confidentiality.
Justification	This permits confidentiality of information
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_8
Title	Anonymus access
Category	Product
Description	The information sharing system shall not allow anonymous access
Justification	This permits non repudiation of actions
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_9
Title	long-term preservation
Category	Product
Description	The information sharing system shall support long-term preservation of data
Justification	This allows to retrieve data even located long time in the past
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_10
Title	Information sharing system capability
Category	Product

Description	The information sharing system shall be capable of providing parallel user sessions managing munienteltiple healthcare records
Justification	This requirement set the feature of this platform to support different sessions and managing different records
Priority	HIGH
Version	1.0
Source	Experts, Scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_11
Title	Recovering
Category	Product
Description	The information sharing system shall be able to recover after a crash or reboot
Justification	Communication is of major importance in healthcare organizations and the channels must be recovered after a crash or reboot
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_12
Title	Information sharing system
Category	Organizational
Description	Healthcare personnel in HCO shall leverage on an information sharing platform to securely share information developed as part of the PANACEA toolkit.
Justification	To support the secure sharing of data, it emerges the need of an ad-hoc software platform.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_13
Title	Platform features
Category	Organizational
Description	The information sharing system shall allow comments to be recorded and exchanged

Justification	N.A.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_14**
Title	Platform features
Category	Organizational
Description	The platform shall permit download of data for offline access
Justification	This permits to consultate information even without an internet connection
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_15**
Title	Directly sharing
Category	Organizational
Description	The information sharing system may allow medical devices to provide data directly into the system through API interoperability
Justification	This will permit to medical device to share information directly with the platform
Priority	LOW
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_ISH_USER_NONFUN_16**
Title	Browser versions supported
Category	Organizational
Description	The information sharing system web client user interface shall support the latest version of Mozilla Firefox, Google Chrome, Microsoft Edge at the time of development
Justification	Platform should support the most used browsers
Priority	HIGH

Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_17
Title	Browser versions supported -Apple
Category	Organizational
Description	The information sharing system web client user interface should support the latest version of Apple Safari at the time of development
Justification	Platform should support the most used browsers
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_ISH_USER_NONFUN_18
Title	Standalone deployment
Category	Organizational
Description	The information sharing system shall allow standalone deployment as a single server installation
Justification	N.A.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-Health Roles

ID	TOP_ISH_USER_NONFUN_19
Title	Distributed disparate deployment
Category	Organizational
Description	The information sharing system shall allow for a distributed disparate deployment where each server can be interconnected via a network
Justification	N.A.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-Health Roles

ID	TOP_ISH_USER_NONFUN_20
Title	API interoperability
Category	Organizational
Description	The information sharing system shall allow for API interoperability
Justification	N.A.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	TOP_ISH_USER_NONFUN_21
Title	Risk magament on mobile devices
Category	External
Description	Policies and security measures shall be adopted to manage the risk introduced by mobile devices
Justification	Mobile device have an high impact on the security
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-Health Roles

ID	TOP_ISH_USER_NONFUN_22
Title	Teleworking
Category	External
Description	A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites
Justification	Access from remote should be performed securly
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-Health Roles

ID	TOP_ISH_USER_NONFUN_23
Title	Informatin classification

Category	External
Description	Information shall be classified in terms of legal requirements, value, criticality and sensitivity and labelled appropriately
Justification	In this way it is possible to distinguish the level of indormation
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Non-Health Roles

ID	**TOP_ISH_USER_NONFUN_24**
Title	Principles
Category	External
Description	Availability, authenticity integrity and confidentiality of information shall be guaranteed
Justification	This is imposed by the cybersecurity act and ISO27001
Priority	HIGH
Version	1.0
Source	Cybersecurity act, ISO27001
User Involved	Managers, Non-Health Roles

ID	**TOP_ISH_USER_NONFUN_25**
Title	Business Continuity
Category	External
Description	Procedures of business continuity shall be defined to tackle with theft of information needed during critical and not critical processes
Justification	Resilience should be implemented in order to be able to handle critical events
Priority	HIGH
Version	1
Source	ISO27001
User Involved	Managers, Non-Health Roles

ID	**TOP_ISH_USER_NONFUN_26**
Title	Data protection
Category	External

Description	Information data shall be protected by distruction, loss or non-authorized modification
Justification	This is imposed by the cybersecurity act
Priority	HIGH
Version	1.0
Source	Cybersecurity act
User Involved	Managers, Non-Health Roles

ID	TOP_ISH_USER_NONFUN_27
Title	Security measures adoption
Category	External
Description	Appropriate technical and organisational measures to ensure a level of security appropriate to the risk of personal data shall be implemented
Justification	Adequate techniques in order to handle with personal data should be put in place
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Non-Health Roles

ID	TOP_ISH_USER_NONFUN_28
Title	Data transfer
Category	External
Description	Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if the recipient guarantees an adequate protection level
Justification	Transfer among countries should be regulated
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Non-Health Roles

ID	TOP_ISH_USER_NONFUN_29
Title	Identification and retrivial of information
Category	External

Description	Records shall be readily identifiable and retrievable. Changes to a record shall remain identifiable.
Justification	This permit to provide availability and integrity of information
Priority	High
Version	1.0
Source	EN ISO 13485
User Involved	Managers, Non-Health Roles

Security-by-design and certification Requirements

ID	TOP_SDC_USER_FUN_1
Title	Medical device manufacturers support during the entire lifecycle of medical devices
Category	Functional
Description	Medical device manufacturers shall be able to perform risk assessments and assess possible cyber-risks associated to the medical device during all its lifecycle.
Justification	It is important to consider cyber-security in all the phases of medical devices life cycle.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Health Roles, Non-Health Roles, External Roles

ID	TOP_SDC_USER_FUN_2
Title	System/software providers support during the entire lifecycle of a new system/software for HC
Category	Functional
Description	System/software providers shall be able to perform risk assessments and assess possible cyber-risks associated to the system/software during all its lifecycle.
Justification	It is important to consider cyber-security in all the phases of new systems/softwares for HC life cycle.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Health Roles, Non-Health Roles, External Roles

ID	TOP_SDC_USER_FUN_3
Title	Medical devices requirements definition
Category	Functional
Description	Medical device manufacturers shall be able to perform a risk assessment over a medical device in development and extract tailored security requirements in relationship with the assessed risks.
Justification	During the requirement phase in particular (but needed in all phases of a medical device lifecycle) it is needed to finalize the missing cyber-security controls into proper requirements for new medical devices.
Priority	HIGH
Version	1.0
Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	TOP_SDC_USER_FUN_4
Title	Medical devices design input management
Category	Functional
Description	Medical device manufacturers shall be able to perform risk assessments over a medical device in development and use the design inputs in order to assess the needed cyber-security controls.
Justification	During the design phase in particular (but needed in all phases of a medical device lifecycle) it is needed to use the design inputs in order to assess the cyber-security risks.
Priority	HIGH
Version	1.0
Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	TOP_SDC_USER_FUN_5
Title	Maintenance of medical devices
Category	Functional
Description	Medical device manufacturers shall capture cyber-security risks introduced by software/hardware updates due to reactions to end-users feedbacks.
Justification	Maintenance of a medical device is a crucial aspect of its life-cycle. Reactions to feedbacks from the customers may lead to software/hardware updates which may acffect the cyber-security posture of the device.
Priority	HIGH
Version	1.0

Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	**TOP_SDC_USER_FUN_6**
Title	System/software providers requirements definition
Category	Functional
Description	System/software providers shall be able to perform risk assessments over a system/software in development and extract tailored security requirements in relationship with the assessed risks.
Justification	During the requirement phase in particular (but needed in all phases of a new system/software for HC) it is needed to finalize the missing cyber-security controls into proper requirements for new system/software for HC.
Priority	HIGH
Version	1.0
Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	**TOP_SDC_USER_FUN_7**
Title	System/software providers design input management
Category	Functional
Description	System/software providers shall be able to perform risk assessments over a system/software in development and use the design inputs in order to assess the needed cyber-security controls.
Justification	During the design phase in particular (but needed in all phases of a new system/software for HC) it is needed to use the design inputs in order to assess the cyber-security risks associated to design for new system/software for HC.
Priority	HIGH
Version	1.0
Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	**TOP_SDC_USER_FUN_8**
Title	Maintenance of system/software for HC
Category	Functional
Description	System/software providers shall capture cyber-security risks introduced by software/hardware updates due to reactions to end-users feedbacks.

Justification	Maintenance of a system/software is a crucial aspect of its life-cycle. Reactions to feedbacks from the customers may lead to software/hardware updates which may affect the cyber-security posture of the device.
Priority	HIGH
Version	1.0
Source	Workshop, Expert
User Involved	Health Roles, Non-Health Roles, External Roles

ID	TOP_SDC_USER_FUN_9
Title	Manifacturers risk management
Category	Functional
Description	Medical devices manufacturers shall be supported on establish, implement, document and maintain a risk management system for their system engineering life-cycle.
Justification	Risk management shall be understood as a continuous iterative process throughout the lifecycle of a system/software/medical requiring regular systematic updating. Risk management is a fundamental step in order to implement resilience. This permits also the continuous improvement.
Priority	HIGH
Version	1.0
Source	MDR
User Involved	External Roles

ID	TOP_SDC_USER_FUN_10
Title	Security requirements definition
Category	Functional
Description	As a result of the cyber-risk assessment, medical device manufacturers and system/software providers shall be able to extract needed cyber-security requirements/controls.
Justification	In order to evaluate the characteristics of the supporting software/hardware for any system/software/medical devices in development it is important to evaluate the cyber-security needs of the system.
Priority	HIGH
Version	1.0
Source	MDR
User Involved	External Roles

ID	TOP_SDC_USER_FUN_11
Title	Confidentiality and secrecy of information
Category	Functional

Description	Confidentiality, integrity and availability of information stored in system/software/medical devices shall be guaranteed by the security-by-design framework.
Justification	Limitate data access in case of theft of device or attack to IT systems
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	External Roles

ID	**TOP_SDC_USER_FUN_12**
Title	Cyber Risk Assessment of medical devices and system/software for HC
Category	Functional
Description	Medical devices manufacturers and system/software providers shall perform cyber-security risk assessments over medical devices and system/software for HC during their life-cycle.
Justification	It is important to understand how to compute the cyber risk within the system life-cycle
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Non-Health Roles, External Roles

ID	**TOP_SDC_USER_FUN_13**
Title	Cyber Risk Assessment of medical devices and system/software for HC-output
Category	Functional
Description	Medical devices manufacturers and system/software providers shall be able to compute the residual cyber risk of the system/software/medical device, after the application of the security requirements/controls suggested by the risk assessment.
Justification	It is important to compute residual cyber risk in order to evaluate the attuated countermeasures and attuate new if the level of risk is not acceptable
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_1**

Title	Trust service involving
Category	Product
Description	Medical devices manufacturers shall involve a Trust Service provider during their manufacturing phase.
Justification	Trust Service provider may be involved on each technical choice for security aspect in order to be compliant with policies and standards for medical devices.
Priority	HIGH
Version	1
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_2**
Title	Guarantee of a secure password
Category	Product
Description	The Security Design Assessment System shall ensure a secure password management.
Justification	Password is a sensitive information and must be protected, especially on any tool dealing with potentially sensitive information.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_3**
Title	Security of transmitted data
Category	Product
Description	The end to end transmission of data within the Security Design Assessment System shall guarantee integrity and confidentiality.
Justification	This allow to avoid information disclosing and man-in-the-middle attacks
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_4**
Title	Uniquely user identification
Category	Product
Description	An authentication mechanism shall be put in place in order to access to the Security Design Assessment System.

Justification	This allow to implement non-repudiation.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_5
Title	Anonymous access
Category	Product
Description	The Security Design Assessment System shall not allow anonymous access.
Justification	This allow to implement non-repudiation.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_6
Title	Data protection
Category	Product
Description	All data managed by the Security Design Assessment System shall be protected in terms of availability, confidentiality and integrity.
Justification	All results of the Security Design Assessment System shall be protected in terms of availability, confidentiality and integrity. Any attacker could greately benefit from these information.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_7
Title	Product risks reduction - Manufacturer
Category	Product
Description	Medical devices manufacturers shall rely on a Security-by-design framework that addresses them on reducing as much as possible cyber- security risks.
Justification	Analysis of the risks should be addressed by the manufacturers during the life-cycle of a medical device

Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_8**
Title	Hardware/software resilience
Category	Functional
Description	Security-by-design framework shall allow the identification of cyber-security risks leading to fault resilience impacts.
Justification	The segnalation of a fault and the management of this fault permits to avoid hardware or software stop working
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_9**
Title	Security-by-design framework
Category	Organizational
Description	The PANACEA toolkit shall encompass the development of a security-by-design framework to support the development of medical devices and system/software for HC organizations and improve their cyber-security posture.
Justification	Securing medical devices and system/software for HC begins in the initial phases and should be considered throughout the system development lifecycle. Ensuring proper controls are in place and identifying cyber vulnerabilities should be central to the System Development Lifecycle methodology.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_10**
Title	Security-by-design tools and functions
Category	Organizational

Description	Security-by-design activities to support the development of a system/software/medical device, shall encompass the following tools/functions: -Security by Design Assessment System (SDAS) -Interactive Application Security Testing System (IAST) -Static Application Security Testing System (SAST)
Justification	While a SDAS can monitor the security posture of an HC system (including medical devices and system/software for HC) during its system engineering life-cycle, IAST and SAST are focused on software quality and vulnerabilities. Embedding their usage in the HC system development life-cycle can greatly improve the resulting security of the products. Many IAST and SAST COTS (Commercial-off-the-Shelfs) products can be found in the market (the PANACEA security-by-design framework will propose possible choices), while SDAS are a relatively new concept, to be tailored ad-hoc for the HC sectorin order to optimize the results. The security-by-design framework developed in PANACEA will hence encompass the development of a SDAS and the adoption of COTS IAST and SAST within the system engineering life-cycle.
Priority	HIGH
Version	1.0
Source	Experts, Workshop
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_11
Title	Guidelines for security-by-design development.
Category	Organizational
Description	The Security-by-design framework shall encompass governance and compliance guidelines
Justification	Guidelines considering the regulamentory landscape (with focus on EU policies) and guiding the manufacturer/provider on improving the system development life-cycle from a cyber-security perspective are a needed component of the framework.
Priority	HIGH
Version	1
Source	Experts
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_12
Title	Follow regulations
Category	External
Description	EU standards and regulations for medical devices manufacturing and certification shall be taken into account while developing the security-by-design framework.

Justification	Medical devices are strictly regulated by EU laws and international standards. A detailed research shall be conducted in order to help users of the security-by-design framework to be aligned with the actual EU policies and standards for medical devices (including the future MDR, Medical Device Regulation, entering in force in 2020). Non EU standards may be taken into account as a reference. Among the considered policies/standards: ISO 13485:2016 IEC 62304 IEC 82304-1 ISO 27001 EU MDR (Medical Device Regulation) UL 2900-1 Cybersecurity Standard for Medical Devices (non EU)
Priority	HIGH
Version	1.0
Source	Experts
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_13**
Title	Safety requirements - design and development
Category	External
Description	Security-by-design framework shall allow the identification of cyber-security risks leading to safety impacts.
Justification	Safety should be anyway central during the development of medical devices.
Priority	HIGH
Version	1.0
Source	EN ISO 13485
User Involved	External Roles

ID	**TOP_SDC_USER_NONFUN_7**
Title	Manifacturers minimum set of requirements
Category	Functional
Description	Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
Justification	In order to identify minimum resources for the normal work of medical devices, requirements that design the capacity should be written.
Priority	HIGH
Version	1.0
Source	MDR/IVDR

User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_8
Title	Manifacturers minimum set of requirements
Category	External
Description	Security-by-design framework shall guide medical device manufacturers on adopting a Unique Device Identification for the medical devices.
Justification	The traceability of devices by means of a Unique Device Identification system (UDI system) based on international guidance should significantly enhance the effectiveness of the post-market safety-related activities for devices, which is owing to improved incident reporting, targeted field safety corrective actions and better monitoring by competent authorities. It should also help to reduce medical errors and to fight against falsified devices.
Priority	HIGH
Version	1.0
Source	MDR
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_9
Title	Privacy handling
Category	External
Description	The Security-by-design framework shall allow the identification of cyber-security risks leading to privacy impacts.
Justification	GDPR regulates the privacy management
Priority	HIGH
Version	1.0
Source	ISO62304
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_10
Title	Aspects of security in suppliers
Category	External

Description	The Security-by-design framework for the development of system/software/medical devices shall cover: compromise of sensitive information, authentication, authorization, communication integrity, audit trail, and system security/malware protection
Justification	Security requirements should support the introduction of security inside well defined areas
Priority	HIGH
Version	1.0
Source	ISO62304
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_11
Title	Problem reports
Category	External
Description	The Security by Design Assessment System shall support the production of reports related to the performed risk assessment iteration(s) over the system/software/medical device in development.
Justification	It is fundamental do document all the risk assessment iterations, related highlighted risks and their treatment and associated security measures. These reports can be used in order to guide the implementation teams and can also justify architectural decisions.
Priority	HIGH
Version	1.0
Source	ISO62304
User Involved	External Roles

ID	TOP_SDC_USER_NONFUN_12
Title	Documentation
Category	External
Description	The Security-by-design framework shall guide manufacturers/system providers on developing detailed technical specifications for the system/software/medical device, including security specifications and protection against malware or similar.
Justification	Documentation is important in order to provide support to the end user
Priority	HIGH
Version	1.0
Source	IEC 82304-1

User Involved	External Roles

Identification and authentication Requirements

ID	TOP_IA_USER_FUN_1
Title	Appropriate access
Category	Functional
Description	HC personnel on a HCO organization shall be uniquely authenticated when accessing HC systems
Justification	This will allow to avoid access violation
Priority	HIGH
Version	1.0
Source	SoA
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_IA_USER_FUN_2
Title	Identification management
Category	Functional
Description	HC personnel on a HCO organization shall be uniquely identified when accessing HC systems
Justification	This will allow to guarantee a secure identification between different entities
Priority	HIGH
Version	1.0
Source	SoA, Workshop
User Involved	Health Roles, External Roles

ID	TOP_IA_USER_FUN_3
Title	Authentication for clinical services.
Category	Functional
Description	Strong authentication (i.e. two factors) shall be applicable to clinical services and internet accessible services.
Justification	Strong authentication protect sensitive information
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_IA_USER_FUN_4
Title	Authentication for facility management services.
Category	Functional
Description	Strong authentication (i.e. two factors) should be applicable to facility management services.
Justification	Strong authentication protect sensitive information
Priority	MEDIUM
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_IA_USER_FUN_5
Title	Identification of medical devices
Category	Functional
Description	Medical devices shall be uniquely identified when connecting to other HC systems/networks
Justification	This will allow to guarantee a secure identification between different entities
Priority	HIGH
Version	1.0
Source	Risk scenarios, Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_IA_USER_FUN_6
Title	Authentication of medical devices
Category	Functional
Description	Medical devices shall be uniquely authenticated when connecting to other HC systems/networks
Justification	This will allow to guarantee a secure identification between different entities
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	TOP_IA_USER_NONFUN_1
Title	Identification and Authentication simplicity

Category	Product
Description	Identification and Authentication processes shall be kept as simple as possible
Justification	This avoid repudiation in order to avoid situation of identity cross-using (e.g. Dottor X use identity of doctor Y)
Priority	HIGH
Version	1.0
Source	Workshop, Risk scenarios, Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_2**
Title	Centralized identification and authentication
Category	Product
Description	Within a distributed HC organization, identification and authentication of HC personnell should be able to be centralized
Justification	HC personnell can be identified and authenticated to HC systems with a single mean within the entire organization
Priority	MEDIUM
Version	1.0
Source	Workshop
User Involved	External Roles

ID	**TOP_IA_USER_NONFUN_3**
Title	Identification and Authentication transparency
Category	Product
Description	Authentication may be transparent for the users
Justification	Users can be facilitated in identification and authentication processes
Priority	LOW
Version	1.0
Source	Workshop
User Involved	External Roles

ID	**TOP_IA_USER_NONFUN_4**
Title	Safeguard of emergency
Category	Organizational

Description	Identification & Authentication shall not obstacolate operations related to emergency situations.
Justification	Safety of patients should be the first aim
Priority	HIGH
Version	1.0
Source	
User Involved	Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_5**
Title	Data exchange with Dynamic Risk Assessment
Category	Organizational
Description	Identification information of medical devices and HC personnell should be available to the activities of dynamic risk assessment
Justification	These information are potentially important for risk computation
Priority	MEDIUM
Version	1.0
Source	scenarios
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_6**
Title	Design principle
Category	Organizational
Description	Identification and authentication tools and processes shall be designed in accordance with Human-Centred Design principles and usability/HCI design standards
Justification	Reference to Identification and Authentication -these should be simple and easy to implement as part of normal working routines without adding burden distraction of complexity to Users tasks - particularly not in health care delivery roles. Effective HCD and usability are important to prevent 'workarounds' on identification and authentication being necessary 'to get the job done'
Priority	HIGH
Version	1.0
Source	Expert
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_7**
Title	Control Policy

Category	External
Description	An access control policy shall be established, documented and reviewed based on business information security requirements
Justification	Documentation about access policy is requested in order to verify its actuation
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_8**
Title	Accesses' distinction
Category	External
Description	Users shall only be provided with access to the network and network services that they have been specifically authorized to use
Justification	Segregation of duties permits not disclosure of information
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_9**
Title	Access rights
Category	External
Description	A formal user registration and de-registration process shall be implemented to enable assignment of access rights
Justification	This is important in order to implement the need-to-know principle
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_10**
Title	formal user provisioning process
Category	External

Description	Access rights introduced in TOP_IA_USER_NONFUN_9 shall be assigned and revoked via a formal user provisioning process. If the allocation of privileged access rights (ADMIN) is needed, it shall be restricted and controlled
Justification	Privileged access management is a critical point
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_11**
Title	Revision of access rights
Category	External
Description	User access rights shall be reviewed at regular intervals. Access rights shall be removed upon termination of employment
Justification	Access rights can change for example for internal changes. All these changes should be reflected on the access rights policy
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_12**
Title	Password management
Category	External
Description	Password management systems shall be interactive and shall ensure quality passwords.
Justification	Important to avoid the usage of weak passwords
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_13**
Title	Personal data management
Category	External

Description	Personal data for identification and authentication shall be limited to what is necessary in relation to the purposes for which they are processed
Justification	For the need to know principle, personnel shall know only the limited portion of information they need in order to proceed with their operations
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_14**
Title	Processing of personnel data
Category	External
Description	Processing of personnel data shall be lawful if: The subject agreed to the process; Processing is necessary for compliance with a legal obligation Processing is necessary in order to protect the vital interests Processing is necessary for the performance of a task carried out in the public interest
Justification	This in order to be compliant with GDPR
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_15**
Title	Authorization of data processing
Category	External
Description	Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
Justification	This in order to be compliant with GDPR
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_16**

Title	Data subject's rights
Category	External
Description	The data subject shall have the right to withdraw his or her consent at any time.
Justification	This in order to be compliant with GDPR
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_17**
Title	Minor's personal data
Category	External
Description	Whenever processing of personal data is requested for people below 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.
Justification	This in order to be compliant with GDPR
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_18**
Title	Processing of personal sensitive data
Category	External
Description	Processing of personal data revealing racial or ethnic origin, religious or philosophical beliefs, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only if: The data subject has given explicit consent Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent processing is necessary for reasons of substantial public interest Processing is necessary for the purposes of preventive or occupational medicine Processing is necessary for reasons of public interest in the area of public health
Justification	This in order to be compliant with GDPR
Priority	HIGH

Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IA_USER_NONFUN_19**
Title	Information non-required
Category	External
Description	If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject
Justification	This in order to be compliant with GDPR
Priority	HIGH
Version	1.0
Source	GDPR
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Security Behaviours Requirements

ID	**TOP_HF_USER_FUN_1**
Title	Integrated layered approch
Category	Functional
Description	Mechanism in the workplace shall support User cyber security behaviours through an integrated layered approach: - Optimising design of software, hardware and facilities for user-centred cyber security - Providing broader organisational/environmental behavioural nudges and performance support - Providing cyber security training (type and level tbd by training needs analysis) - Providing feedback on positive and negative cyber-security performance and consequences.
Justification	Human Factors approaches need to include features built into to the design of software and hardware that easily support security behaviour that are then reinforced by messages and support from the wider organisation and environment and with training - for those groups were training can be managed, i.e. not for patients.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_2**
Title	Training remainding

Category	Functional
Description	Mechanisms that remind training shall be implemented
Justification	Remaind of training in order to ensure that personnel follow it
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_3**
Title	Nudging
Category	Functional
Description	Mechanisms in the workplace which routinely remind and guide on cyber-security threats and processes shall be put in place
Justification	Sudgestion on the workplace supports a right behavior
Priority	HIGH
Version	1.0
Source	Experts, Risk scenarios
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_4**
Title	Simulation training
Category	Functional
Description	Users shall be involved in simulation and training in order to understand the risk of lackin cyber security.
Justification	Interaction and simulation are more engaging than lessons
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_5**
Title	Role segregation in training
Category	Functional
Description	Training shall be provided to the users according to their roles
Justification	Not all the roles in the organization have the same impact on cybersecurity
Priority	HIGH
Version	1.0
Source	Workshop

User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_6**
Title	Categories of training
Category	Functional
Description	In training, at least these roles shall be taken into account: Managers Health roles Non-Health roles External Roles
Justification	Not all the roles in the organization have the same impact on cybersecurity
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_7**
Title	Training repo
Category	Functional
Description	Training shall take into account the management of a common repository where maintain the training materials
Justification	A common repository permits to the users to reach the material in a easier way
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_FUN_8**
Title	Learning management system
Category	Functional
Description	Training shall take into account the management of a learining mamagement system in order to manage personnel training
Justification	This should permit to retrieve the status of the training done and other materials
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_FUN_9
Title	Statistics generation
Category	Functional
Description	Statistics about the staff misbehaving shall be generated in order to evaluate level of security
Justification	This is an indicator about the effectiveness of training
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_FUN_10
Title	Self assessment
Category	Functional
Description	Tools of self assessment may be provided to the personnel
Justification	Can be useful to personnel to test themselves
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_1
Title	Frequency of training
Category	Product
Description	Frequency on which users are sensitized shall be adequate respect with their responsibility.
Justification	Training and nudging should be done also based on duties of personnel.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles

ID	TOP_HF_USER_NONFUN_2
Title	Explaination
Category	Product
Description	Actions needed in order to correct behaviour of users should be also integrable in tools in order to force their activities.

Justification	Knowing consequences of actions prevents the lack in cyber security.
Priority	MEDIUM
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_3**
Title	Bring Your Own Device policies
Category	Organizational
Description	HCOs users shall be sensitized and supported on the usage of non-conventional tools and BYOD instead of approved/provided one.
Justification	This usage can lead to break laws (e.g. GDPR …)
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_5**
Title	Updates
Category	Organizational
Description	IT Departement users shall be sensitized on update of hardware and software.
Justification	Installation of update make the system more reliable and robust to cyber attaks
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_6**
Title	Backup needs
Category	Organizational
Description	IT Departement users shall be sensitized on creation and management of backup system.
Justification	Backup helps in business continuity procedures.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_7
Title	Default settings
Category	Organizational
Description	IT Departement users shall be sensitized on usage of default settings.
Justification	Settings of default are the first used by an attacker during an attack
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_8
Title	Password management
Category	Organizational
Description	Users shall be sensitized, supported and warned about processes of password management.
Justification	PANACEA end users should understand that the password is something to permit confidentiality and not disclosure of information
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_9
Title	E-mail risks awareness
Category	Organizational
Description	Users shall be sensitized and supported about the threats that can be derived from the mail (e.g. phishing, ransomware, virus …)
Justification	The most used vehicle to attack an organization is the e-mail.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_10
Title	Unattendance of devices
Category	Organizational
Description	Users shall be sensitized and supported about devices unattending

Justification	It is needed to take some particular precautions when device are left unattended
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_11**
Title	Users contribute
Category	Organizational
Description	Users shall be sensitized on the importance of their contribution in supporting cyber security.
Justification	Cyber security is not something we can demand to other. Cyber Security level depends from the weakest part.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_12**
Title	Consequences awareness
Category	Organizational
Description	Users shall be sensitized about the consequences of lack in cyber security. This shall be tailored on their daily work.
Justification	Knowing consequences of actions prevents the lack in cyber security.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_13**
Title	Cyber-security in real processes
Category	Organizational

Description	Training on cyber security shall be provided to HCO operative personnel at least at the following processes: Hospital workflows Inter-hospital medical consultations Territorial workflows Cross-border exchange of patient related data Emergency pre-hospital workflows
Justification	It is important to identify cyber-security countermeasures in organization's real processes
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_14**
Title	Cyber-security in real processes
Category	Organizational
Description	Training on cyber security shall be provided to HCO IT and administrative personnel at least at the following processes: Patient billing Human resources (not payroll) Human resources (payroll) Procurement Accounting Information and Communication Technology Facility management Critical infrastructure Incident management
Justification	It is important to identify cyber-security countermeasures in organization's real processes
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_15**
Title	Continuous improvement awareness
Category	Organizational
Description	Users that provide medical devices shall be sensitized about continuous improvement in efficiency of their devices in order to provide update / upgrade of hardware and software.

Justification	The continuous improvement lead to discovery bug and fix them in order to create more reliable devices
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_15**
Title	Recognised Behavioural Change Approaches
Category	Organizational
Description	PANACEA behavioural tools to support users' cyber-security shall be designed in accordance with recognised behavioural change approaches and following Human-Centred Design principles.
Justification	This refers to tools for health roles, managers and non-health roles who are not ICT/cyber security professional. Depending on the specific behaviour to be changed different approaches will be explored but all must be developed in the context of user roles and tasks.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	**TOP_HF_USER_NONFUN_16**
Title	Human-Centred Design principles
Category	Organizational
Description	Security features on medical devices shall be designed in accordance with Human-Centred Design principles and usability/HCI design standards
Justification	Reference to Security by Design Certification - security features should not interfere with overall device usability and should support users in remaining secure whist integrating with the device. Usability is important to prevent 'workaround' on security features
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_17
Title	Clear Desk policies
Category	External
Description	A clear desk and clear screen policy shall be adopted by the personnel in order to avoid disclosure of information
Justification	Hiding information is the first step for non disclosure
Priority	MEDIUM
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_17
Title	Guarantee of competences
Category	External
Description	Organisation shall determine the necessary competences of the personnel for each role involved in cyber security and ensure that the personnel is competent on the basis of proper education, training or experience
Justification	Hiding information is the first step for non disclosure
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_17
Title	Personnel competence as documented information
Category	External
Description	Competence of personnel should be available as a documented information and properly retained
Justification	Competent personnel is important in order to achieve organization's objectives
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_17
Title	Education and training
Category	External

Description	All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training as relevant for their job function
Justification	Competent personnel is important in order to achieve organization's objectives
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-health roles, External Roles

ID	TOP_HF_USER_NONFUN_18
Title	Communication of documented procedures
Category	External
Description	All the documented procedures shall be communicated to all the interested parts
Justification	Dissemination of procedures is the only way to perform process correctly
Priority	HIGH
Version	1.0
Source	ISO27001
User Involved	Managers, Health Roles, Non-health roles, External Roles

Governance Requirements

ID	TOP_GOV_USER_FUN_1
Title	Security Governance model
Category	Functional
Description	A PANACEA CyberSecurity Governance toolkit, able to assess the Cybersecurity Governance (Information Security Management System, ISMS) in relationship with actual standards (ISO27k,NIST,COBIT,etc) shall be provided to end users
Justification	A cybersecurity governance tool should be available to end users in order to assess their governance under the cybersecurity aspect and should be alligned to the most common standards
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	TOP_GOV_USER_FUN_2
Title	Security Governance model Metrics
Category	Functional
Description	The CyberSecurity Governace toolkit shall be able to provide indications about status and gaps of roles, procedures and policies of the cybersecurity Governance.

Justification	The cybersecurity governance should support end users defining roles and procedures
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_3**
Title	Security Governance Outcomes
Category	Functional
Description	The Cybersecurity Governance toolkit shall take into account security Roles, Procedures, Policy, Users and Assets taken into account by the cyber risks assessment
Justification	The cybersecurity governance should support end users defining roles and procedures also taking into account cyber risk assessment
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_4**
Title	Security Governance external integrations
Category	Functional
Description	The CyberSecurity Governace toolkit shall be able to map security roles and users and the assets involved in cyber incident management
Justification	A map between users and assets is recommended by all the most important regulations
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_5**
Title	Ad-hoc task force
Category	Functional
Description	An ad-hoc task force reporting to the head of HCO shall be described in the Cybersecurity Governance toolkit in order to manage critical cyber security incident situations affecting the processes of the HCO
Justification	A task force composed from heterogeneus personnel can be useful to solve critical solution
Priority	HIGH

Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_6**
Title	Review of ISMS
Category	Functional
Description	CyberSecurity Governace toolkit shall support top management in reviewing the ISMS at planned intervals
Justification	In planned periods the ISMS should be reviewed in order to understand if changes are needed
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_7**
Title	Continuos improvement
Category	Functional
Description	CyberSecurity Governace toolkit shall support the HC organization by continually improve the suitability, adequacy and effectiveness of the information security management system
Justification	Follow the principle of continuous improvement
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_8**
Title	Changes assessment
Category	Functional
Description	CyberSecurity Governace toolkit shall support the HC organization by assessing every change with an impact on information security
Justification	Changes can have positive or negative impact. It should be evaluated
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers, Health Roles, Non-Health Roles

ID	**TOP_GOV_USER_FUN_9**

Title	Documented information
Category	Functional
Description	CyberSecurity Governace toolkit shall take into account which should be the documented information
Justification	This permit to make training and awareness in the HCO
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Manager, Non-Health Roles

ID	**TOP_GOV_USER_FUN_10**
Title	Communication channel definition
Category	Functional
Description	CyberSecurity Governace toolkit shall support HCOs on defining procedures for providing notification to the appropriate regulatory authorities about complaints, adverse events or issuance of advisory notices.
Justification	Channel with appropriate regulatory authorities should be put in place
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Manager, Non-Health Roles

ID	**TOP_GOV_USER_FUN_11**
Title	CyberSecurity Governace sub-model
Category	Functional
Description	CyberSecurity Governance toolkit shall be structured to assess the information security management system of the HCO organization on the following areas: Identification capability area; Protection capability Area; Detection capability Area; Respond capability Area; Recovery capability area
Justification	Let to describe the cyber security Governace in 5 coordinations that are able to cover horizzontally the Organization
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Manager, Non-Health Roles

ID	**TOP_GOV_USER_NONFUN_1**
Title	Interdepartement process
Category	Product
Description	Cyber-security governance shall be managed as an interdepartement process
Justification	Governance is a process that engage different disciplines

Priority	HIGH
Version	1.0
Source	Workshop, Experts
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

Cyber-security Value Assessment Requirements

ID	TOP_VAL_USER_FUN_1
Title	Value assessment methodology
Category	Functional
Description	The PANACEA toolkit (delivery aspect) shall encompass a value assessment methodology to evaluate the return of investment due to the deployment of the solution aspect (or a subset of its components).
Justification	The PANACEA toolkit is composed by a solution aspect (including the tools of the toolkit) and a delivery aspect, detailing how to deploy ad validate the solution aspect in the HC organization.
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers

ID	TOP_VAL_USER_FUN_2
Title	Depreciation of investment
Category	Functional
Description	The value assessment methodology shall take into consideration the depreciation of the investment
Justification	One of the index for an investment assessment is the depreciation
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers

ID	TOP_VAL_USER_FUN_3
Title	Budget for cyber security
Category	Functional
Description	The value assessment methodology shall permit to insert the yearly budget allocated for cyber security
Justification	The yearly budget may introduces a ceiling to the budget for the mitigation actions that can be implemented; this may have an impact on the security level that can be actually achieved
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_VAL_USER_FUN_4
Title	Size of attack
Category	Functional
Description	The value assessment methodology shall take into account the expected magnitude and impact of the cyber attacks
Justification	Relationship between value and size of attack to contrast could be useful in order to decide to invest.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_VAL_USER_FUN_5
Title	Impact from past attacks
Category	Functional
Description	The value assessment methodology shall be able to consider also impact of past cyber attacks
Justification	Past attacks is the base knowledge in order to evaluate the solution
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_VAL_USER_FUN_6
Title	Time to recover
Category	Functional
Description	The value assessment methodology shall be able to consider also the time to recover after a cyber attack.
Justification	The time of recover can support the value of the solution. The faster the more valuable
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_VAL_USER_FUN_7
Title	Mitigation activities
Category	Functional
Description	The value assessment methodology shall be able to take into account ongoing and planned mitigation activities

Justification	Which is the cost of each mitigation action is an index about the investment to sustain
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	**TOP_VAL_USER_FUN_8**
Title	Minimal configuration
Category	Functional
Description	The value assessment methodology shall take into account the minimum functionalities needed to the hospital in order to be defined as operative
Justification	During the assessment of the value for a solution, it is needed to take into account the minimum functionalities organization wants to guarantee in order to defend at least those.
Priority	HIGH
Version	1.0
Source	Experts, Risk scenarios
User Involved	Managers

ID	**TOP_VAL_USER_NONFUN_1**
Title	Minimal indicators for assessment
Category	Product
Description	Assessment of the added value brought by a component of the PANACEA toolkit in the HC organization shall be based at least from the following indicators: Costs Impact on Patients Activities to be performed Impact on the existing infrastructure
Justification	These were the most important indicators provided by the stakeholders during the 1st End Users and Stakeholders Workshop.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	**TOP_VAL_USER_NONFUN_2**
Title	Minimum investment time horizon
Category	Product

Description	The time horizon over which the investment should be evaluated is 5 years
Justification	N.A.
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers

ID	**TOP_VAL_USER_NONFUN_3**
Title	Results showing
Category	Product
Description	The value assessment methodology should encompass the definition of guidelines for properly reporting to decision makers the evaluation of the value assessment
Justification	Decision makers in general are not thechnical people; appropriate language must be used with them. A good starting point, for instance, is to "tell the story" of the last important cyberattack
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers

ID	**TOP_VAL_USER_NONFUN_4**
Title	Future scenarios
Category	Product
Description	The methodology should recommend methods for identifying the future scenarios of cyberattacks, in which the investment is expected to operate.
Justification	Scenario bulding is a key success factor of the methodology, because the impact (financial and non-finsncial) of the investment is evaluated in the future. "Open mind approach" helps in capturing scenarios that may emerge in the future. A "foresight exercise", based on a PEST-SEH (Political, Economic, Societal, Technological, Security, Environmental, Healthcare trends); in the S (security) emrging type of attack shuld be considered (for intance, nowadays the hybrid threats coud be considered)
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers

ID	**TOP_VAL_USER_NONFUN_5**
Title	Budgeting and investment
Category	Product

Description	The value assessment should consider the rules/criteria for budgeting and investmment decisions in place for the public healthcare providers in the country
Justification	N.A.
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Managers

Cyber-security Solutions Implementation Requirements

ID	TOP_IMP_USER_FUN_1
Title	Implementation guidelines
Category	Functional
Description	The PANACEA toolkit (delivery aspect) shall encompass implementation guidelines for the solution aspect of the toolkit
Justification	The PANACEA toolkit is composed by a solution aspect (including the tools of the toolkit) and a delivery aspect, detailing how to deploy ad validate the solution aspect in the HC organization.
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_IMP_USER_FUN_2
Title	Initial Assessment
Category	Functional
Description	As part of the implementation guidelines, an initial assessment of security level of the HCO shall be included.
Justification	The initial assessment permits to understand the environment in which PANACEA will operate and the level of security ensured without PANACEA
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_IMP_USER_FUN_3
Title	Existent Solution
Category	Functional
Description	As part of the implementation guidelines, an evaluation of the existing cyber-security tools and products in the HCO shall be included.
Justification	The initial evaluation of existent security solutions already implemented by the organization permits to understand how to integrate the PANACEA solution with the already existent tools
Priority	HIGH
Version	1.0

Source	Workshop
User Involved	Managers, Non-Health Roles

ID	**TOP_IMP_USER_FUN_4**
Title	Installation guide
Category	Functional
Description	The PANACEA toolkit implementation guidelines shall detail the installation of the components of the toolkit in the HCO.
Justification	A support foe installation is mandatory
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Non-Health Roles

ID	**TOP_IMP_USER_FUN_5**
Title	Validation period
Category	Functional
Description	As part of the implementation guidelines, a period of validation shall be foreseen for the PANACEA toolkit (solution aspect)
Justification	During this period it is possible to verify the effectiveness of PANACEA and of the integration with other solutions
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers, Health Roles, Non-Health Roles, External Roles

ID	**TOP_IMP_USER_NONFUN_1**
Title	Indexes supporting assessment
Category	Product
Description	Initial Assessment shall be done by considering at least the following indexes: Vision Asset Inventory Resistance to change
Justification	Definition of indexes in order to evaluate the progress of the solution is of vital importance
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	**TOP_IMP_USER_NONFUN_2**
Title	Assessment indexes for evaluation
Category	Product

Description	The evaluation of the existing cyber-security tools and product shall at least consider the following indexes: Financial Actual IT architecture Criticality of department
Justification	Definition of indexes in order to evaluate the progress of the solution is of vital importance
Priority	HIGH
Version	1.0
Source	Workshop
User Involved	Managers

ID	TOP_IMP_USER_NONFUN_3
Title	Implementation logic
Category	Product
Description	The implementation guidelines should consider two possible options for the implementation logic: a waterfall logic, an agile logic.
Justification	These are the most usable logic for implementation
Priority	MEDIUM
Version	1.0
Source	Experts
User Involved	Manager, Non-Health Roles, External Roles

ID	TOP_IMP_USER_NONFUN_4
Title	Culture in healthcare
Category	Product
Description	The change management thread of activity of the implementation guidelines should consider the different types of culture that can be found in a healthcare provider; a key dinstinction, for instance, is between staff with "work hours" mentality (e.g. administrative staff) and staff with "shifts" mentality.
Justification	Activities should be dimensioned based on different aspects. Among these, work hours is a good aspect
Priority	HIGH
Version	1.0
Source	Experts
User Involved	Managers

ID	TOP_IMP_USER_NONFUN_5
Title	Minimum documentation available
Category	External

Description	In order to provide a quality system, documentation of the implementation guidelines shall include: a manual documented procedures and records; other documentation specified by applicable regulatory requirements.
Justification	Basic documentation to provide after solution release for quality systems
Priority	HIGH
Version	1.0
Source	EN ISO 13485
User Involved	Managers

END OF DOCUMENT