Panacea
People-centric cybersecurity in healthcare

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

D9.3DATA MANAGEMENT PLAN

Work Package	WP9 PROJECT MANAGEMENT
Lead author	Lorenzo Marchesi (UCSC), Saverio Caruso UCSC), Fabio Rizzoni (FPG)
Contributors	Monica Bernassola (UCSC), Laura Motta (UCSC)
Peer reviewers	Emmanouil Spanakis (FORTH), Vangelis Sakkalis (FORTH), Matteo Merialdo (RHEA)
Version	V1.0
Due Date	30/06/2019
Submission Date	30/06/2019

Dissemination Level:

X	PU: Public
	CO: Confidential, only for members of the consortium (including the Commission)
	EU-RES.Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)
	EU-CON. Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)
	EU-SEC. Classified Information: SECRET UE (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 R01	19/06/2019	Lorenzo Marchesi (UCSC), Saverio Caruso UCSC), Monica Bernassola (UCSC), Laura Motta (UCSC), Fabio Rizzoni (UCSC)	Development of V01 R01
0.1 R02	30/06/2019	Emmanouil Spanakis (FORTH), Vangelis Sakkalis (FORTH), Matteo Merialdo (RHEA)	Review/comments to V01 R01
0.1 R03	30/06/2019	Lorenzo Marchesi (UCSC), Saverio Caruso (UCSC), Daniele Gui (UCSC)	Development of V01R03 after peer review

List of Contributors

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

Section	Author(s)
All	UCSC, FPG

Keywords

INFORMED CONSENT, PRIVACY STATEMENT, ANONYMIZATION, FURTHER PROCESSING OF PERSONAL DATA, SECURITY MEASURES, DATA PROTECTION, GDPR, FAIR, METADATA, INTEROPERABLE, ACCESSIBLE, FINDABLE

Disclaimer

This document contains information which is proprietary to the PANACEA consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or parts, except with the prior written consent of the PANACEA consortium.

Executive Summary

This Deliverable was written following the structure of the H2020 DMP template (http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm).

In the framework of the rapid evolution of health systems towards digitalization, the PANACEA Project is focused on strengthening awareness of cyber vulnerabilities delivering a Dynamic Risk Management Platform; through a series of toolkits (Solution toolkit and Delivery toolkit) and field demonstrations in an emulated environment, the PANACEA Project will enable healthcare facilities to assess the nature and severity of a cyber-threat, and sustainably decide to adopt strategies to strengthen preparedness and response.

This deliverable is centred on:

which categories of data will be collected or processed by the Panacea Project, how they will be processed and protected through the compliance with recognized standards and Regulations. Different options are indicated as to which data sets will be chosen for the emulated environments as the requirements unfold (e.g. previously collected data, mock data generated by an algorithm, data specifically collected etc.).

How FAIR - findability, accessibility, interoperability, and reusability principles will be applied through: the Open Science Policy Platform OSSP recommendations (findability); Zenodo and B2Share channels (accessibility); outputs resulting as publicly available for further research and scientific publications in formats commonly used such as JSON or XML (interoperability); licensing of data not protected by other IPRs through Creative Commons (CC), will be either CC-0 (public domain) or CC-BY (attribution) (re-use).

Data security is focused on two categories of data: security of dataflow and data used to validate the toolkits (the data fed into the emulated environments for the validation processes) and the security of the personal data related to Project workshops (contact information and feedbacks from stakeholders/end-users such as questionnaires). More details are provided in D10.1 (dissemination level “Confidential”),

Where ethical aspects are concerned, relevant reference deliverables are indicated.

Table of Contents

1. Introduction

1.1 Purpose

This deliverable (D9.3 Data Management Plan) describes how, in the framework of the PANACEA Project, data will be handled, protected and made available according to the FAIR principles and circulated within the Consortium. Its dissemination level is public. The sections dedicated to data security and ethical aspects are also considered in D10.1 which, to the contrary, is set as dissemination level “Confidential, for Consortium members only and Commission services”. For this reason, some aspects from D9.3 which are not intended for public dissemination, will not be included. As will be explained in the following sections, complete definition of the data which will be used in the toolkit demonstration is not yet available at the time of writing, because it is part of a process which is still unfolding in the scenario and requirements development phase. For these reasons, an update of the Data Management Plan will be necessary as the technical analysis unfolds.

1.2 About PANACEA

Healthcare is increasingly evolving towards digitalisation: from the development of electronic health records, of teleconsultation and tele-expertise is thriving and connected objects are on the rise. It is evident that threats and potential damages to healthcare critical infrastructures due to cyberattacks require a fortification of the security features in the industry.

The PANACEA Research & Innovation Action, referred to as PANACEA, will be the field demonstration that security stems from awareness of cyber vulnerabilities, enabling healthcare facilities to assess the nature and severity of a threat, and sustainably decide to adopt strategies to strengthen its preparedness and response.

PANACEA will deliver a Dynamic Risk Management Platform, analysing the risk of the IT infrastructure leveraging the healthcare processes. The Secure Information Sharing Platform will manage information sharing between healthcare organizations, multi-tenant and cross boundaries.

On one hand, PANACEA will address the need to respond swiftly to a complex, multi-faceted cyber threat landscape, on the other hand, it will address the need for highly-skilled cybersecurity professionals to help reduce cyber risks in healthcare.

As general impacts, PANACEA looks to:

- Reinforce Europe’s position as a key security provider for Healthcare IT systems;
- Allow for a continued development and improvement of fully tailored identity management and secure data management solutions for Healthcare;
- Proceed with the development of new prototypes to improve the security of IT infrastructures leveraging the healthcare processes;
- Accelerate its growth in the Healthcare ecosystem to attract more customers and to increase its market share with the target to reach $2bn revenues by 2020;
- Extend and reinforce its European network of stakeholders and decision makers

1.2.1 Objectives and outcomes

PANACEA delivers two toolkits for **cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices**:

- The PANACEA **Solution Toolkit** (made up of 4 technological tools and 3 organizational tools) and
- The PANACEA **Delivery Toolkit** (made up of 2 support tools).

The technical tools of the toolkit will be demonstrated on relevant environments (Technology Readiness Level 6) and will benefit from ambitious research goals, achieved by moving beyond the current state of the art in strategic areas such as:

- **Dynamic risk assessment & mitigation** (threat modelling, attack modelling, response management through technical and non-technical security measures, visual analytics);
- **Blockchain**for secure information sharing of healthcare data;
- **Identification & authentication** (cryptographic authentication protocols, biometric recognition/digital identity, IoMT identification);
- **Security-by-design** methods and tools for healthcare systems and software;
- **Secure behaviours decision models** and influencers.

Three end-user scenarios, developed in Italy, Crete and Ireland, will provide a solid test-bed.

The PANACEA main objectives are listed below:

- Objective 1: Develop and validate tools for dynamic risk assessment and mitigation
- Objective 2: Develop and validate tools for Secure Information Sharing
- Objective 3: Develop and validate tools for System Security-by-design and certification
- Objective 4: Develop and validate tools for identification and authentication
- Objective 5: Develop and validate an educational package for cybersecurity in the health sector
- Objective 6: Develop and validate tools for resilience governance
- Objective 7: Develop tools for secure behaviours nudging
- Objective 8: Develop and validate Implementation Guidelines for cybersecurity solutions adoption
- Objective 9: Develop and validate a Security-ROI methodology
- Objective 10: Engage a representative community of stakeholders and identify a sustainability path for the PANACEA vision

1.2.2 Use cases

PANACEA offers a significant improvement in multiple areas (from threat awareness to security-by-design and secure information sharing).

However, results can only be measured in the context of realistic data, use cases and scenarios. At the same time it is not possible to rely on the operational IT infrastructure of the hospitals for research, development and testing activities, due to their criticality. For this reason, the consortium will adopt the use of emulation environments based on a set of heterogeneous user scenarios developed by End Users and relevant for their businesses.

The User Scenarios will be hosted by three end-users in Italy, Crete and Ireland and will be elicited in order to give the consortium a wide potential dataset representing different networks and organisations, heterogeneous threats and incidents situations.

User scenarios have a critical importance for the development, test and validation of the PANACEA toolkit: using virtualization techniques on private cloud environments, fractions of the end users IT infrastructures will be virtualized and emulated in order to create a safe virtual environment with affinity to the operational but fully available for testing and validation. User scenarios will be hence fundamental in order to understand how the emulation environments will need to be composed.
User Scenarios will be detailed in deliverable D1.4 (31 September 2019).

1.2.3 Innovations

PANACEA research will deliver two toolkits for cyber security assessment and preparedness of Healthcare ICT infrastructures and connected devices: the Solution Toolkit and the Delivery Toolkit.

1- The **Solution Toolkit** will positively affect the cybersecurity of a Healthcare Centre (HCC) according to a holistic modality, assessing (and acting on) the physical, software and organizational/human components of the HCC, relevant for the cybersecurity.
It is composed of four technological tools:

- a dynamic risk assessment & mitigation tool (helping to perform risk assessment evaluation and mitigation measures)
- a secure information sharing tool for the protection of data
- a security-by-design & certification tool
- a tool for identification & authentication

Moreover, it comprises three organizational tools:

- a tool composed by models, guidelines and best practices for training & education
- a tool aimed at resilience governance
- a tool for secure behaviours nudging

How does the Solution Toolkit effectively interact with the Healthcare Center components?
Each component of the Solution Toolkit, can be implemented and used separately by the management and the security staff of the healthcare center. Once implemented, they operate by protecting an ecosystem made up of a variety of components, as for example:

- The Healthcare Center network composed of operators, patients, citizens, security staff, medical doctors, nurses, top management, employees and administrative staff.
- The clinical information systems and related processes (EHP, PHR)
- The administrative information systems
- The connected devices used in and outside of the hospital

The Solution Toolkit also manages the connections with other HCCs, even when this HCCs are not adopting PANACEA research's solutions (these are represented on the right).

2. The **Delivery Toolkit** is conceived as a support for the adoption of the Solution Toolkit. It involves two support tools:

- a methodology to evaluate the Return of Investment (ROI) of cybersecurity interventions, therefore the advantages of following a cybersecurity approach in an Healthcare Center
- a set of guidelines to be applied for the adoption of the Solution Toolkit

PANACEA research follows two Innovative approaches:

1) A Holistic approach to cybersecurity: the underlying paradigm of PANACEA research is that real improvement in the domain of cybersecurity can only come from change to human behaviour, technology and processes as part of a holistic solution; the Toolkit contains all these ingredients; and the project is structured to allow their codesign and the strict collaboration between end-users and researchers/developers

2) An Impact oriented approach: the Consortium has put itself in the shoes of the public health decision makers and of the HCC managers, as prospect users of PANACEA research, and has decided not only to design effective solutions, but also to make them easy to adopt.

The PANACEA research Toolkit is expected to be used for prevention purposes. The toolkit helps the HCC to proactively protect the IT infrastructure. It does not include an incident management component. The Consortium considers that existing technical and organizational solutions already cover the incident management/response phase and assumes that to invest in preparedness reduces the likelihood and criticality of the incidents to a level that ensures an overall positive return.

1.3 Quality assurance

1.3.1 Quality criteria

The QA in the PANACEA project relies on the assessment of a work product (i.e. deliverable) according to lists of QA checks (QA checklists – [QAPeer]) established with the QAM, validated at a project management level and centralized in the [PMP].

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

- PEER REVIEW (PR) QA CHECKLIST [QAPeer]: this deliverable is a report, it then requires a proper peer review according to the checks defined in this checklist;

1.3.2 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 [PMP]. The QA validation process is scheduled in the QA Schedule [QASchedule] managed by the QAM.

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
[PMP]	PANACEA Project Management Plan		0.5	01/01/2019
[QAPeer]	PANACEA Peer Review QA Checklist		0.5	01/01/2019
[QAReqs]	PANACEA Requirements Review QA Checklist		0.5	01/01/2019
[QASchedule]	PANACEA QA Schedule		0.5	01/01/2019

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
Grant Agreement	Annex 1 – Description of Action – Part A	Ref. Ares(2018)5691185 - 07/11/2018		07/11/2018
Grant	Annex 1 –	Ref. Ares(2018)5691185		07/11/2018

Reference	Document Title	Document Reference	Version	Date
Agreement	Description of Action – Part B	- 07/11/2018		
Horizon 2020 offical DMP template	TEMPLATE HORIZON 2020 DATA MANAGEMENT PLAN (DMP)		01	13/10/2016
GDPR	Reg. 2016/679 General Data Protection Regulation	https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679		
FAIR	The FAIR Guiding Principles for scientific data management and stewardship (Wilkinson M.D., Dumontier M. et alia	Scientific Data volume 3, Article number: 160018 (2016)https://www.nature.com/articles/sdata201618		2016
DMP	Horizon 2020 FAIR Data Management Plan (DMP) template	http://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/open-access-data-management/data-management_en.htm		

Table 2: Reference Documents

3. Glossary of Acronyms

Acronym	Description
DMP	Data Management Plan
Dx.x	Deliverable number x.x
FAIR	Findable, Accessible, Interoperable, Re-usable
GA	Grant Agreement
GDPR	General Data Protection Regulation (Reg. 2016/679)
WP	WorkPackage

Table 3. Table of acronyms

4. Data summary

The purpose of the data collection/generation and processing in the PANACEA framework is instrumental to the objectives of the Project. The types of data collected can be divided in groups:

1. Collection of contact information (name, e-mail, phone, affiliation, professional details) from Partners’ staff for the purpose of internal communications, project activities and registration in PANACEA meetings and events;
2. Collection of information (name, e-mail, phone, affiliation, professional details) from stakeholders and experts for communications regarding workshops, training course and registration in PANACEA Platforms and events;
3. Collection of technical and scientific inputs and opinions from end-users and stakeholders in the framework of PANACEA’s purposes, mainly on Healthcare system gaps, vulnerabilities and viable fixes. This activity aims at collecting information on different healthcare models, structures and procedures and eventually on gaps that need to be filled;
4. Collection of data regarding the 3 Use Cases IT infrastructure, necessary to simulate part of them in the emulation environments PANACEA will build for the development and validation of the toolkit. IP addresses, networks structure, users (healthcare personnel or patients), installed applications and existing vulnerabilities will be analysed in order to understand which sections of the infrastructures will be emulated;
5. Collection of biometric data of healthcare personnel for the Identity Management Platform (full details on D10.1) – in any case, the scope of the Platform is to be applied only to healthcare personnel;
6. Collection of healthcare patients’ record data to test the Secure Information Sharing Platform;
7. Collection of data on behavioural patterns of selected staff to assess their awareness of cyber-risks;
8. Collection of information from stakeholders and beneficiary staff on problems and issues related to their experience on the field and on lessons learnt.

In relationship to previous items 4, 5, 6 and 7, personal data of healthcare personnel or patients will be involved. In order to deal with these personal data, several options will be explored:

- Personal “sensitive” data of healthcare personnel or patients collected, or previously collected, by the validation and demonstration host organizations (the three Use Case)will be anonymized with FORTH provided technology and software directly on the premises of the three Use Cases;
- Personal “sensitive” data of healthcare personnel or patients collected, or previously collected, by the validation and demonstration host organizations (the three Use Cases) anonymized with FORTH provided technology and software on the FORTH premises;
- Personal “sensitive” data of healthcare personnel or patients collected, or previously collected, by the validation and demonstration host organizations (the three Use Cases)and anonymized internally by each of the organization;
- Personal “sensitive” data collected from data subjects who have expressly consented to the collection and processing of their data for the purposes of the PANACEA project (this strategy will be probably adopted for the biometric data to test and validate the Identity Management Platform);
- Personal data created expressly by an algorithm generating mock data to be fed into the emulated environments (no real personal data would be used in the development of toolkits and in the validation and demonstration activities) or using test data already available in the three Use Cases;

The **personal “sensitive” data** referred to is constituted by patients’ health records and by healthcare personnel user/biometric data which should populate, realistically, the emulated environments.

The quantity and quality of the data to be fed, and how it will be processed, will be more precisely defined once the emulation environments are at a more advanced phase, in particular when the Validation Plan and the Emulation Environments are developed. The information still to be defined at a later stage includes the types of formats the project will collect or generate, the size of the data.

The **personal data of end-users and stakeholders** will be used only for PANACEA project purposes: the informed consent for the collection and processing (contact data and technical/scientific information or opinions) is given by these data subjects for the mentioned purposes. Nonetheless the information contained in Deliverables with a public dissemination level will be available.

In case the anonymization strategy will be adopted, a combination of Randomization and Generalization techniques is proposed. In compliance with the guidelines of Health Information Portability and Accountability Act (HIPAA) the following eighteen categories of Protected Health Information (PHI) in the HIPAA Privacy Rule “Safe Harbor” standard1 (https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf) will be removed or generalized:

- First and last names of patients;
- Geographic locations;
- All elements of dates (except year) for dates directly related to an individual;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

5. FAIR Data

The PANACEA Project has opted out of the Open Pilot on Open Research Data in Horizon 2020 for incompatibility with privacy/data protection. Nonetheless the Consortium will recur to given channels in order to adhere to FAIR principles. Only the data which has a public dissemination level will be made available outside the Consortium (including Stakeholder platform members, External Ethics Review Members) and Commission staff or appointed experts linked to the implementation of the Grant Agreement or review activities.

5.1 Making data findable, including provisions for metadata

The Consortium is committed to making data findable. PANACEA complies with the principal priorities laid out by the Open Science Policy Platform OSSP recommendations (https://ec.europa.eu/research/openscience/index.cfm?pg=open-science-policy-platform), one of the core eight areas is linked with Research Indicators that confirm that data, metadata and methods that are relevant to research evaluation, including but not limited to citations, downloads and other potential indicators or academic re-use will be publicly available for independent scrutiny and analysis by researches, institutions, funder and other stakeholders.

[1] Office for Civil Rights (OCR). "Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule." (2012).

The website will be maintained, also from the content point of view, keeping in mind the best practices in terms of SEO. Metatag, keywords and other traditional means of SEO are nowadays not sufficient for optimal positioning with the main search engines

5.2 Making data openly accessible

Publications and public deliverables will be made openly accessible through dissemination and communication activities.

At the time of writing, the channels identified for making PANACEA scientific publications openly are ZENODO (https://zenodo.org/) or B2Share (https://b2share.eudat.eu/) unless identified as potentially exploitable outputs.

The following channels enabling data accessibility are fully described in D8.2 “Communication and dissemination: strategy and achievements, 1st version” which has a public dissemination level:

- Website
- Social media and Professional Networks
- Promotional material
- Videos
- Press Releases and Announcements
- Events (physical and virtual, e.g. webinars)
- Traditional media
- Other channels

The deliverables which have a public dissemination level, once approved by the European Commission, will be publicly accessible on https://cordis.europa.eu/projects selecting the appropriate filters.

The PANACEA deliverables with public dissemination level are:

Deliverable	Deliverable title	Due month	Dissemination level
D1.1	Models of health services and of medical device lifecycle for cybersecurity	M4	Public
D1.2	Panacea User Requirements	M7	Public
D2.1	Analysis of cyber vulnerabilities and SoA countermeasures in HCC	M7	Public
D2.2	Human Factors, Threat Models Analysis and Risk Quantification in HCC	M12	Public
D2.3	Advanced Response Methods	M15	Public
D2.4	Secure information sharing, interconnectivity, cloud, authentication and interoperability aspects	M15	Public
D3.3	Dynamic Risk Management Platform High-Level Design - Update	M15	Public
D3.4	Secure Information Sharing Platform HighLevel Design - Update	M15	Public
D3.13	Dynamic Risk Management Platform and Secure Information Sharing Platform Verification Plan	M20	Public
D3.14	Dynamic Risk Management Platform and Secure Information Sharing Platform Verification Report	M24	Public
D7.4	White paper: lessons learnt from PANACEA project and recommendations for the cyber-protection of hospitals and care centres	M35	Public
D8.1	PANACEA Security Framework for Hospitals and care	M36	Public

	centres		
D8.2	Communication and dissemination: strategy and achievements, 1st version	M5	Public
D8.3	Communication and dissemination: strategy and achievements, intermediate version	M18	Public
D8.4	Communication and dissemination: strategy and achievements, final version	M30	Public
D9.3	Data Management Plan	M6	Public

Table 4: Public deliverables

5.3 Making data interoperable

The interoperability for inputs and outputs of the toolkits will be identified by language (definitions) and format (logical). At the time of writing, specific standards have yet to be identified in the light of the architecture of the toolkits under development and inclusion of requirements’ analysis. It is the aim of the Consortium to define interoperability criteria as development unfolds. Any output resulting as publicly available for further research and scientific publications will, if technically possible, be in formats commonly used such as JSON or XML.

5.4 Increase data re-use (through clarifying licences)

Licensing of any data not otherwise protected by other IPRs will be done through Creative Commons (CC) where reuse will be either CC-0 (public domain) or CC-BY (attribution) wherever possible. However, due to the nature of the studies and of the data, there will be restrictions made in some cases:

- Approval will be sought from institutional Ethical Board when required by European or national regulatory
- Reusability of health data collected in routine care of individuals requires internal procedures of healthcare providers according to the legal frameworks of health and biomedical research
- In many cases, authorized access to data will be limited to researchers who are listed and accepted in the authorization request, whether anonymised or not.

6. Allocation of resources

For the costs to be incurred in (staff or other structural or service costs) the Consortium will rely on the budget allocated by the Grant Agreement.

7. Data security

Data Security characteristics relevant for the PANACEA project can be categorized in two main types:

- security of dataflow and data used to validate the toolkits (the data fed into the emulated environments for the validation processes – items 4, 5, 6 and 7 in Section 4);
- security of the personal data related to Project activities (contact information and feedbacks from stakeholders/end-users, items 1 and 2 in Section 4).

The first type refers to data collected by medical devices, biometric devices and medical systems/databases in the context of the emulation environments built for the development and the validation of the toolkit. As stated in Section 4, any patient or healthcare personnel data to be used to develop or validate the toolkit will be treated (anonymized, mocked-up or explicit consent will be requested). Data will be stored in the emulation environments built by the Consortium and hosted, in-site, within RHEA and FPG premises (at the moment of writing, it is still to be understood if the emulation environments will also be hosted by other Consortium entities, for example the other end users). The emulation environments will be based on RHEA’s CITEF platform (Cyber-security Integration, Test and Evaluation Framework, developed within the CSCE program for the European Space Agency, https://artes.esa.int/projects/csce). CITEF offers full segregation of any element the emulated environments, while VPN connections will be offered to PANACEA partners in order to connect and use the environments during the development phases. CITEF also allow physical appliances (medical devices, biometric tools) to be connected to the virtual emulation environments: this will allow PANACEA team to full test and validate the output of the project.

Where the second type is concerned, data security is aimed at protecting data against misuse and unauthorized access. A series of physical, behavioral and logical measures have been listed in D10.1. Full GDPR compliance will clearly be ensured, considering provenance of results from the healthcare sector. All legal constraints linked to the nature and sensitivity of the data at stake will be fully respected. For dissemination level issues it is not possible to provide further details in the present document.

Each beneficiary is responsible for application of the protection measures and the contingency plan adopted (D10.1) and for providing training where required.

8. Ethical aspects

Ethical aspects related to data collection and processing will be closely monitored in the framework of Task 9.4 (Ethics and legal monitoring and assessment) and of the activities of the EERB- External Ethics Review Board.

Delivrable D9.1 (Ethical and legal monitoring plan) provides guidance on how to adhere to recognized ethics standards with a strong accent on data collection and processing.
In D10.1, an assessment of ethics risks related to collection of personal data is made and an opinion on the eventuality of a DPIA-Data Processing Impact Assessment is provided.
Further details on the contents of these Deliverables have a confidential dissemination level and cannot be provided here.

9. Conclusions

At Month 6 of the Project the development has not yet completely unfolded, therefore an addenda may be released to include new elements to the Data Management Plan after the first reporting period is concluded. The Consortium is committed to a Data Management approach which should primarily offer results to the healthcare community and research and industrial environment at large and at the same time protect rights of Data Subjects and information which may be subject to IPRs. Data resulting from the Project promises interesting outcomes which will be usable for future research and industrial developments. The PANACEA Consortium is sensitive to maximize the results and potential outcomes in terms of Data and to sharing the results obtained. As mentioned, the developments of the unfolding activities will lead to a greater definition of Data related aspects, refining and tailoring the approach to Data management (e.g. more detailed information on input and output formats, which of the mentioned solutions will be adopted to de-identify data etc.).

For any query or issue related to Protection of Personal Data (POPD) an on Data Management it is possible to contact the team at POPD-helpdesk@chirurgia-urgenza.it.