Misuse of Research Findings Risk Assessment and Prevention

WP1 – Project Management

Version 1.0

SPHINX

A Universal Cyber Security Toolkit for Health-Care Industry

Disclaimer

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	Reza RAZAVI (CNECT/H/03)		
Project Coordinator	Dimitris Askounis, National Technical University of Athens - NTUA		
Deliverable	D1.4. Misuse of Research Finding Risk Assessment and Prevention		
Work Package	WP1 – Project Management		
Date of Delivery	**Contractual** M6	**Actual**	M6
Nature	R - Report	**Dissemination Level**	P - Public
Lead Beneficiary	VUB-LSTS		
Responsible Author	Dimitra Markopoulou	**Email**	Dimitra.Markopoulou@vub.be
	Vagelis Papakonstantinou	**Email**	Evangelos.Papakonstantinou@vub.be
Reviewer(s):	Bárbara Guerra and Marco Manso (EDGE), Carlos Gonçalves (INCM)		
Keywords	Misuse of Research Findings, Risk Assessment		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Document History

Version	Issue Date	Stage	Changes	Contributor
0.10	29/03/2019	Draft	ToC	Dimitra Markopoulou (VUB-LSTS)
0.20	15/04/2019	Draft	First draft	Dimitra Markopoulou (VUB-LSTS)
0.30	15/05/2019	Draft	Second draft	Dimitra Markopoulou (VUB-LSTS)
0.40	25/06/2019	Draft	Final draft submitted for review	Dimitra Markopoulou, Vagelis Papakonstantinou (VUB-LSTS)
0.50	26/06/2019	Pre-Final	Review 1	Bárbara Guerra and Marco Manso (EDGE)
0.60	27/06/2019	Pre-Final	Review 2	Carlos Gonçalves (INCM)
0.80	29/06/2019	Pre-Final	Validation of changes	Dimitra Markopoulou, Vagelis Papakonstantinou (VUB-LSTS)
0.90	30/06/2019	Pre-Final	Validation of changes, Quality Control	Christos Ntanos (NTUA)
1.00	30/01/2019	Final	Final	Christos Ntanos (NTUA)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Executive Summary

For all activities funded by the European Union, ethics is an integral part of research from beginning to end, and so is ethical compliance. Ethical compliance can be achieved through the performance of an ethics assessment that should address the following issues: human embryos and foetuses, human beings, human cells or tissues, personal data, animals, non-EU countries, environment, health & safety, dual use, exclusive focus on civil applications, potential misuse of research results and any other ethics issues not included in this list. This report highlights the points to be taken into consideration while conducting such an assessment; Relevant questionnaires to the same end have been drafted and are provided to all project partners to be filed in and submitted, as appropriate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Contents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1. Misuse of research findings. The EU approach

1.1 Introduction-misuse of research findings as an ethics issue

For all activities funded by the European Union, ethics is an integral part of research from beginning to end, and so is ethical compliance. Ethical compliance can be achieved through the performance of an ethics assessment that should address the following issues: human embryos and foetuses, human beings, human cells or tissues, personal data, animals, non-EU countries, environment, health & safety, dual use, exclusive focus on civil applications, potential misuse of research results and any other ethics issues not included in this list.

The potential misuse of research findings in particular has received great attention in the last years. Given the serious consequences the potential misuse of research could have on the general public, the need to protect research findings has turned into a critical parameter to be taken into serious consideration by anyone activated in the research field. Such risk is evidently present and therefore needs to be addressed in EU funded research. To this effect, the Commission has issued a guidance note in order to help all parties involved in H2020-funded projects to take the necessary measures to avoid potential misuse of research findings.[1] In the same context, the risk of misuse of research findings has motivated scientists and scientific institutions.[2] EU Ethics, following collective discussions, recently reached the conclusion that "Research misconduct and potential misuse constitute an ethical issue in the context of EU funded research and should be systematically addressed in EU Ethic's oversight (Screening, Review and Audit)"[3].

1.2 Commission's Guidance Note on misuse of research findings; Definitions and other parameters to be taken into account

1.2.1 Definition

A definition of misuse of research findings is included in the Commission's Guidance Note, as well as in the explanatory note issued also by the Commission.[4] On this basis, "potential misuse of research refers to research involving or generating materials, methods, technologies or knowledge that could be misused for unethical purposes".

The definition of misuse of research provided by the Commission allows for some further thoughts and clarification. In this context:

Misuse is defined as an occasion when something is used in an unsuitable way or in a way that was not intended.

a) Research is defined as the systematic investigation into and study of materials and sources in order to establish facts and reach new conclusions.

b) Research findings are the results of a research (as this is defined under b).

[1] EU Commission, H2020 Programme, Guidance, How to complete your ethics self-assessment, version 6.1, February 2019 (the "Guidance Note").
[2] See, for example, Swiss Academy of Sciences, Misuse potential and biosecurity in life sciences research, 2017, and Managing Risks of Research Misuse, A joint Biotechnology and Biological Sciences Research Council (BBSRC), Medical Research Council (MRC) and Wellcome Trust policy statement, available at https://bbsrc.ukri.org.
[3] EU Commission, Research Ethics: A comprehensive strategy on how to minimize research misconduct and the potential misuse of research in EU funded research
[4] EU Commission, Explanatory note on potential misuse of research (https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

c) Unethical purposes include purposes that are not based on moral beliefs and principles.

1.2.2 Research vulnerable to misuse

According to the note, the research most vulnerable to misuse is research that:

- Provides knowledge, materials and technologies that could be channelled into crime or terrorism.
- Could result in chemical, biological, radiological or nuclear weapons and the means for their delivery.
- Involves developing surveillance technologies that could curtail human rights and civil liberties.
- Involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people.

Consequently, the unethical use of research is not restricted to its use for actions of terrorism and crime. It also includes misuse that leads to discrimination based on profiling for instance, threat to human rights and liberties, as well as for developing and delivering chemical, biological and nuclear weapons.

1.2.3 Definition of research misconduct

Research misuse should not be confused with "research misconduct". Even though the term does not fall within the scope of this text, for consistency reasons, it is mentioned that research misconduct is defined as: fabrication, falsification and plagiarism. Falsification is defined as the misrepresentation of results. Fabrication is defined as the reporting on experiments never performed. Plagiarism is defined as taking the writings or ideas of another and representing them as one's own.

1.3 The role of risk assessment

1.3.1 What is a risk assessment?

Given the constantly increasing number of people working in research today and respectively the number of people having access to research findings, it is very difficult to eliminate misuse of research findings. The risk of misuse could though be minimised if a sound risk assessment is performed to make sure that all parties involved got familiar with the assessment findings. The purpose and benefits of performing a risk assessment are well described in a report titled "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools".[5] It is stated that "Every organization is continuously exposed to an endless number of new or changing threats and vulnerabilities that may affect its operation or the fulfilment of its objectives. Identification, analysis and evaluation of these threats and vulnerabilities are the only way to understand and measure the impact of the risk involved and hence to decide on the appropriate measures and controls to manage them". In the case of research findings, risk assessment will cover the process of identifying threats, risks and vulnerabilities and their potential impact. It will furthermore define a set of priorities/ measures to be taken in order to prevent or at least minimise the risk.

1.3.2 How to perform a risk assessment?

ENISA gives thorough guidance on how to perform a risk assessment in its report mentioned under 3.1. above **"**Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools". The report is a useful tool for conducting an accurate, well-structured and complete risk assessment. The main stages of a risk assessment as suggested by ENISA have as follows:

[5] See https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Risk Identification. First step when conducting a risk assessment is to identify potential risks, threats and vulnerabilities. It is very important that during this stage all risks are identified and recorded. According to ENISA's analysis, a risk can be related to or characterized by:

(a) its origin (e.g., threat agents like hostile employees or employees not properly trained, competitors, governments, etc.);
(b) a certain activity, event or incident (i.e. threat) (e.g., unauthorized dissemination of confidential data, competitor deploys a new marketing policy, new or revised data protection regulations, an extensive power failure);
(c) its consequences, results or impact (e.g., service unavailability, loss or increase of market/profits, increase in regulation increase or decrease in competitiveness, penalties, etc.);
(d) a specific reason for its occurrence (e.g., system design error, human intervention, prediction or failure to predict competitor activity);
(e) protective mechanisms and controls (together with their possible lack of effectiveness) (e.g., access control and detection systems, policies, security training, market research and surveillance of market);
(f) time and place of occurrence (e.g., during extreme environmental conditions there is a flood in the computer room)".

There are several methods and tools that may be used in order to identify potential risks such as checklists, brainstorming, systems analysis, scenario analysis and others.

Risk analysis. During this phase, the level of the risk and its nature are assessed. In more detail, risk analysis involves:

a) thorough examination of the risk sources;
b) their positive and negative consequences;
c) the likelihood that those consequences may occur and the factors that affect them;
d) assessment of any existing controls or processes that tend to minimize negative risks; or
e) enhance positive risks.

Evaluation of Risks is the third phase of the risk assessment. During the risk evaluation phase, decisions have to be made concerning which risks need treatment and which do not, as well as what the treatment priorities are. It is important to note that, in some cases, the risk evaluation may lead to a decision to undertake further analysis.

Risk Treatment is the process of selecting and implementing the measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk. According to ENISA, risk treatment includes the identification of options, that is, identification of alternative appropriate actions for managing these risks, the development of the action plan, the approval of such plan and, of course, the implementation of the action plan.

Establishing an ongoing monitor and review process is described as one of the most critical factors affecting the efficiency and effectiveness of risk assessment. This process makes sure that the specified management action plans remain relevant and updated.

As far as the conduct of the risk assessment is concerned, as well as the indication of the specific measures to be implemented, it is recommended that researchers are involved in the process as they are the most suitable to recognise and manage potential harms and risks relating to their research. At the same time, security experts could contribute to the process. It is also noted that any measures should be proportionate to the risk and the consequences of the potential misuse. Finally, it is very important to point out that Risk assessment records and relevant documentation contain extremely critical and confidential information that should be treated with the appropriate classification level requirements (e.g. critical, restricted-access, non-critical etc.).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1.4 Commission's guidance note on identifying and addressing potential misuse

1.4.1 Identify potential misuse

The Commission's guidance note has addressed the issue by listing a number of questions one should ask in order to identify potential misuse. In particular:

- Could the materials/methods/technologies and knowledge concerned harm people, animals or the environment if modified or enhanced?
- What would happen if they ended up in the wrong hands and knowledge involved or generated would end up in the hands of malevolent individuals?
- Could they serve any purposes other than the intended ones? If so, would that be unethical?

1.4.2 Address potential misuse once identified

Once potential misuse is identified, the next step is to see how it could be prevented. In other words, what measures should be taken in order to minimise the risk of misuse to the extent possible. Again, the explanatory note mentions several ways to mitigate risks, such as:

- Take additional security measures, e.g. physical security measures, classification of certain deliverables, compulsory security clearance for those involved in the project;
- Take additional safety measures, e.g. compulsory safety training for staff;
- Adjust the research design, e.g. use dummy data;
- Limit dissemination, e.g. by publishing only part of the research results, regulating export, etc.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2. The SPHINX project

2.1 Project description and other parameters to be taken into account. Is SPHINX research vulnerable to misuse?

2.1.1 Project's description

SPHINX aims to introduce a universal cyber security toolkit that will enhance the cyber protection of the Health IT Ecosystem and ensure the patients' data privacy and integrity. The SHPINX toolkit will be easily adapted or embedded on existing, medical, clinical or health available infrastructures. In the context of the project, SPHINX's cyber-security ecosystem shall be validated and evaluated against performance, effectiveness and usability indicators at three different countries (Romania, Portugal and Greece). Hospitals, care centers and device manufacturers participating in the project's pilots will deploy and evaluate the solution at business as usual and emergency situations across various use case scenarios.

The project's description indicates that any research findings generated during the project's life shall focus on cybersecurity in the health sector. In particular, vulnerabilities of the Health IT Ecosystem to cyber threats, existing cybersecurity solutions already used and ways to better protect the Health IT Ecosystem against such threats, are some of the issues that shall be examined and evaluated during the project's progress. SPHINX research findings, as well as the SPHINX's cyber-security ecosystem itself, shall be based on existing medical, clinical or health available infrastructures and shall be tested in practice (pilots) by specific healthcare providers (hospitals, care centres and regional health authority), as described in the project's agreement.

2.1.2 SPHINX's particularities

SPHINX has two particularities that raise concern in case a misuse of research findings occurs. The first one relates to the fact that SPHINX is focusing on the health sector and the second one is that sensitive personal data (patients' data) could be at risk in the event of a cyber-attack. As far as the first parameter is concerned, it is unquestionable that hospitals and care centres are prime targets for cyber criminals, especially concerning data theft, denial-of-service and ransomware. The question that needs to be asked in the context of this report is how and to what effect a potential misuse of SPHINX's findings could enable a cyber-attack and how could this be avoided in practice. With regard to the personal data parameter, a potential misuse of the project's research findings could result in violation of sensitive health data. This factor makes the need of addressing the risk of misuse even more crucial.

2.1.3 SPHINX research misuse in the context of the Commission's Guidance Note

Based on the above, and in the context of the list of research that is more vulnerable to misuse according to the Commission's guidance note, SPHINX research could fall within the following categories:

a) SPHINX research could be characterised as research that provides knowledge, materials and technologies that could be channelled into crime or terrorism. In particular, SPHINX research findings, if ended up in the wrong hands, could lead to acts of cyber-crime and cyber-terrorism (see also below under 2).

b) At the same time, it could be suggested that SPHINX research involves developing surveillance technologies that could curtail human rights and civil liberties. As a cybersecurity solution, SHPINX is based on surveillance methods of internet traffic within an organisation that could raise issues of

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

privacy and data protection of the subjects involved in the research (patients and employees of the sites).

c) As far as the third category included in the Commission's note is concerned, it is not likely that SPHINX research could result in chemical, biological, radiological or nuclear weapons and the means for their delivery.

d) The last type of research – the one that involves minority or vulnerable groups or develops social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people – could raise some concerns. Even though SPHINX research does not per se fall within such category, it indirectly involves vulnerable groups - people with health issues do certainly fall within such category. As already mentioned, SPHINX does not process patients' personal (health) data, however potential misuse of SPHINX findings and the solution as such could lead to violation of such data. If this occurs, the misuse of health data to discriminate against or stigmatise people is possible.

2.2 Identifying potential risks in the event of misuse of SPHINX's research findings in terms of cybersecurity and personal data breach

2.2.1 The case of a cyber threat/cyber-attack

In SPHINX's case, researchers/partners involved in the project shall conduct a series of vulnerability assessments to identify shortcomings in the security systems of healthcare providers. Specific healthcare infrastructures shall be deployed to this effect and, at the end of the day, SPHINX's cybersecurity solution shall be tested by the healthcare providers participating in the project pilots. Research findings shall therefore include information and data regarding:

- the hospitals' IT infrastructures and systems,
- details of their IT functions,
- the solutions already used in such healthcare providers in order to react to a possible cyber-attack,
- deficiencies and gaps in security,
- risks for security,
- organisational parameters, such as personnel's access to the healthcare providers' systems,
- use of passwords,
- existing security policy,
- personnel's knowledge and training on security issues,
- incident detection and notification policy in force
- any research findings related to the SPHINX solution itself.

Potential misuse of such findings could lead to the opposite result of what SPHINX aspires to. Data regarding the vulnerabilities of the healthcare IT systems, their existing security systems, their infrastructures and cyber-security operation capabilities, their existing cybersecurity tools and of course the proposed cybersecurity technology itself, if ended up in the wrong hands, could be used to plan an attack on the healthcare providers participating in the project or constitute useful know-how in the hands of criminals planting to attack the health system in general. To avoid such scenario, a risk assessment should be put in place investigating potential risks and suggesting measures to address them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

2.2.2 The case of personal data violation

As far as personal data is concerned, their exposure to violation in case of a cyber threat is another parameter that should be taken into consideration when making the risk assessment. The principle of data security requires that appropriate technical or organisational measures are implemented when processing personal data to protect the data against accidental, unauthorised or unlawful access, use, modification, disclosure, loss, destruction or damage. The General Data Protection Regulation (GDPR) states that the controller and the processor should take into account "the state of the art, the costs of implementation and the nature, scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons" when implementing such measures.

Depending on the specific circumstances of each case, appropriate technical and organisational measures could include, for example, pseudonymising and encrypting personal data and/or regularly testing and evaluating the effectiveness of the measures to ensure the data processing is secure. Even though data security burdens the processor and/or controller (in SPHINX's case the healthcare providers), SPHINX aims to offer a holistic solution that will protect the Health IT ecosystem against cyber-attacks, including data breaches. In other words, the SPHINX project aims to offer a security by design approach that will protect, among others, data subjects, namely patients, against possible cyber threats that would lead to violation of their personal data. Having this in mind, in the event that a misuse of the project's research findings is to occur, personal data, and in particular sensitive data (health data), would very likely be disposed to risks such as violation, theft or modification.

2.2.3 ENISA's report on top cyberthreats and trends: The healthcare sector

According to ENISA's report "ENISA Threat Landscape Report 2018 15 Top Cyberthreats and Trends"[6], the Healthcare sector continues to lead in the number of incidents. The report further justifies this as the healthcare sector provides an easy target to attackers due to the usual lack of integration between IT policies and the core hospital operations. Additionally, the nature of such organisations in many cases forces them to give in to ransom demands, putting a swift end to the attack. These reasons make healthcare organisations appealing to ransomware attackers.

The report provides some statistics: the largest incident was reported by 211 LA County, disclosing the exposure of 3,5 million records from accidental loss, 10% of the UK healthcare organisations have been breached more than 10 times in the last year (2018). Some of the top ransomware threats in the health sector took place in 2017 and 2018. WannaCry, for instance, is a ransomworm that is based on the combination of technically simple exploits (the EternalBlue, the DoublePulsar and cryptocurrency miners). WannaCry is replicated without any human interference and spreads from one computer to others on the same network. A global WannaCry attack targeting healthcare organisations started in May 2017 and managed to infect more than 200.000 computers spread in 150 countries, including systems of the National Health Services of Great Britain. It was estimated that more than 312 ransom payments were made for WannaCry attacks. What this implies is that sensitive personal health data attract the attention of cyber criminals, thus making the need for a risk assessment even more profound.

It is certain that, besides the monetary implications for both patients and the health system, the biggest problem arising from data breaches in the health sector is patients losing trust in providing their personal information. When individuals begin to believe that their data will be compromised, it increases the likelihood that sensitive information will be withheld. By not providing details about substance abuse or mental health, care plans could be severely compromised.

[6] See https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

3. Questionnaires provided in the context of the risk assessment

3.1 Project description and other parameters to be taken into account. Is SPHINX research vulnerable to misuse?

3.1.1 How to identify potential misuse

The questions that follow need to be answered by the participants in the project as part of the risk assessment in order to identify potential risks of misuse of research findings:

1ST QUESTIONAIRE	YES	NO	PROBABILITY OF MISUSE (%)
Does your research provide knowledge, materials and technologies that could be channelled into crime or terrorism?			
Could your research findings be used for cyber-crime and/or cyber terrorism?			
Could your research result in chemical, biological, radiological or nuclear weapons and the means for their delivery?			
Does your research involve developing surveillance technologies that could curtail human rights and civil liberties?			
Could your research findings be used in human or embryos trials?			
Does your research involve minority or vulnerable groups or develop social, behavioural or genetic profiling technologies that could be misused to stigmatise, discriminate against, harass or intimidate people?			
Could the materials/methods/technologies and knowledge concerned harm people, animals or the environment if modified or enhanced?			
Is there a risk to public safety and security?			
Are any risks that will outlast the project itself?			

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

1ST QUESTIONAIRE	YES	NO	PROBABILITY OF MISUSE (%)
Could your research findings end up in the hands of malevolent individuals?			
Could they serve any purposes other than the intended ones? If so, would that be unethical?			
Does your research involve children?			
Are there any others risks of misuse, not listed in this questionnaire? If yes please list them			

3.1.2 How to prevent and address potential misuse

As mentioned already, in order for a risk assessment to be completed, a prediction regarding possible ways to address a potential misuse should also be provided for. This could include measures in order to both prevent and of course address the misuse in the event it actually occurs.

A questionnaire follows with the main questions that should be checked to this effect.

2ND QUESTIONAIRE	YES	NO
Have you taken additional security measures, e.g. physical security measures, classification of certain deliverables, compulsory security clearance for those involved in the project?		
Have you taken additional safety measures, e.g. compulsory safety training for staff?		
Have you adjusted the research design, e.g. use dummy data?		
Have you limited dissemination, e.g. by publishing only part of the research results, regulating export, etc.?		
Do you use encryption?		
Do you ensure adequate data protection during the course of the project?		
Do you process any sensitive data?		
Do you protect electronic files? If yes, by what means?		

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Do you apply a strict use of passwords?		
Have you raised awareness among the parties involved in the research about threats, risk and vulnerabilities?		
Do you disclose as little as possible?		
Do you have confidentiality agreements with any third parties that may be recipients of your research findings?		
Do you maintain confidentiality unless there is prior approval for disclosure?		
Can unauthorised individuals easily acquire access to your research findings?		
Do you apply a detection mechanism for possible misuse?		
Do you have an incident response plan as soon as misuse comes into attention?		
Do you have a data breach report mechanism?		

In order for the research findings misuse risk assessment to be completed, the questionnaires will be circulated to all project partners. Each partner shall answer the questions and return the questionnaire filled in as appropriate.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.

Annex I: **References**

European Commission, **Guidance note — Potential misuse of research**, available at http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf

European Commission, **Explanatory note on potential misuse of research**, available at https://ec.europa.eu/research/participants/portal/doc/call/h2020/fct-16-2015/1645168-explanatory_note_on_potential_misuse_of_research_en.pdf

European Commission, **Research Ethics: A comprehensive strategy on how to minimize research misconduct and the potential misuse of research in EU funded research**, available at http://ec.europa.eu/research/participants/data/ref/fp7/89797/improper-use_en.pdf

ENISA, **Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools**, June 2006, available at https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

ENISA, **ENISA Threat Landscape Report 2018**, 2019, available at https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 826183 - Digital Society, Trust & Cyber Security E-Health, Well-being and Ageing.