D1.14 Ethical HelpDesk Report v2

WP1 – Project Management

Version: 1.00

SPHINX

A Universal Cyber Security Toolkit for
Health-Care Industry

Disclaimer

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

Copyright message

Document information

Grant Agreement Number	826183	Acronym	SPHINX
Full Title	A Universal Cyber Security Toolkit for Health-Care Industry		
Topic	SU-TDS-02-2018 Toolkit for assessing and reducing cyber risks in hospitals and care centres to protect privacy/data/infrastructures		
Funding scheme	RIA - Research and Innovation action		
Start Date	1st January 2019	**Duration**	36 months
Project URL	http://sphinx-project.eu/		
EU Project Officer	Christos Maramis (HaDEA)		
Project Coordinator	National Technical University of Athens - NTUA		
Deliverable	D1.14 Ethical HelpDesk Report v2		
Work Package	WP1 – Project Management		
Date of Delivery	**Contractual** M36	**Actual**	M36
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	NTUA		
Responsible Author	George Doukas	**Email**	gdoukas@epu.ntua.gr
		Phone	
Reviewer(s):	Vagelis Papakonstantinou [VUB-LSTS], Ilias Trochidis [ViLabs]		
Keywords	Ethics, Data Processing		

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	03/12/2021	Draft	ToC	George Doukas (NTUA)
0.20	15/12/2021	Draft	First Draft	George Doukas (NTUA)
0.30	22/12/2021	Draft	Draft report for internal review	George Doukas (NTUA)
0.40	28/12/2021	Draft	Upadate draft based on Reviewers' comments	George Doukas (NTUA)
0.50	29/12/2021	Pre-Final	Quality Control	Michael Kontoulis (NTUA)
1.00	29/12/2021	Final	Final	Christos Ntanos (NTUA)

Executive Summary

It is the firm intention of all the partners involved in SPHINX to perform the research activities in compliance with all relevant legal and ethical rules which apply. To ensure this, the research activities include a legal and ethical analysis to be undertaken and recommendations for legal compliance. To this end the role of the Ethics Helpdesk is essential. The Ethics Helpdesk (D1.14 due to M36) scrutinizes the research, to guarantee that no undue risk for the user, whether technically, nor related to the breach of privacy, is possible. Thus, the Consortium shall implement the research project in full respect of the legal and ethical national requirements and code of practice.

The purpose of this document is to report the ethical issues, or any other complication arose from the beginning of SPHINX implementation to date and how these were treated. The document focuses on three ethical issues: Processing of personal data, discovery of incidental findings and misuse of research findings which were highlighted in (Deliverable 1.10, 2019).

Contents

Table of Abbreviations

GDPR : General Data Protection Regulation

WP : Work Package

Dx.xx : SPHINX Deliverables

1 Introduction

1.1 Purpose & Scope

The Ethics Helpdesk (D1.14 due to M36) scrutinizes the research, to guarantee that no undue risk for the user, whether technically, nor related to the breach of privacy, is possible. Thus, the Consortium shall implement the research project in full respect of the legal and ethical national requirements and code of practice. The purpose of this document is to report the ethical issues, or any other complication arose from the beginning of SPHINX implementation to date and how these were treated.

1.2 Structure of the deliverable

This document is structured as follows: section 1 introduces the document; section 2 presents any ethical issues that have arisen regarding the participants in the SPHINX survey; section 3 presents any ethical or legal complication that have arisen regarding processing of personal data, discovery of incidental findings and misuse of research findings; finally, section 4 concludes the document.

1.3 Relation to other WPs & Tasks

This document is related to the work performed under the scope of WP1: Project Management included in (Deliverable 1.4, 2019), (Deliverable 1.6, 2019), (Deliverable 1.7, 2019) and (Deliverable 1.10, 2019), in the scope of WP2: Conceptualisation, Use Cases and System Architecture in (Deliverable 2.2, 2019) and in the scope of WP7: Technology Validation Pilots and Privacy assessment in (Deliverable 7.2, 2021) and (Deliverable 7.3, 2021).

2 Participation in the SPHINX research

In (Deliverable 1.7, 2019) it was predicated that no research participants, other than existing employees of the pilot partners, are expected to take part in the pilot trials of the SPHINX project. In more detail, the trials of SPHINX will involve existing personnel of Polaris Medical, HESE and DYPE5 that are already working at the specific organisations.

To date, personnel's participation in SPHINX activities was asked only through two surveys trying to capture cybersecurity awareness in the healthcare pilot organisations involved in the SPHINX. The first was targeted to the ICT departments and the second one was focused on the non-ICT employees (medical, auxiliary, laboratory and administrative personnel). In both two surveys, all participants provided their answers to cyber-related queries completely anonymously.

Regarding the development of SPHINX components, in cases that real data were required (e.g. network traffic, etc.), an emulated encironment was created and public datasets were used for the design phase, the testing and validation of their functionality.

Specifically, in the context of the implementation of the task "T5.4 Behavior Simulation- Experimentation Environment Development", leaded by NTUA, it was necessary to be conducted the analysis of network connections metadata. The term "metadata" is emphasised, as these are network traffic metrics that are completely devoid of the content of the network traffic packages (also known as payload). More specifically, they summarise network connections, ie provide statistics (types of connection protocols, connection start / end times, amount of information exchanged, protocol flags) for each connection observed while removing fields related to personal data (hospital's internal IPs, MAC addresses of connected devices), making the retrieval and processing of any personal data impossible. The anonymised metadata had to be analysed in order to simulate realistic network traffic in the already installed cyber security infrastructure, for supporting the implementation and the testing of all SPHINX components.

These metadata were provided by DYPE5 to NTUA, upon official request, in their final anonymised form. More specifically, the anonymization process took place inside the facilities of DYPE5 based on the ISO / TS 25237: 2017 standard.

3 Potential ethical and legal complications

Based on indications of (Deliverable 1.10, 2019) regarding the possible complications that SPHINX project may present in terms of its compliance with legal and ethical guidelines and legislation, at the time being, none has been recorded.

3.1 Ethics and Security internal project boards

Both Ethics and Security internal project boards consist of the following members:

- *Dr Christos Ntanos* of NTUA
- *Dr Vagelis Papakonstantinou* of VUB-LSTS
- *Dr Aggelos Liapis* of KT
- *Mr George Doukas* of NTUA
- *Mr Evangelos Stamatiadis* of DYPE5

Meetings and Telcos

- June 24th 2020 (Microsoft Teams Meeting)– the first telco focused mostly on the progress of the project. Since there were no complications it was highlighted, once again, the importance of monitoring of ethic-related issues.
- November 27th 2020 (Microsoft Teams Meeting)– the telco focused mostly on the traffic capturing processes and the overall setup of the testing environment on the pilot site.
- Bilateral meetings with the pilot partners prior to pilot(s) start.
- June 25th 2021 (Microsoft Teams Meeting)– the telco focused mostly on the current status of the project. For each module it was verified that no ethic-related issues arose during the implementation phase.
- March 2022 – Regarding next meeting, if no other issue appears, the Boards decided to be held by the end of March 2022, following the approved extension of the project. In the final plenary meeting, a closing session shall be held to provide the final assessment of any project-related ethics issues that arose throughout the implementation of the project.

3.2 Protection of personal data

Note: The embedment of the SPHINX toolkit in hospitals' infrastructures indicates that SPHINX may acquire, through its platform, access to patients' personal data (health data and other personal details). However, even in this case, SPHINX shall be the *processor* of the personal data. The *controller* shall always be the hospital and any other health infrastructure that will use the SPHINX solution.

3.2.1 Personal data processing activities in SPHINX

All partners replied that no personal data processing (let alone sensitive data, such as genetic or health data), which may result to serious complications, is conducted in the context of SPHINX. Moreover, it has been verified by all partners that no true personal data will be used during the SPHINX project.

To date, there was no event invalidating the above statement. However, in the case that such event occurs, Ethics and Security internal project boards shall be immediately informed, in order to deal with the specific matter accordingly.

3.2.2 Security/ organisational measures and privacy policies

The majority of the partners apply security measures, both organisational and technical for the project's purposes.

To date, although there has been no need to secure data, as there were no real-life data, no incident has been reported to any of the partners.

3.2.3 Data subjects' rights

Safeguarding the rights of the data subjects is of major importance. Data subjects' rights are respected to a great extent by most of the partners.

To date, there was no issue arisen as no real-life data were used by the partners.

3.2.4 Lawfulness of processing

Almost all partners have stated that the data they collect are proportionate to the purpose of the processing.

To date, there was no issue arisen as no real-life data were used by the partners.

3.2.5 Security of data

Most of the partners responded positively on the organisational and technical measures they implement to safeguard the security of the personal data of the people participating in the SPHINX research.

To date, there was no event invalidating the above statement.

3.3 Incidental findings policy

Incidental findings policy as an ethic issue is addressed in the Commission's guidance entitled "How to Complete your Ethics Self-Assessment". The possibility of their occurrence presents a range of ethical, legal, and practical challenges, for both their recipients, as well as the researchers who encounter them. The majority of partners do not anticipate the use of personal data in their activities, so the discovery of incidental findings is even more unlikely.

To date, there was no issue arisen as no real-life data were used by the partners.

3.4 Misuse of research findings

Misuse of research findings may lead to serious consequences for both the researchers and the recipients of such findings. No serious complications are anticipated during the SPHINX project.

To date, there was no issue arisen as no real-life data were used by the partners.

4 Conclusions

This deliverable is the summary of all the ethical issues, or any other complication arisen from the beginning of SPHINX implementation to date. As it is recorded in (Deliverable 1.10, 2019), no major ethical concerns are expected to be raised during the project's execution.

Currently, there are no implications on SPHINX implementation regarding compliance with legal and ethical guidelines and legislation. This is quite expected since real-life data are not envisaged to be used. However, even if such data shall be used, all partners running the pilots and the consortium itself have already undertaken the necessary measures in order to safeguard the rights of the data subjects/research participants, including the protection of their personal information.

5   References

Deliverable 1.4. (2019). *Misuse of Research Finding Risk Assessment and Prevention (M6).*

Deliverable 1.6. (2019). Incidental Findings Policy (M9).

Deliverable 1.7. (2019). Ethics Data Processing Activities Risk Evaluation (M9).

Deliverable 1.10. (2019). Ethics State-of-art Report (M12).

Deliverable 2.2. (2019). Ethical Requirements (M9).

Deliverable 7.2. (2021). Legal assessment of SPHINX use case scenarios v1 (M24).

Deliverable 7.3. (2021). *Legal analysis evaluation of the SPHINX business model v1 (M24).*