D7.4 Ethics, Privacy and Security Handbook

April 27th, 2022

NIGHTINGALE

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 101021957

DOCUMENT SUMMARY INFORMATION

Grant Agreement No	101021957	**Acronym**	NIGHTINGALE
Full Title	Novel InteGrated toolkit for enhanced pre-Hospital life support and Triage IN challenGing And Large Emergencies		
Start Date	01/10/2021	**Duration**	36 months
Project URL	https://www.nightingale-triage.eu		
Deliverable	D7.4 Ethics, Privacy and Security Handbook		
Work Package	7		
Deliverable type	Report	**Dissemination Level**	Public
Due Date of Deliverable	31/03/2022	**Actual Submission Date**	27/04/2022
Deliverable Identifier		**Deliverable Version**	Final
Lead Beneficiary	UCSC		
Authors	Lorenzo Marchesi (UCSC), Saverio Caruso (UCSC)		
Co-authors			
Reviewers	Yael Vias Gvirsman (IDC), Luca Ragazzoni (UPO)		
Security Assessment	☒ Passed	☐ Rejected	☐ Not Required
Status	☐ Draft	☒ Peer Reviewed	☒ Coordinator Accepted

DISCLAIMER

NIGHTINGALE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021957. The sole responsibility for the content of this document lies with the authors. It does not necessarily reflect the opinion of the European Union. The European Commission is not responsible for any use that may be made of the information contained herein.

HISTORY OF CHANGES

Version	Date	Changes
0.1	07/03/2022	Initial version
0.2	22/03/2022	Version ready for QA review
0.3	11/04/2022	Internal review completed
0.4	20/4/2022	Internal reviewers' comments addressed
1.0	26/04/2022	Final version

PROJECT PARTNERS

No.	Logo	Partner	Short name	Country
1		INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	ICCS	Greece
2		TOTALFORSVARETS FORSKNINGSINSTITUT	FOI	Sweden
3		LEONARDO – SOCIETA PER AZIONI	LDO	Italy
4		C4CONTROLS LTD *[TERMINATED]*	C4C *[TERMINATED]*	UK *[TERMINATED]*
5		NETCOMPANY-INTRASOFT	INTRA	Luxembourg
6		INOV INSTITUTO DE ENGENHARIA DE SISTEMAS E COMPUTADORES, INOVACAO	INOV	Portugal
7		EXUS SOFTWARE MONOPROSOPI ETAIRIA PERIORISMENIS EVTHINIS	EXUS	Greece
8		UNIVERSITAT POLITECNICA DE VALENCIA	UPV	Spain
9		ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	Greece
10		DEVERYWARE	DW	France
11		PARTICLE SUMMARY	PARTICLE	Portugal
12		TREE TECHNOLOGY SA	TREE	Spain
13		EUROPAISCHE GESENLLSCHAFT FUR TRAUMA -UND AKUTCHIRURGIE - ESTES	ESTES	Austria
14		INTERNATIONAL MRMID ASSOSIATION	MRMID	Sweden
15		UNIVERSITA DEGLI STUDI DEL PIEMONTE ORIENTALE AMEDEO AVOGADRO	UPO	Italy
16		ASSISTANCE PUBLIQUE HOPITAUX DE PARIS	APHP-SAMU	France
17		UNIVERSITA CATTOLICA DEL SACRO CUORE	UCSC	Italy
18		MINISTERO DELL' INTERNO	MININT	Italy
19		AZIENDA SANITARIA LOCALE N 2 SAVONESE	ASL2	Italy
20		MAGEN DAVID ADOM IN ISRAEL	MDA	Israel
21		CARR COMMUNICATIONS LIMITED	CCL	Ireland
22		ASSOCIAZIONE CITTADINANZATTIVA ONLUS	CA	Italy
23		INTERDISCIPLINARY CENTER (IDC) HERZLIYA	IDC	Israel
24		ASTRIAL GmbH	ASTRIAL	Germany

LIST OF ABBREVIATIONS

Abbreviation	Full Name
CoI	Conflict of Interest
DoA	Description of Action (technical annex to the GA)
DPO	Data Protection Officer
DU	Dual Use
EAB	Ethics Advisory Board
EC	European Commission
EU	European Union
EU-OSHA	European Agency for Safety and Health at Work
FR	First Respondents
GA	Grant Agreement
GDPR	General Data Protection Regulation (EU Reg. 2016/679)
GDPR	EU Regulation 679/2016 General Data Protection Regulation
GEN	General
H	Humans
ICO	Information Commissioner's Office (United Kingdom)
IEA	Independent Ethics Advisor
M	Misuse
M1, M2…	Month 1, Month 2…
NEC	Non-European Country
NIT-MR	Novel Integrated Toolkit for Emergency Medical Response
PB	Project Board
POPD	Protection of Personal Data
QA	Quality Assurance
S2B	Security Scrutiny Board
T (n.n)	Task (n.n)
WP(n)	Work Package (n)

Executive Summary

Deliverable 7.4 Ethics, Privacy and Security Handbook is a public dissemination level deliverable structured as follows, in two main sections and a number of subsections.

Section 1 Ethics, privacy and security considerations for Nightingale tools and outputs. Its subsections focus on main issues to be considered in the framework of the ethics, privacy and security monitoring: recruitment and safety of research participants, incidental findings policy, considerations on personal data and ethics, import/export of materials to/from the EU, potential dual use and misuse risks, conflict of interest, equal opportunities and non-discrimination.

Section 2 Monitoring procedures focuses on the Governance of ethics, privacy and security in the project framework covering the internal bodies (Ethics Advisory Board, Security Advisory Board) and external ones (Independent Ethics Advisor) committed to a smooth and successful compliance to all ethics, privacy and security Grant Agreement Requirements and applicable regulatory, standards and best practices. The role and functions of these bodies is addressed. Other governing bodies which will provide support are identified.

Instruments for the monitoring activity are also indicated, namely the ethics helpdesk managed by the Leader of Task 7.6 Ethics, privacy and security office and the Ethics Systematic Monitoring Scheme.

Annex 1 is represented by the Ethics Systematic Monitoring Scheme template and Annex 2 is represented by the Gender Equal Opportunities Checklist.

Table of Contents

Introduction

This Ethics Handbook, as described in the Description of Action, reports on ethics, privacy and security considerations for Nightingale tools and outputs as well as the process for monitoring sensitive deliverables. It is also indicated in the DoA that it will provide ethics guidelines and protocols that all project partners need to follow when collecting, storing, using, analysing, and publishing data and results (this task is in concurrence with the Data Management Plan which will have a strong focus on this). The handbook will also provide details on how the safety of staff and research participants will be ensured throughout the project.

D7.4 has a public dissemination level. Therefore, contents are accordingly tailored for such a dissemination level and no information which cannot be released on a public level will be included. In particular, no personal data (e.g., name, affiliation, contact information) of members of any of the Project governing bodies or of the Independent Ethics Advisor is disclosed. The names and contacts of the Data Protection Officers mentioned are not included because of the public dissemination level of this deliverable. Any request for further information must be sent to the coordinator through the following link https://www.nightingale-h2020.eu/contact-us or to the e-mail nightingale@ethics-helpdesk.eu.

Some of the issues and matters addressed by this deliverable are also addressed in deliverables of WP8 Ethics Requirements (described below as in the DoA). It must be noted that these, to the contrary, have a Confidential dissemination level (only for consortium members and Commission services). Therefore, this document will align to what is already provided for in the WP8 (Ethics Requirements) deliverables adapting, where necessary, those parts containing confidential information.

D8.1 : H - Requirement No. 1 [3]
The beneficiary must submit a deliverable including: - The procedures and criteria that will be used to identify/ recruit research participants. - The final informed consent procedures including personal data processing that will be implemented for the participation of humans. - Final templates of the informed consent/assent forms and information sheets (in language and terms intelligible to the participants) including personal data processing. – Details on incidental findings policy.

D8.2 : H - Requirement No. 2 [6] Copies of opinions/approvals by ethics committees and/or competent authorities for the research with humans must be submitted as a deliverable.

D8.3 : POPD - Requirement No. 3 [3] The beneficiary must submit a deliverable including: - Confirmation that the host institution has appointed a Data Protection Officer (DPO) and that the contact details of the DPO are made available to all data subjects involved in the research. The DPO's relevant competencies must be included in the deliverable. For host institutions not required to appoint a DPO under the GDPR, a detailed data protection policy for the project must be submitted. Explanation of how all of the data they intend to process is relevant and limited to the purposes of the research project (in accordance with the 'data minimisation 'principle). - A description of the technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants. - A description of the security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for

processing. - Description of the anonymisation/pseudonymisation techniques that will be implemented.

D8.4 : NEC - Requirement No. 5 [3] The beneficiary must submit a deliverable including: - Details on the materials which will be imported to/exported from the EU. - Copies of import/export authorisations, as required by national/EU legislation.

D8.5 : DU - Requirement No. 6 [3]
Details on potential dual use implications of the project and risk-mitigation strategies must be submitted as a deliverable.

D8.6 : M - Requirement No. 7 [3]
Risk assessment and details on measures to prevent misuse of research findings must be submitted as a deliverable.

D8.7 : GEN - Requirement No. 8 [1]
The envisaged independent Ethics Advisor and Ethics Advisory Board (EAB) must be appointed at the beginning to monitor the ethics issues involved in this project and how they are handled. The Advisor and Board must be consulted and fully involved in the overall ethics monitoring of the project, and in particular, in data collection and protection, in the drafting of the unexpected/incidental findings policy, and in the monitoring of the overall ethics compliance of the final tool. The relevant competencies of the Advisor ad of the members of the EAB must be submitted as a deliverable.

D8.8 : GEN - Requirement No. 9 [12]
A report by the Ethics Advisor together with the Ethics Advisory Board must be submitted as a deliverable in month 12.

D8.9 : GEN - Requirement No. 10 [24] A report by the Ethics Advisor together with the Ethics Advisory Board must be submitted as a deliverable in month 24.

D8.10 : GEN - Requirement No. 11 [36]
A report by the Ethics Advisor together with the Ethics Advisory Board must be submitted as a deliverable in month 36.

The deliverable's contents were discussed on March 18th, 2022, during a joint meeting between the Ethics Advisory Board and the Independent Ethics Advisor.

1 Ethics, privacy and security considerations for NIGHTINGALE tools & outputs

1.1 Recruitment and safety of research participants

1.1.1 Procedures and criteria that will be used to identify research participants

The following table presents the procedures and criteria that will be used to identify research participants in the context of NIGHTINGALE activities.

Procedures and criteria that will be used to identify research participants

Research participants will be:	Identification channel	Inclusion criteria
Involved in virtual exercises (e.g., table-top)	Through direct contacts with experts/stakeholder or through professional associations or groups such as health professionals involved in emergency medical services.	Persons not under tutelage who are adult (above 18 years of age) capable of expressing a valid consent and interested in participating. Professional inclusion criteria will be identified before recruitment. A general criterion is represented by the professional experience and expertise. The research participants may also be recruited within the Partner organizations of the project. In such case it is highlighted that participation is only voluntary and that no pressure will be exercised, nor will there be any negative consequences in case of refusal. The participants must be able to understand and speak the national language fluently. Participants must have a valid work permit. Absence of any major medical condition that could impact the possibility to take part in any exercise or require medical intervention during the exercise and should generally be in good health.
Involved in live exercises		
Involved in workgroups, workshops, round tables etc.		
Involved in surveys or questionnaires (live or online)		

		*other research partners not actively participating may participate as observers; *all participants and observers are bound by the research confidentiality requirements and rules *explicit terms for participation must be expressly defined in writing prior to participation (i.e. on a voluntary, pro bono or paid basis).

1.1.2 Final informed consent procedures including personal data processing that will be implemented for the participation of humans

1.1.2.1 Introduction to informed consent procedures

NIGHTINGALE is a research project based on the interaction with individuals belonging to various categories and involved at different levels. The main actors involved, besides the Partner organizations and their staff, are:

- External professionals/stakeholders who are asked to provide expertise/opinions
- Research participants involved in the implementation of use cases asked to provide information and feedback about their experience and issues with emergency and mass-casualty incidents. The main focus is on medical and non-medical emergency workers, stakeholders and experts

It is essential to underline that all participants will be strictly voluntary and that no persons (such as children or adults under tutelage) who cannot give their free and willing consent will be enrolled.

The main instruments to reach the goals of the project are:

- the implementation of use cases, each with a specific focus on one given area or target group
- the networking activities between stakeholders which would contribute to the project's scopes (e.g., meetings, workshops etc.)

Informed consent procedures are illustrated in this deliverable.

Informed consent, in its typical definition, is a process for getting permission before conducting a healthcare intervention on a person, for conducting some form of research involving a person (though not necessarily in the medical domain), or for collecting personal data and then using, storing or disseminating/disclosing it. A healthcare provider may ask a patient to consent to receive therapy before providing it just as a researcher may ask consent to a research participant before enrolling that person in a research program or in some form of controlled experiment. Informed

consent is collected according to guidelines from the fields of both medical ethics and research ethics. It is important to emphasize that no real patients will be included in the NIGHTINGALE exercises. All participants, whether they be health professionals or lay people who are 'acting' in the exercises will be of good health and none will receive any medical treatment during the course of the exercise. All participants should be in good health before the exercise starts.

For an individual to give valid informed consent, three components must be present: disclosure, capacity, and voluntariness.

- Disclosure requires the researcher to supply each prospective subject with the information necessary to make an autonomous decision and also to ensure that the subject adequately understands the information provided. This latter requirement implies that a written consent form be written in the national language suited for the comprehension skills of subject population, as well as assessing the level of understanding through conversation.
- Capacity pertains to the ability of the subject to both understand the information provided and to form a reasonable judgment based on the potential consequences of the information provided and her/his decision to participate.
- Voluntariness refers to the subject's right to freely exercise her/his decision making without being subjected to external pressure such as coercion, manipulation, or undue influence both before, during and after the consent process.

The informed consent procedures foresee two contextual steps:

- the Information sheet which must be explained by the researcher and understood by the participant, in particular for what concerns potential risks for the participation and the rights of the participants (such as the right to withdraw at any time without proving reasons or explanations or the right to access personal data and to ask that it be modified or deleted)
- the expression of informed consent by the participant which must be freely and fairly obtained and fully understand. Consent must be signed on a paper version or a digital version (signed on a tablet).

The information sheet and consent must cover the following:

- participation in the research use cases or in other events such as workshops
- collection and processing of personal data
- audio/video recording and photography (where relevant)
- the incidental findings policy

Consent must be obtained before the involvement, preferably with sufficient advance in order to leave enough time for both a correct understanding of the nature of the exercise and the individual's participation and for the exercise of rights such as withdrawal (which in any case can be exercised at any time). The information sheet and consent forms must be clearly explained with

understandable terms in the national language and the researchers must be available for answering any questions and providing all clarifications requested both during and the involvement.

A template of information sheet and informed consent form are provided. The information provided is about NIGHTINGALE in general, while the details on the different use cases will be completed when available by the partners responsible. At the time of writing the phase of the development of the scenarios and specifications is still under development. As soon as these are available the informed consent forms will be adequately completed and translated in the identified languages. The language, also in the part on the specific experiments/use cases will be simple and understandable by the research participants and, as said, translated in the languages understood by the research participants.

1.1.3 Final templates of informed consent/assent forms and information sheets including personal data processing

These documents will be provided in the different languages understood by the candidate research participants.

1.1.3.1 Information sheet

About the NIGHTINGALE project

In a world where disasters and crises also evolve and cross boundaries with speed and ease, their complexity and magnitude increase, and societal repercussions often reach severe scales, it is imperative to increase citizens' resilience and to enhance capacity to survive, the feeling of safety while providing affected individuals with top-level healthcare that modern technology and current civil protection systems can offer. However, today's emergency medical services and non-medical civil protection practitioners (e.g., police, firefighters, other) in a mass casualty incident scene ('First Respondents (FR), striving to save lives and nursing the injured, often have to rely on complicated or even outdated procedures (multiple protocols or lack of homogeneity in response methods and guidelines) and outdated technology. NIGHTINGALE will develop, integrate, test, deploy, demonstrate, and validate a Novel Integrated Toolkit for Emergency Medical Response (NIT-MR) which ensures an upgrade to Prehospital life support and Triage. This will comprise a multitude of tools, services and applications required for 1) upgrading evaluation of injured and affected population and handle casualties (Triage (including first and second triage or pre-triage and triage – according to domestic custom or regulation)-for the purposes If the Nightingale project is the initial evaluation of injured patients in situations od Mass Casualty Incidents) by offering FRs the means to perform digital identification, allow traceability, support fast diagnosis and prognosis, continuous monitoring and enable accurate classification of medical condition; 2) optimizing pre-hospital life support and damage control through Artificial Intelligence (AI)-based tracking, tracing, routing and utilization enhancements of assets, resources and capacities as well as enabling continuous monitoring and correlation of vital signs and actions; 3) allowing shared response across emergency medical services, non-medical civil protection personnel, volunteers and citizens. The NIT-MR is provided at the service of the emergency medical services, non-medical civil protection personnel, volunteers and citizens for extensive testing, training, and validation in the framework of a Training and Validation Program.

About the NIGHTINGALE methodology

The main actors involved in NIGHTINGALE, besides the Partner organizations and their staff, are:

- external professionals/stakeholders who are asked to provide expertise/opinions;
- research participants involved in the implementation of use cases asked to provide information and feedback about their experience. The main focus is on vulnerable groups which may be represented by – only as non-exhaustive examples – medical staff and their families.

It is essential to underline, is that all participation will be strictly voluntary and that no persons (such as children) who cannot give legal consent, will be enrolled.

The main instruments to reach the goals of the project are:

- the implementation of use cases, each with a specific focus on one given area or target group;
- the networking activities between stakeholders which would contribute to the project's scopes (e.g., meetings, workshops etc.);

The NIGHTINGALE project is developed above all through the inputs from different sources (the use cases, the expertise of partners and expert opinions) and cross-fertilization and comparative study between the different partners based in different jurisdictions. Personal data are collected through the use of questionnaires, surveys or interviews.

Personal data is collected and stored in compliance with the General Data Protection Regulation (GDPR).

NIGHTINGALE will not collect from research participants data revealing even partially racial or ethnic origin, political opinions, religious or philosophical beliefs, religious, party or trade union membership, genetic code, addictions or sexual life, details of convictions, decisions on punishment and fines and other decisions issued in court or administrative proceedings.

It might occur that, for the scopes of the project, the stored personal data may be transferred to and from non-EU countries, in compliance with GDPR and relevant legislation. This possibility is indicated in the informed consent form. E-mail addresses may be visible to all recipients of mails sent out to more than one address.

Personal data collected during the NIGHTINGALE project will be destroyed when the scopes of NIGHTINGALE project come to an end, even if this should survive the formal end of the project, and in any case no longer than 2 years from the end of the project.

About the case study/exercise/activity

(To be filled out by the NIGHTINGALE partner responsible with details on scope, methods and duration)

[...]

Safety, risks and incidental findings

Safety of research participants is at the centre of the planning of the research activities. All safety provisions provided for by applicable law and regulatory and by best practices are adopted in this research activity.

Foreseeable potential risks have been assessed and measures necessary to avoid these have been adopted.

Incidental findings will be handled according to the Project's Incidental Findings Policy.

You can ask any questions to the staff administering this informed consent on the incidental finding policy, on safety and risks or any other aspect of the research or your participation.

Data Controller (person or institution): [...]

Contacts of Data Controller

Name: [...]

Surname: [...]

Function/role: [...]

Email: [...]

Phone: [...]

Contacts of Data Processor (if applicable)

Name: [...]

Surname: [...]

Function/role: [...]

E-mail: [...]

Phone: [...]

Contacts of Researcher responsible for the action

Name: [...]

Surname: [...]

Email: [...]

Phone: [...]

Contacts of Data Protection Officer

Name: [...]

Surname: [...]

Email: [...]

Phone: [...]

The **Supervisory Authority** with which you can file a complaint is: [...]

If you have any further questions considering any aspect of NIGHTINGALE project and the processing of personal data gathered, please ask the staff administering the informed consent or contact the researcher responsible for this activity or the Data Protection Officer where applicable at the contacts hereby provided.

You have the right to access personal data, rectify, delete and revoke your consent, including the request for any information regarding the processing of personal data at any time.

1.1.3.2 Informed consent form

By signing the NIGHTINGALE consent form, you are confirming that you have read and understood the Information Sheet and that you have been given the chance to ask any questions.

I confirm that I was fully informed in a language I understand about the scope and nature of NIGHTINGALE project and about participation in the research, that I was correctly informed about my rights, in particular of withdrawing at any time without any obligation of providing explanations, that I was correctly informed about the safety of my participation in the research and on the incidental findings policy, and that I hereby provide my written consent to participate.

I confirm that I was fully informed about the collection and processing of personal data, of my rights to access my personal data, rectify, delete, and withdraw consent, including the possibility to request any information regarding the processing of this data at any time and on how to exercise these rights.

I also confirm that I was fully informed of the use case (or event, or survey) [...] which I have been invited to participate in and that I am participating freely under no pressure or constraint and that I am free to withdraw at any time providing no explanation.

I agree to provide my personal information, such as name, contact information (e.g., mailing address, e-mail address, telephone number, professional information, and affiliation).

I accept to participate in workshops or to be contacted by email or telephone for observations, recommendations, regarding my specific professional field and the NIGHTINGALE project.

I accept to participate in the evaluation questionnaires as practitioners for inputs, observations, and recommendations with a focus on my specific professional field and that the data contained in the filled-out forms may be used for advancing the project and related dissemination.

I accept that it might occur that for the scope of the project, the stored personal data may be transferred to and from non-EU countries, in compliance with GDPR and relevant legislation. One example for export of data to potentially occur is when data storage space is physically located outside the EU,

I accept that photographic or video footage and/or vocal recordings may be acquired during the workshops or exercises and used only for project activities and related dissemination and that I have been offered the possibility to opt out from the present clause.

Any sensitive or personal data will not be shared publicly and will be limited to the parties/participants of the Nightingale project.

Additional notes (e.g., indicate eventual opt out from photographic/video/audio clause):

_____

First and last name of person giving consent (data subject) .....

Date ___/___/_____

e-mail (or phone) of person giving consent .....

Signature of the person giving consent: .....

Name of person administering the information sheet and consent form .....

Date ___/___/_____

Signature of the person administering consent: .....

1.1.4 Safety requirements

Occupational safety within the framework of the Nightingale activities and exercises is guaranteed by the compliance of the partner organisations with respective national regulatory on safety in workplaces and by regular assessments of risks and hazards in the workplace. A European framework, reflected by national regulators in national rules, is set forth by the European Agency for Safety and Health at Work (EU-OSHO) in Directive 89/391 - OSH "Framework Directive" (update 17/02/2022). All partner organisations are required to comply with national regulatory and with recognized best practices.

Wherever a partner organisation is required to comply as above-mentioned, the partner organisation also bears the responsibility for its compliance obligations on a national level or any other directly relevant regulation.

Particular attention is given to human research participants in the Nightingale activities. They will be made aware of risks linked to their involvement in the specific information sheets administered with the informed consent form.

Ordinary activity within the project activities (e.g., work by research staff on the premises of their own organization) will be monitored in the framework of the occupational safety policies adopted by each organization in compliance with national regulatory

Activities by research participants in the framework of exercise activities planned in the Nightingale project are subject to an assessment on specific risks. Results of the assessment will be acquired by the organizers in order to adopt necessary measures to minimise any risk.

1.2 Incidental findings policy

1.2.1 General notions on incidental findings

An incidental finding is an unintentional discovery of an element or factor while looking for something different.

Incidental findings, in the most common conception, are related to medical and diagnostic processes, in a high percentage of case in radiological diagnostics and in particular in neurological imaging. Also, in this case no unique protocol is available and the medical community tends to attain to a generic set of standards and to the individual professional approach for the specific case. Other areas invested by the issue of incidental findings are that of psychiatric diagnosis and treatment processes and that of genetic analyses.

Although a codified set of rules has not been adopted on a general scale, most scientific societies recommend defining before starting any research a set of rules, or a protocol, to handle any cases of incidental finding.

Two main categories of incidental findings are largely recognized:

- Anticipatable incidental findings: referred to “a finding that is known to be associated with a test or procedure”.
- Un-anticipatable incidental finding: referred to “a finding that could not have been anticipated given the current state of scientific knowledge”.

Main ethical challenges arise when trying to identify when it is ethically permissible or obligatory to disclose or not disclose incidental findings to research participants and how to manage such process. Four ethical principles are found to be directly related to this issue:

- Principle of respect for persons: which recognizes the fundamental human capacity for rational self-determination;
- Principle of beneficence: that "calls on professionals to take actions to ensure the wellbeing of others";
- Principle of justice and fairness: that requires fair and equitable treatment of all;
- Principle of intellectual freedom and responsibility: that "...protects sustained and dedicated creative intellectual exploration that furthers scientific progress, while requiring that practitioners take responsibility for their actions."
- Principle of non-malfeasance (applied to incidental findings): this requires practitioners to always act in the better interests of their patients whether or not this may be for the good of society in general.

1.2.2 Focus on incidental findings and medical emergency

The most relevant literature on incidental findings in medical emergency identifies the potential upcoming of such findings in diagnostic imaging. In the case of nightingale at the time of writing no specific concerns can be recorded where the project activities and methodologies are concerned. Nonetheless a policy has been drafted for potential incidental finding cases which may emerge in the course of the research activity, useful also for future applications. The bibliography included in this deliverable proposes a short survey of relevant scientific literature.

As said the majority" of incidental findings come to light in medical practice or procedures (e.g., in radiology, haematology etc.). Nonetheless, they may also come up in the domain of social sciences which only marginally may touch Nightingale. The first reaction which may come up, when considering the issue in case of vulnerabilities and vulnerable groups of individuals, is that these should be handled in the same way for all human beings, that is maintaining an equilibrium between inalienable rights of the individual (or a group) and scientific importance or legal obligations.

The parameter to bear in mind is the following:

- Does the vulnerable person or member of the vulnerable group have the background necessary to understand implications in case of incidental findings?
- What consequences may the handling of incidental findings have on the vulnerability?
- Does the researcher need expert advice?

1.2.3 NIGHTINGALE incidental findings policy

Each partner organisation, as well as each researcher, is responsible for incidental findings they may be confronted with. Nonetheless, the project maintains the responsibility that incidental findings are correctly handled in accordance to best practices within the framework of the NIGHTINGALE activities.

Some fundamental guidelines must be respected:

- information on the potential disclosure of incidental findings (to the subject or to third parties such as e.g., authorities when required by law), on the rights of the subject and on how compliance with these rights will be included in the information sheet/consent form;
- no personal or sensitive information may be disclosed by the individual who becomes aware of the finding to anyone other than the subject of the finding, or who has the legal representation of the subject (but in NIGHTINGALE, as a general rule, this should not apply because no participants will be recruited in the case studies who cannot provide their fully informed consent);
- the disclosure of the finding to the subject must be the object of an assessment of the responsible physician whether this may produce negative or harmful effects on her/his physical or mental wellbeing and integrity or on the quality of her/his life;
- the importance or, on the other hand, marginality of the disclosure of the finding to the subject (e.g., if the disclosure may potentially be life-saving);
- whether the disclosure (or non-disclosure) is subject to legal obligations;
- whether the disclosure or non-disclosure may put at risk in any way the physical or mental wellbeing and integrity of other subjects (e.g., family, co-workers etc.) or of others at large.

When a NIGHTINGALE researcher becomes aware of an incidental finding, the guidelines adopted by the organization (in compliance with national laws and standards recognized on a European level) must be followed and the coordinator of NIGHTINGALE must be advised promptly of the occurrence of incidental findings, without disclosing personal information or information which may lead to the identification of persons.

Thus, the coordinator and relevant bodies within the Project (Ethics Advisory Board, Project Executive Board) will decide whether, in the light of the disclosed elements, the use case must be halted, suspended temporarily, modified or can continue and if expert advice is required.

It is useful, for the picture on the mechanisms to be complete, to mention the scale of severity adopted by researchers at Columbia University:

Level 1 No medically significant findings (normal or normal variant findings)

Level 2 Minor findings to be considered with no predetermined timeframe

Level 3 Abnormal findings requiring expedited evaluation

Level 4 Acute abnormal findings requiring immediate evaluation

1.2.4 Incidental findings checklist

Checklist item	Response
Do the elements under assessment represent an incidental finding?	
Does this incidental finding represent any risk for the subject or her/his community?	
What type of risk is at stake?	
Is disclosure (e.g., to the subject or to authorities) or non-disclosure object of any legal obligation?	
Would disclosure or non-disclosure potentially harm the subject?	
Would disclosure or non-disclosure produce harmful effects on the community at large?	
Would disclosure or non-disclosure produce harmful effects on the researchers or their organization?	
Did the informed consent form provide details for the case of incidental findings?	
If the incidental findings are referrable to data, do any GDPR provisions apply?	
If an ethical approval/opinion was obtained, did it contain any indications in the case of incidental findings?	
Is it necessary or advisable to get expert advice e.g. (legal, medical, psychological, ethics experts or panel)?	
Is there a timeframe involved indicating the urgency of the issue?	

1.3 Considerations on personal data and ethics

The present deliverable provides a section on personal data and ethics. One of the roles of ethics in relation to the collection of personal data is that of monitoring the scopes, the informed consent, the correct use and the protection of the data against unauthorized disclosure, misuse and illegal exploitation. Prime instrument to this end is compliance with EU regulation 679/2016 General Data protection Regulation. Further in-depth analysis is provided for in the Nightingale Data Management Plan (deliverable).

The Grant Agreement requires that DPOs be identified for each partner collecting personal data. Where a partner is not required by Reg EU 2016/679 GDPR to have an appointed DPO, the adoption of a Data Protection Policy is required.

1.3.1 Appointed Data Protection Officers

The following partners have indicated their appointed Data Protection Officers (DPO). Names and contacts are not included because of the public dissemination level of this deliverable.

Partner short name	Data Protection Officer
ICCS	YES
FOI	YES
LDO	YES
C4C	*PARTICIPATION TERMINATED*
INTRA	YES
INOV	YES
EXUS	YES
UPVLC	YES
CERTH	YES
DW	YES
PARTICLE	YES
TREE	YES
ESTES	YES
MRMID	Not required
UPO	YES
APHP-SAMU	YES
UCSC	YES
MININT	YES
ASL2	YES
MDA	YES
CCL	YES
CA	YES
IDC	Not required
ASTRIAL	YES

1.3.2 Competencies of the Data Protection Officers

The competencies of the Data Protection Officers in the Nightingale Framework are those provided for by EU Regulation 679/2016 General Data Protection Regulation. In particular:

- Control activity for GDPR compliance
- Control of the regularity of consent procedures
- Control of any relevant data breach incidents and reporting to relevant national Data Protection Authorities
- Control that data subjects have the possibility of exercising their rights
- Receive complaints from Data Subjects (these complaints must also be sent to the Data Controller)

1.3.3 Detailed Data Protection Policy for partners not required to have an appointed DPO under GDPR

The following represents the detailed Data protection Policy to be adopted by those partners who are not under the obligation of having an appointed Data Protection Officer under GDPR. It is formulated according to the template proposed by IAPP (International Association of Privacy Professionals). In this template the Controller organization will be named as "partner".

Data protection principles

The Partner is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

General provisions

a. This policy applies to all personal data processed by the Partner.
b. The Responsible Person shall take responsibility for the Partner's ongoing compliance with this policy.
c. This policy shall be reviewed at least annually.
d. The Partner shall register with the Information Commissioner's Office as an organisation that processes personal data.

Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Partner shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the partner shall be dealt with in a timely manner.

Lawful purposes

a. All data processed by the partner must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests (see ICO guidance for more information).
b. The Partner shall note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Partner's systems.

Data minimisation

a. The Partner shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

a. The Partner shall take reasonable steps to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

Archiving/removal

a. To ensure that personal data is kept for no longer than necessary, the Partner shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

b. The archiving policy shall consider what data should/must be retained, for how long, and why.

Security

a. The Partner shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions shall be in place.

Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Partner shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO (more information on the ICO website).

1.3.4 Data minimisation policy

Personal data should only be processed where it is not reasonably feasible to carry out the research in another manner. Where possible, it is preferable to use anonymous data. Where personal data is needed, it should be adequate, relevant, and limited to what is necessary for the purpose ('data minimisation'). Access should be limited to those processors or staff members/authorized persons who, for reasons functional to the Nightingale project's scopes, will need to collect/access/process personal data. The data should be limited only to the data strictly necessary for the purpose. The data minimization principle requires entities to process only 'adequate, relevant and limited' personal data that is 'necessary'. EU data protection law does not define what 'adequate, relevant and limited' means but states that the assessment of what is 'necessary' must be done in relation to the purposes for processing.

Because the assessment of what data is needed should be based on the purposes of the processing itself, a controller or processor should never have more data than what is needed to achieve the purposes of the processing. The following criteria should be adopted:

- collection of personal data actually needed for the specified purposes and only in a transparent and legal framework
- no collection of data when sufficient personal data to properly fulfil the defined purposes is already achieved
- periodical review of the necessity of the data collected and destruction of all un-necessary data held

1.3.5 Technical and Organisational measures to safeguard rights and freedoms of data subjects/research participants

In order to protect the research participants rights to privacy and to the protection of their personal information NIGHTINGALE will adhere to the highest standards of privacy and data protection, as enshrined European Law, including the General Data Protection Regulation. These standards will apply to all research activities carried out within the project and which involve research participants' privacy especially with regard to the processing of their personal information. It means that NIGHTINGALE will adopt and enforce the core data protection principles, norms and obligations and base the involvement of any research participants on the core principle of informed explicit and targeted consent.

NIGHTINGALE is a dynamic project with intensive project participants/project participants and project participants/external participants interactions during the scheduled Joint Actions and Workshops. This requires particular care with regard to the protection of the rights and freedoms of the data subjects and research participants.

The whole NIGHTINGALE Consortium is aware of the data processing operations that will be carried out during the project. In particular, the NIGHTINGALE Consortium:

- will not process personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, genetic, sexual orientation and trade union membership
- will involve process of health-related data
- will not process data of children, vulnerable people and people who have not given their explicit and duly informed consent to participate in project activities
- will not involve large-scale data processing
- will not involve systematic monitoring of a publicly accessible area on a large scale
- will not involve data mining and social network analysis
- will not involve processing techniques for profiling individuals or groups
- will not involve intensive monitoring and tracking of research participants
- may only potentially involve transfer of personal data to non-EU countries (or from EU countries) due to the fact that the Nightingale Consortium has a partner from one non-EU country (Israel). Data protection issues with this country are in any case covered by adequacy decisions or equivalent provisions of the EU. The adequacy decisions will be reviewed periodically by relevant Consortium members. The issue is also covered in D8.4. The only potential data which potentially might be transferred are contact information of experts and stakeholders to be invited to participate in events or workshops, and only upon their information and consent.

The Project coordinator and the Ethics Advisory Board will be steadily monitoring project's activities in order to identify, assess and manage/respond timely to any possible deviation from the types of processing operations listed above.

1.3.6 Security measures to prevent unauthorised access to personal data and relevant equipment

Protection measures to prevent unauthorised access to personal data will be of three types: organisational, physical security and logical.

Organisational measures

Access to personal data, in any case, will be granted by beneficiaries on a need-to-know basis in order to limit the number of potential risks; Any sensitive data transfer will be anonymised or pseudonymized; Collection, back-ups and copies of files containing personal data will be subject to a minimization policy and subject to the same standards of protection; Beneficiaries guarantee that staff handling personal data will be subject to obligations set forth in this deliverable and to a non-disclosure policy.

Physical security measures

Protection of physical environments and equipment used for the collection, processing and storage of personal data in the NIGHTINGALE context implies a series of measures for which each Beneficiary takes responsibility: hardware used for such scope shall not be left unattended while its functionalities are accessible; access to venues where such hardware is located will be closed while unstaffed and access will be controlled by physical key or other means such as badge recognition; portable devices such as notebooks will be stored securely while not in use; paper copies of documents containing personal data will be produced and distributed only on a need-to-have basis; the documents will be physically destroyed once their scope has been fulfilled; those authorized to handle paper copies will diligently protect them from unauthorized access by means of physical protection (not in sight, inaccessible to unauthorized access and securely stored); destruction of such documents must be conducted so that the contents are not identifiable nor re-assembled. Signed and dated informed consent forms will be stored in hardcopy in a locked file cabinet by the partner carrying out the research, and will not be scanned, copied, or transferred. In cases in which informed consent is sought verbally, the individual digital recording of the consent procedure will also be stored in a locked file cabinet and will not be copied or transferred.

Logical measures

Beneficiaries will adhere to principles contained in recognized, domestic or EU, best practices such as, for example, those promoted in ISO 27001, ENISA (Guideline for SMEs on the security for personal data processing) and AGID (Misure minime di sicurezza ICT per le pubbliche amministrazioni). In particular each Beneficiary is responsible for the adoption of the following measures:

- Firewall (either network or local, with an appropriately protective configuration on personal computers);
- Proxies if adopted by company policy;
- Antivirus protection either on server or locally;
- Encryption or password protection of storage environments;

- E-mail access using POP and IMAP with SSL, TLS and STARTTLS;
- Cloud password protected access;
- Use of complex passwords regularly changed and possibly created by password generation software or utilities;
- Anonymisation or pseudonymisation (art. 25 GDPR) of personal data;
    - anonymization, compatible with technical specifications of the research environment, will be preferred. In the unlikely circumstance that pseudonymization may be preferred, strengthened protection measures are required as well as consultation with the relevant DPO of the Beneficiary who is controller;
    - biometric data, if any, will be pseudonymized;
- For the anonymization requirements in NIGHTINGALE 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” standard (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) will be removed or generalised:
    - First and last names of research participants;
    - 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.

Data protection by design will be at the base of the NIGHTINGALE research environment and outputs. An assessment aimed at verifying the implementation of the appropriate technical and organisational measures - taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of processing as well as the risks of a varying likelihood and the severity for rights and freedoms of natural persons posed by processing - will be made to implement this.

Contingency plan

Beneficiaries will diligently protect Personal Data and will, in case of unauthorised access or security issues which may have put protection at risk (defined as Data Breach), comply with measures set forth by Regulation 2016/679 (GDPR – General Data Protection Regulation). In particular:

- Art. 33 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Supervisory Authority;
- Art. 34 When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller (the beneficiary responsible for that data processing activity) shall communicate the personal data breach to the data subject without undue delay;
- Beneficiaries who were subject to a data breach will conduct necessary internal audits and assessments in order to adopt appropriate behavioral, physical, and logical measures in place to control damages and to restore a secure environment.

Anonymisation/pseudonymisation techniques

In all cases, if any, where deidentification is required, anonymisation will be preferred to pseudonymisation. Nonetheless, in case anonymisation is not possible, pseudonymisation will follow ENISA (European Union Agency for Cybersecurity) best practices (https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation).

1.4 Import/export of materials to/from the EU

This section addresses the following requirements:

- Details on the materials which will be imported to/exported from the EU
- Copies of import/export authorisations, as required by national/EU legislation

Two categories will be imported to/exported from the EU (Israel): 1) data and 2) elements of the toolkit (the latter only temporarily in order to allow for a tabletop exercise to take place - TTX2, month 17 of the project).

Data will be imported to/exported from the EU, including 'sensitive data' as defined by applicable EU regulations, namely Article 4(13), (14) and (15) and Article 9 and Recitals (51) to (56) of the

GDPR and relevant implementation decisions. 'Sensitive data' is subject to specific processing conditions that must be protected by equivalent conditions upon export/import between the EU and a third country (Israel in the case of the Nightingale project).

In principle, the authors of this deliverable have identified a three-step process in terms of applicable obligations related to import/export of data in and out of the EU, as follows:

- **Step 1**: the existence of an **EU adequacy decision**: requires no further action from partners but to ensure the adequacy decision is valid with the designated State (Israel) at the time of export/import, alongside the usual obligations applicable for the collection, processing, storing, and sharing data, and especially 'sensitive data' such as health data, under the GDPR and all applicable domestic laws.
- **Step 2**: in the absence or invalidity of an adequacy decision, the partners will apply **Standard Contractual Clauses (SCCs)** to any import/export if data between EU and a third country, as articulated by the latest EU Commission Implementation Decision of June 2021 (see below). This includes special consideration of 'sensitive data' under Annex I.B of that Decision.
- **Step 3**: In the absence of an adequacy decision, and in case the national laws of the third country present specific challenges making the SCCs insufficient to protect data (including sensitive data), partners will apply **special protection measures** such as, anonymisation, pseudonymisation, restricting access to data to limited and defined personnel, security measures, etc.

Where elements of the toolkit to be temporarily exported to Israel in the framework of the tabletop exercise are concerned, D8.5 (DU – Requirement No. 6) on dual use risk assessment and mitigation measures and the requirement of export licenses provides useful details. Further details are also to be found in the section of the present document “Materials which will be imported to/exported from the EU”.

1.4.1 Materials which will be imported to/exported from the EU

Materials which will be imported to /exported from the EU are 1) data (including sensitive data as defined under GDPR) and 2) elements of the toolkit (the latter only temporarily in order to allow for a tabletop exercise to take place - TTX2, month 17 of the project).

The countries which would be involved in transferal of data are the non-EU countries where partners of the Consortium are registered, namely Israel.

The compliance of national norms of Israel with the European regulatory is sanctioned by a series of instruments and conditions. The principal instrument is the Adequacy Decision (as per art. 45 of the Regulation 2016/699 General Data Protection Regulation) by which means the European Union determines if a non-EU country has an adequate level of data protection as described further on in this document.

Where the elements of the toolkit which may be temporarily exported to Israel for the tabletop exercise are concerned, it is not possible to define already which specific ones they may be (and

therefore file requests for export and import licenses, where required), because the toolkit is under development at the time of writing. This will be assessed in parallel with the dual use assessment (with a focus on security issues and export/import authorisations).

Although it is not possible to define in detail at the time of writing the exact elements relevant for the import/export matter that will in parallel allow the proper execution of the 2nd TTX, the following table provides a comprehensive sketch of the different categories of import/export elements that will also require review during the preparation activities of the given TTX. In such table we classify the different types of import/export elements, further classified into the Toolkit's building blocks, whilst identifying the owners of such elements as well as the intended deployment perspective and purpose. Such table will act as the NIGHTINGALE import/export plan to ensure monitoring of relevant matters and compliance with appropriate procedures/regulations by M16, just before the execution of the 2nd TTX. Noteworthy, the activities implemented to ensure appropriate protection and safeguarding of the import/export elements as well as any associated documentation produced will be reported to EC as an update of the current deliverable.

Categories of elements relevant for import/export issues

Main Category of Elements to be reviewed for import/export procedures and regulations	**Secondary Category of Elements (NIGHTINGALE building blocks) to be reviewed for import/export procedures and regulations**	**Owner**	**Deployment perspective/purpose within the 2nd TTX**
Data	Details (name, role, expertise) of exercise participants (invitees and within the consortium) to the 2nd TTX	MDA	Such information will be used for the appropriate design of the exercise scenario and objectives
Data	Exercise specific information such as storyline, patient data (factionary but realistic and anonymised), points of interest, objectives, incidents, actors, and roles	MDA	The entire 2nd TTX script, storyline and objectives will be produced by MDA to satisfy project needs
Hardware	Triage bracelet and/or earplug	ICCS and/or UPV	As the exercise is intended to be executed in a tabletop set up there is no need expected for deployment of triage bracelet/earplug devices. Possibly an early prototype of such device may be demonstrated to give the exercise participants a good understanding of its intended use in real life scenarios
Hardware	Triage UAV	FOI	No deployment of the UAV developed by FOI within NIGHTINGALE is expected to

Main Category of Elements to be reviewed for import/export procedures and regulations	Secondary Category of Elements (NIGHTINGALE building blocks) to be reviewed for import/export procedures and regulations	Owner	Deployment perspective/purpose within the 2nd TTX
			be part of the 2nd TTX (hence no import/export need)
Hardware	Thermal cameras for thermographic scanning application	LDO	No such deployment is envisaged for the 2nd TTX ((hence no import/export need)
Hardware	Computers/Laptops	ASTRIAL, PARTICLE, DW, EXUS, TREE, CERTH	It might be the case that some of the technical partners utilise laptops for visualising their applications in the context of the 2nd TTX. Such laptops will be COTS equipment and will not serve as local installation (local server) of the relevant partners' software applications. The developed applications will only be accessed online (data servers within EU) and by using appropriate VPN to ensure security of information transmitted.
Hardware	Smartphones	ASTRIAL, ICCS, UPV, PARTICLE	It might be the case that some of the technical partners utilise smartphones for visualising their mobile applications in the context of the 2nd TTX. Such smartphones will be COTS equipment and will not serve as local installation (local server) of the relevant partners' software applications. The developed applications will only be accessed online (data servers within EU) and by using appropriate VPN to ensure security of information transmitted.
Software	NIGHTINGALE C2/IMS, NIGHTINGALE PSAP, Fusion Services, Scenario builder, Triage App	ASTRIAL, DW and PARTICLE, CERTH, EXUS and INTRA, EXUS, ICCS and TREE and UPV	No local installation of software will be used in the 2nd TTX. No source code will be exported to non-EU country. All functionalities will only be accessed by end devices (laptops and smartphones) using VPN as described above.

1.4.2 Non-EU countries involved

As mentioned above, the compliance of national norms with the European regulatory is sanctioned by a series of instruments and conditions.

Under Article 45 of the EU's General Data Protection Regulation 2016/679 (GDPR), the European Commission may issue a decision that a third country ensures an adequate level of data protection, which was also possible under Article 25 of the EU Data Protection Directive 95/46 (the "Directive") that preceded the GDPR. Since adequacy decisions allow for an unimpeded flow of personal data from the EU to the third country involved, they may only be issued when the legal system of such country guarantees a standard of protection that is essentially equivalent to that under EU law (see Recital 104 of the GDPR).

Under Article 45(2)(a) of the GDPR, when assessing the adequacy of the level of protection in a third country, the Commission must take account of, among other things, "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation…" This means that an adequacy decision requires a holistic assessment of the legal system of a third country that goes beyond an examination of its data protection legislation and may include evaluating data gathering and data sharing measures in an area such as combatting pandemics. Adequacy must also be re-assessed as part of a periodic review by the Commission as circumstances change (see Article 46(3) of the GDPR).

Since the outbreak of the SARS-COV-2 pandemic (also known as COVID-19) the EU has kept under observation data protection in countries with which an Adequacy Decision is in place to monitor if the collection and processing of data is being stretched beyond what is recognized in the Adequacy Decisions. It has been observed by EU authorities that data collection and processing measures taken in third countries to combat the coronavirus are relevant to an evaluation of the continued validity of existing adequacy decisions and the potential conclusion of new ones.

1.4.3 Israel

Where Israel is concerned, an Adequacy Decision has been adopted by the EU on 31 January 2011.[1] The Decision is available at:

https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1527151074764&uri=CELEX:32011D0061

Articles 1 and 2 provide an overview of the scope of the decision.

Article 1

1. For the purposes of Article 25(2) of Directive 95/46/EC, the State of Israel is considered as providing an adequate level of protection for personal data transferred from the European Union in relation to automated international transfers of personal data from the European Union or, where they are not automated, they are subject to further automated processing in the State of Israel.

2. The competent supervisory authority of the State of Israel for the application of the legal data protection standards in the State of Israel is the 'Israeli Law, Information and Technology Authority (ILITA)', referred to in the Annex to this Decision.

[1] still in force, changed and consolidated version dates 17 December 2016.

Article 2

This Decision concerns only the adequacy of protection provided in the State of Israel, as defined in accordance with international law, with a view to meeting the requirements of Article 25(1) of Directive 95/46/EC and does not affect other conditions or restrictions implementing other provisions of that Directive that pertain to the processing of personal data within the Member States [...].

European Authorities in the light of modifications of data protection policies or their application in third states, in particular those for which there is an Adequacy Decision in place, is closely monitoring the effective compliance with European standards contemplated by the adequacy decisions. Both Israel and South Korea's collection of location data of persons from telecom operators have been under European Commission scrutiny. In the case of Israel, it has been established that this does not affect the Adequacy Decision when the data under observation is not exported to the EU (Art. 2 comma 1).

Any update on the issue will be closely monitored also in the light of any developments in security requirements.

The competent supervisory authority referred to in Article 1(2) of the Adequacy Decision:
The Israeli Law, Information and Technology Authority (ILITA@justice.gov.il and http://www.justice.gov.il/MOJEng/RashutTech/default.htm)

1.4.4 Standard contractual clauses

For the completeness of the survey of applicable standards it is worth mentioning the Standard Contractual Clauses (SCCs).

The European Commission can decide that standard contractual clauses offer sufficient safeguards on data protection for the data to be transferred internationally, wherever the data is to be transferred to a third country for which there is **no valid EU Adequacy Decision** at the time of the transfer.

It has so far issued two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA).

It has also issued one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.

The text of the Clauses is available at the following links:

EU controller to non-EU or EEA controller

- **decision 2001/497/EC- this decision has been consolidated from time to time and most recently on 27 September 2021**
- **(https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32001D0497)**

- **decision 2004/915/EC**
- **(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915)**

- **EU controller to non-EU or EEA processor**

- **decision 2010/87/EU**
(https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087)

Notably, the Clauses above are updated from time to time. The most recent and comprehensive decision relating to different models of export/import relating to controller-controller; controller-processor is the **EU COMMISSION IMPLEMENTING DECISION 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (EU COMMISSION IMPLEMENTING DECISION 2021)**
(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021D0914#ntr2-L_2021199EN.01003101-E0002)

In relation to the transfer of sensitive data from controller to controller, relative section 8.6. of the EU COMMISSION IMPLEMENTING DECISION 2021 reads:

"8.6 Sensitive data
Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure."

In relation to transfer from controller to processor, the EU COMMISSION IMPLEMENTING DECISION 2021, provides specific safeguards in its Annex I.B., namely:

" *Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*."

1.4.5 Special Measures

Wherever the legal order in third country does not permit SCCs to offer adequate legal safeguards, special measures need to be implemented such as restricting the personnel having access to the data, pseudonymisation of data, anonymisation, etc. This is especially true relating to 'sensitive data' including medical data as used in the NIGHTINGALE project. Special safeguards are specified in Annex I.B. of EU COMMISSION IMPLEMENTING DECISION 2021:

"*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures*."

1.4.6 Essentials of the management of import/export to/from the EU

In the framework of the Nightingale project the only non-EU country with whom there will be import /export exchanges is the state of Israel. The object of these exchanges are data and components of the toolkit as described. A detailed definition of what data and materials will be exported (or imported) cannot be made until the integration of the toolkit is under way. Nevertheless, a comprehensive sketch of the different categories of import/export elements has been provided, serving as the NIGHTINGALE import/export plan to ensure monitoring of relevant matters. In the case of the components the exportation will only be temporary, for the time necessary for the implementation of the tabletop exercise. As soon as the necessary information is available, an assessment of the materials and goods to be exported/imported will be made both for import/export reasons and for security scrutiny reasons. All necessary authorisations will be sought from European national authorities and from Israeli authorities, where required.

Where data is concerned, special safeguards will be taken to ensure the protection of 'sensitive data' in accordance with the GDPR, and partners have the responsibility of checking the validity of Adequacy Decisions before transfer of data, and in case of invalidity during the timespan of the project, commit to applying SCCs and special measures, in view of recent ECJ case law and EU Commission decisions.

The activities implemented to ensure appropriate protection and safeguarding of the import/export elements as well as any associated documentation produced will be reported to EC as an update of the current deliverable.

1.5 Dual use

Potential dual-use (civilian versus military use) issues must always be identified. The project is not intended for dual use solutions, but the solutions may potentially lead to dual use contexts. Import/export related aspects are assessed together with the broader dual use risks of civilian/military use where data, knowledge software and devices/tools are concerned. All risks must be explored, especially those involving research outcomes from which, unintentionally, dual-use potentiality might emerge, and mitigation measures must be provided.

All Consortium partners are bound by their national dual-use risk mitigation laws – for reasons of higher efficiency and sustainability of a secure working environment mitigating dual use.

1.5.1 Considerations on Dual use

The main dual use risks which need to be monitored are represented by integration of components (e.g., UAVs and sensors) and potentially by data. Dual use categories may be subject to import/export (for non-EU countries) restrictions for which licenses by national authorities will be sought as soon as possible.

At the time of writing, the project is work-in-progress and, as said, the possible risk deriving from integration of components is not verifiable. The integration of components which, on a stand-alone basis do not represent a risk, may potentially represent one if integrated with other components. Therefore, the monitoring and continuous assessment of dual use potential risks will verify this as tasks unfold. This assessment will be conducted by the bodies indicated in the mitigation measures section, in particular the Coordinator, the Task leader of T7.6 Ethical Privacy and Security Office, the Ethics Advisory Board, the Security Advisory Board and the Independent Ethics Advisor.

1.5.2 Assessment of risks

Notwithstanding the non-relevance for export control regulations, research outcomes on the following categories must be monitored for dual-use issues (*).

Assessment of risks

Category	Description	YES/NO	Comments
Category 0	Nuclear materials, facilities and equipment	NO	
Category 1	Special materials and related equipment	NO	
Category 2	Materials processing	NO	
Category 3	Electronics	YES	This category will not be developed but will only be used and integrated in the toolkit for nonmilitary scopes. An Example of electronics which may be integrated are bracelets and sensors useful for tracking patients in the triage phase. At the time of writing the knowledge and devices have not been defined or developed. The risks will be periodically assessed by the governing bodies of the Project (Coordinator, Task leader of T7.6 Ethical Privacy and Security Office, Ethics Advisory Board,

			Security Advisory Board and Independent Ethics Advisor). Particular attention will be given to the issue of integration of technologies - both on the work-in-progress and on the outcomes level - which, on a standalone basis, may not pose a serious risk but will need assessment and potentially mitigation measures when integrated.
Category 4	Computers	YES	In the context of computers (but also of telecommunications and information security) the issue of dual use of data must also be considered. Data, if used in a civilian or military perspective, may assume different outcomes as well as potential forms of malevolent use. The use of the data and the risks of the collection and processing will be monitored in order to assess risks, level of protection standards and adequacy of mitigation strategies.
Category 5	Telecommunications and Information security	YES	
Category 6	Sensors and Lasers	YES	
Category 7	Navigation and Avionics	YES	The use of UAVs and outcomes of integration with other components such as sensors, electronic devices are highly sensitive in the framework of dual use. This will be closely monitored as described in category 3 of this table.
Category 8	Maritime	NO	
Category 9	Aerospace and Propulsion	NO	

(*) As listed in Annex I to Regulation (EC) No 428/2009

1.5.3 Relevance for export control regulations

Dual-use export controls, according to the EU Dual Use Research guidance-draft version for Targeted Consultation, EU compliance guidance for research involving dual-use items, exist to govern activities involving items (materials, equipment, software and technologies) which can be used for both civil and military purposes and possibly associated with the creation of conventional military items or the proliferation of nuclear, radiological, chemical or biological weapons, also known as Weapons of Mass Destruction, and their delivery systems such as missiles and drones.

This framework applicable to the Nightingale context will foresee the potential exchange of data (import/export) with partners in the project from Israel, as described in D8.4 *NEC – Requirement No. 5* (Details on the materials which will be imported to/exported from the EU; Copies of import/export authorisations, as required by national/EU legislation). Adequacy decisions on data protection compliance have been issued by the EU for Israel. This data will be represented by contact information for experts/stakeholders to be invited to workshops or events and on data necessary for the implementation of the tabletop exercise in Israel (e.g., specifications and requirements of toolbox components).

Where knowledge is concerned, The EU dual-use Regulation does not foresee controls for non-EU persons accessing dual-use items inside the EU Territory. Hence, no license is needed as long as the controlled dual-use items remain inside the EU Territory. When the visiting third country researcher returns home with access to (or in possession of) the controlled dual-use item, whether located in the EU or exported, then a license is required.

The project foresees a tabletop exercise in Israel. Some knowledge might be exported or access to knowledge within Israel granted and some research results (e.g., devices) may be exported only temporarily to Israel for the purpose of the tabletop exercise. At the time of writing the knowledge and devices have not been defined or developed as also the exercise action plan is not yet available. It is not possible therefore to file a request for export licenses where required. To this end all steps necessary to obtain the relevant licenses will be taken with no delay as soon as technically possible.

1.5.4 Risk mitigation strategies

The NIGHTINGALE project has a well organised management and scientific structure. The following structures and roles have the collective function, each for their own part, of monitoring and recording any potential changes in the risk level of the project progress and outcomes. The following are the structures and roles involved:

Collective

- User Advisory Board
- Project Board
- Project Executive Board
- Security Advisory Board
- Ethics Advisory Board

Internal functions

- Project Coordinator (ICCS)
- Technical Manager (ASTRIAL)
- Integration Manager (INTRA)
- User Advisory Board Coordinator (ESTES)

- End User Partners Coordinator (UPO)
- Risk and Mitigation Planning Manager (INTRA)
- Quality Manager (EXUS)
- Ethical, Privacy and Security Issues Manager (UCSC)
- Legal, Societal and Humanitarian Aspects Manager (IDC)
- Exploitation and Innovation Manager (LDO)
- Dissemination Manager (CCL)

Independent

- Independent Ethics Advisor

A **quarterly dual-use risk assessment** will be made, in parallel with the quarterly misuse risk assessment involving the Security Advisory Board, the Ethics Advisory Board, the Independent Ethics Advisor and the relevant internal project functions.

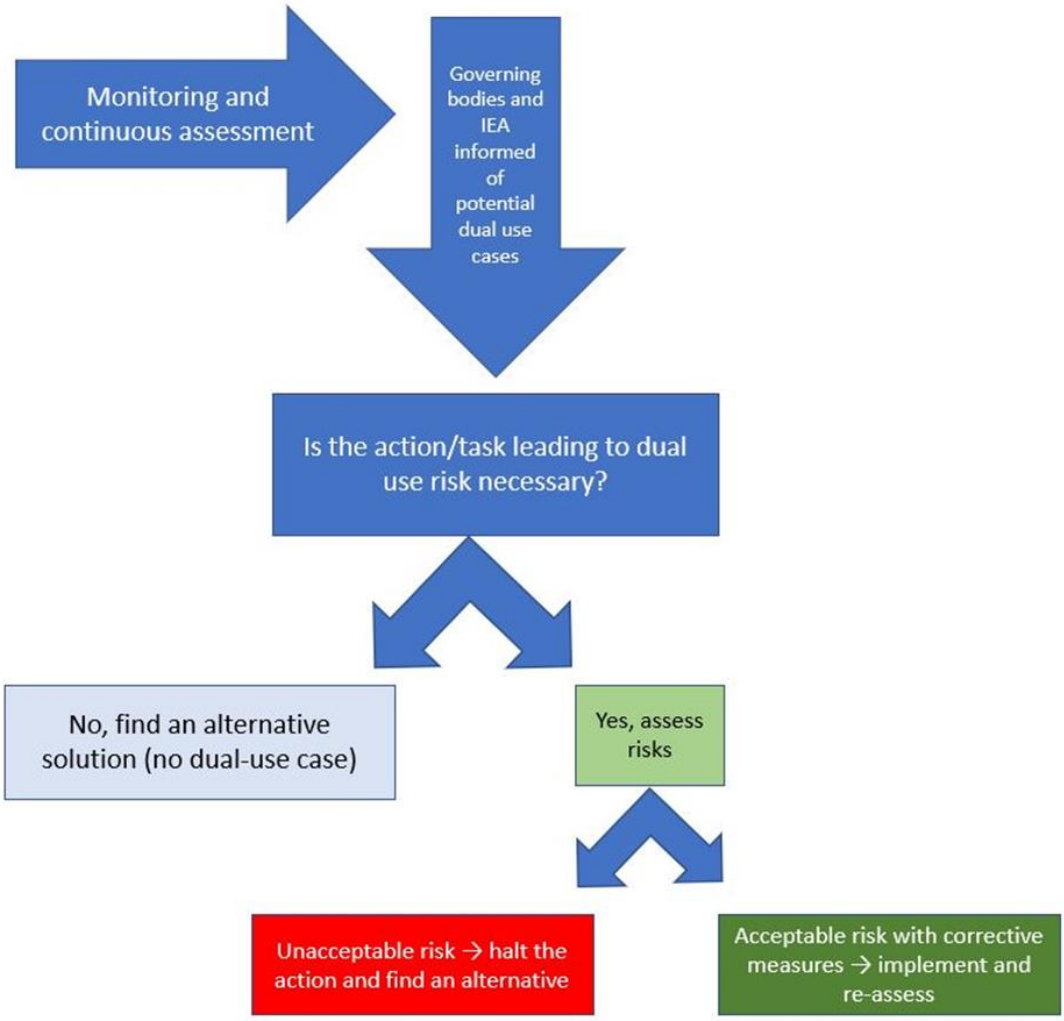
The protective measures set forth in the Project's framework will represent a very useful instrument to mitigate possible dual use risks. Namely the provisions contained in the following deliverables:

- D8.2 H – Requirement No. 2 (approvals by Ethics Committees)
- D8.3 POPD – Requirement No. 3 (Data Minimisation policy, technical and organisational measures to protect rights and freedoms of data subjects, security measures to prevent unauthorised access to personal data)
- D8.4 NEC – Requirement No. 5 (import/export authorisations for exchanges with non-EU countries)
- D8.6 M- Requirement No. 7 (measures to prevent misuse of research findings)

Where data is concerned it must be noted that special safeguards, required for the protection of sensitive data, such as applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved will be adopted, These may include for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

1.5.5 Monitoring and continuous assessment

The risks will be monitored throughout the duration of the project, under the supervision of the Coordinator, by the Security Advisory Board, the Ethics Advisory Board, the Independent Ethics Advisor and the relevant internal project functions. The mitigation strategies will follow the following scheme and all cases will be reported in the quarterly risk assessment.



Schematic diagram of mitigation actions

1.6 Misuse

This section describes the measures adopted by the project to prevent that research findings can be misused by individuals or organizations with malevolent intentions towards the health of humans, the environments, and the properties. Misuse of research findings is a risk that must be assessed in order to put necessary measures in place to contrast this possibility. Research findings may be subject to misuse or of unethical use. Both may originate from deliberate conducts or unawareness. Notwithstanding the intentionality or not, misuse must always be prevented in order not to overwhelm the benefits from project activities with the collateral effects arising.

Partners must act as much as possible to prevent misuse by applying with their national data privacy rules, especially relating to sensitive data (patient data) obligations and other goods/products (e.g., UAVs) or software/ knowledge (e.g. facial recognition, tracking) restricted by prevention of dual-use rules or any other that may be coveted by malevolent entities.

This deliverable is centred on the assessment of risks both from the outcomes point of view and the process, focusing on the phases in which the outcomes will be developed.

1.6.1 Description of potential misuse for the NIGHTINGALE context

At the centre of the NIGHTINGALE project are background information and information generated by the Project activities as well as all research outcomes. It is a best practice to consider, in any case, that they may be sensitive and may be misused or unethically used if they should fall into unauthorized hands or if not correctly disseminated. Therefore, it is crucial that alert be kept on the respect of dissemination level and/or classification and, if deemed necessary by the Consortium bodies, that they be upgraded to higher levels. In case of doubt, a cautious approach is called for deploying the highest security to protect (sensitive) data, specific software or hardware from intrusion or diversion to aims different from the aims of the project that may be unethical or contrary to law.

Element of concern for misuse is the development of a UAV platform to be used in the context of the UAV-based Rapid Triaging and Documentation System. UAVs have a heavy impact on the risk assessment for misuse (or dual use), in particular the aerial data collection function. The data collected and conserved and, potentially, shared will be subject to highest safeguard measures. In particular D8.3 *POPD – Requirement No. 3* defines technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants and security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing; D8.4 *NEC – Requirement No. 5* provides details on the handling of import/export operations involving non-EU countries as a measure of protection.

A detailed analysis of the NIGHTINGALE research perimeter and of data that are at risk for malevolent misuse represents a useful instrument for a correct assessment.

1.6.2 Potential methods for misuse

Misuse may derive from disclosure of information (authorized or unauthorized) or fraudulent access to data. The risk of misuse grows when data is not only collected but is also stored and shared between different entities. Early and precise identification of the possible methods and potential interests are involved in misusing or unethically using research findings, is needed in advance of collecting sensitive data.

A summary classification of causes may include:

- release of sensitive data in deliverables because of inadequate dissemination level or classification
- release of sensitive data in dissemination activities
- access to data by unauthorized subjects due to insufficient protection (physical or cyber-protection)
- an insufficient awareness, independently of the issue of dissemination levels or classification, of the risks, causes, methods and impact of misuse or unethical use of data or information

- the use of non-protected means of communication (e.g., oral communication in the presence of subjects not cleared for the given information, the use of unprotected mail protocols to exchange sensitive information etc.)
- breach of the rules in handling EU classified information (EUCI) (in the case of NIGHTINGALE no EUCI information is included)
- unauthorized or malevolent access to the Unmanned Aerial Vehicle (UAV)-based Rapid Triaging and Documentation System development environment or manipulation of the firmware
- Incorrect definition of which data is to be collected, stored or shared in the software specifications
- unauthorised use of the UAV or subtraction of the devices used for exercise or system validation purposes
- unauthorised modification of the features for malevolent use
- inappropriate custody of devices used for exercise or system validation purposes

1.6.3 Scopes of potential misuse

Information leeks may lead to misuse finalized at (non-exclusive list):

- Terrorist related activities
- Political gain in times of peace or of armed conflict
- Harming individuals or populations
- Damaging goods
- Harming the environment
- Unlawful profit/manipulating markets
- Manipulating public opinion/social disruption
- Extortion and criminal activity (possibly related to organized crime, money laundering or terrorist activity)

It is also important to be aware, as well as of the scope of misuse, also of the “actors” involved in such events. These may be, hypothetically speaking, the unconscious or not properly trained staff members of a Project Partner (in good faith), the unfaithful staff members (therefore intentionally, but this is only a theoretical example!) on one side, but more importantly from external entities to the project partners, and a variety of recipients such as subjects aiming at producing harm to persons or goods, to the environment, at creating social disruption, at obtaining economical advantage from misuse (e.g. through Cyber Security breach or Cyberattack).

1.6.4 Impact of misuse

When considering protection measures aimed at contrasting potential misuse, it is important to consider the potential impact of this.

The parameters to be considered are:

- The qualitative measure of the impact (low, medium, high)
    - Could the data / information / 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?
    - Could the UAV-based Rapid Triaging and Documentation System if misused harm people, animals or the environment?
    - Can malevolent entities take control of UAV remotely? Take control, divert, disrupt or change data or algorithms remotely? For example, during the use of the technology developed within the NIGHTINGALE project, therefore hindering FR ability to save lives in MCIs?
    - Could they serve any purposes other than the intended ones? If so, would that be unethical?

- Range of the impact (generalized, moderately diffuse, contained)
- Duration in time of the impacts and if any risks or impact will outlast the Project itself

1.6.5 Causes of potential divulgation and use of data leading to potential misuse

Among the causes of divulgation and use of data leading to potential misuse the following must be considered:

- Insufficient physical protection, which would allow unauthorised subjects to easily access either hard copies of documentation or files (e.g., rooms or physical environments where data would be accessible with no access/control)
- Insufficient virtual protection (cyber-protection) such as unencrypted transmission and storage, inadequate protective software such as antivirus and firewall protection etc.
- Insufficient awareness of the issue by those handling sensitive information in the Project framework
- Insufficient knowledge of protection techniques
- Negligence
- Untrustworthiness

1.6.6 Data protection measures required to contrast potential misuse

Protection measures are addressed in D8.3 (POPD – Requirement No. 3) with regard to personal data and are here further expanded to all sensitive data and in D8.4 (NEC – Requirement No. 5) where the control of import/export of data involving non-EU countries is concerned.

1.6.6.1 Organisational measures

Access to personal data, in any case, will be granted by beneficiaries on a need-to-know basis in order to limit the number of potential risks; Collection, back-ups and copies of files containing personal data will be subject to a minimisation policy and subject to the same standards of protection; Beneficiaries guarantee that staff handling personal data will be subject to obligations set forth in this deliverable and to a non-disclosure policy.

1.6.6.2 Physical security measures

Protection of physical environments and equipment used for the collection, processing and storage of personal data in the NIGHTINGALE context implies a series of measures for which each Beneficiary takes responsibility: hardware used for such scope shall not be left unattended while its functionalities are accessible; access to venues where such hardware is located will be closed while unstaffed and access will be controlled by physical key or other means such as badge recognition; portable devices such as notebooks will be stored securely while not in use; paper copies of documents containing personal data will be produced and distributed only on a need-to-have basis; the documents will be physically destroyed once their scope has been fulfilled; those authorised to handle paper copies will diligently protect them from unauthorised access by means of physical protection (not in sight, inaccessible to unauthorised access and securely stored); destruction of such documents must be conducted so that the contents are not identifiable nor re-assembled. Signed and dated informed consent forms will be stored in hardcopy in a locked file cabinet by the partner carrying out the research, and will not be scanned, copied, or transferred. In cases in which informed consent is sought verbally, the individual digital recording of the consent procedure will also be stored in a locked file cabinet and will not be copied or transferred.

1.6.6.3 Logical measures

Beneficiaries will adhere to principles contained in recognised best practices such as, for example, those promoted in ISO 27001, ENISA (Guideline for SMEs on the security for personal data processing) and AGID (Misure minime di sicurezza ICT per le pubbliche amministrazioni). In particular each Beneficiary is responsible for the adoption of the following measures:

- Firewall (either network or local, with an appropriately protective configuration on personal computers);
- Proxies if adopted by company policy;
- Antivirus protection either on server or locally;
- Encryption or password protection of storage environments;
- E-mail access using Post Office Protocol (POP) and Internet Message Access Protocol (IMAP) with Secure Sockets Layer (SSL), Transport Layer Security (TLS) and STARTTLS;
- Cloud password protected access;
- Use of complex passwords regularly changed and possibly created by password generation software or utilities;
- Anonymisation or pseudonymisation (art. 25 GDPR) of personal data;
- Anonymisation, compatibly with technical specifications of the research environment, will be preferred. In the unlikely circumstance that pseudonymisation may be preferred,

strengthened protection measures are required as well as consultation with the relevant Data Protection Officer (DPO) of the Beneficiary who is controller;
- Biometric data will be pseudonymized or anonymized

1.6.7 Focus on tracking tools and image capturing

Tracking tools and image capturing systems (e.g., with the use of UAVs) represent an element of risk of misuse. The risks can be identified in different elements in:

- the development environment of the specific user platform
- the use of the UAVs or devices such as triage bracelets, ear plugs and mobile applications in an exercise
- the loss or theft of devices
- use by untrained staff
- the aerial data collection function (which potentially, when associated with UAV integrated systems) can be misused for malevolent scopes.

The main concern is that the system, in wrong hands, can be misused, or modified for illegitimate or unethical scopes. On the other hand, it can be misused also in authorised hands, when staff is not properly trained. For these reasons a series of measures must be adopted to minimise the risks of misuse of the research findings. Specific measures are indicated in D8.3 (POPD- Requirement No. 3) defining technical and organisational measures that will be implemented to safeguard the rights and freedoms of the data subjects/research participants and security measures that will be implemented to prevent unauthorised access to personal data or the equipment used for processing. D8.4 (NEC – Requirement No. 5) provides details on the handling of import/export operations involving no-EU countries as a measure of protection. To these it is necessary to add measures which are relevant both for the outcomes of the research and for the work-in-progress of the action. Schematically:

- Access to the research environment (including data) must be minimised to the strictly necessary
- Persons should be authorised to access the data and the environment only on a need to know/need to do basis
- Data must be safely collected, processed and stored according to best practices and a traceable log of users must be kept
- UAVs, whether off-the-shelf or under customization for exercise and validation purposes of the UAV-based Rapid Triaging and Documentation System, must be protected diligently against intrusion, theft, tampering both physically and logically
- Any unexpected or risk event must be reported to the Coordinator and, where required, to the relevant authorities
- A security by design approach must be adopted in order to prevent unauthorised access
- Particular attention must be given to aerial data collection technology potentially used. This technology represents an added risk of misuse also because it can be used for unauthorised or malevolent tracing. This also applies to other tracing tools such as bracelets associated to a given identity.

1.6.8 Management Structures involved in monitoring potential misuse cases

The NIGHTINGALE project has a well organised management structure. The following structures and roles have the collective function, each for their own part, of monitoring and recording any potential changes in the risk level of the project progress and outcomes. The following are the structure and roles:

Collective

- Project Board
- Project Executive Board
- Security Advisory Board
- Ethics Advisory Board
- User Advisory Board

Internal functions

- Project Coordinator (ICCS)
- Technical Manager (ASTRIAL)
- Integration Manager (INTRA)
- User Advisory Board Coordinator (ESTES)
- End User Partners Coordinator (UPO)
- Risk and Mitigation Planning Manager (INTRA)
- Quality Manager (EXUS)
- Ethical, Privacy and Security Issues Manager (UCSC)
- Legal, Societal and Humanitarian Aspects Manager (IDC)
- Exploitation and Innovation Manager (LDO)
- Dissemination Manager (CCL)

Independent

- Independent Ethics Advisor

1.6.9 Misuse risk assessment/mitigation

The quarterly Misuse risk assessment/mitigation NIGHTINGALE is the prime instrument for assessing and proposing mitigation actions of the risks and is disciplined as described in the description of action. The present Deliverable represents the first quarterly issue of the document.

Besides, a dedicated section will be introduced in the peer review process in which the deliverables' authors and reviewers will provide a notification to the Ethical, Privacy and Security Issues Manager and the Legal, Societal and Humanitarian Aspects Manager about the inclusion of material that may lead to misuse.

(Conducted on the basis of the EU document *EU Grants: Potential misuse of research: V2.0 – 14.09.2021*

https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf)

NIGHTINGALE Outcomes under observation

Research Domain	Outcome
Technology	Triage Device (bracelet and earplug) and Mobile Application
Technology	UAV-based Rapid Triaging and Documentation System
Technology	Wide area rapid thermographic scanning
Technology	Optimized transportation capabilities
Technology	Optimised Hospitals & Medical Resources
Technology	Damage Control and AI-based diagnosis and prognosis
Technology	Multi Information Fusion Module
Technology	SWAPP – The Citizen App connected to NG112
Technology	Multilingual Operations
Knowledge	User Questionnaires and Interviews
Knowledge	End users operational procedures (at national and European levels)
Knowledge	Field Tests and Validations
Knowledge	Evaluation of NIGHTINGALE components and system as a whole

Misuse Assessment Checklist

The research:	Yes/No[2]	Comments (subject to review as development unfolds)
generates knowledge, materials and technologies that could be used for criminal or terrorist purposes	No	The research will use existing and already available technologies. In particular the UAV platform does not develop any new technologies but binds the existing ones with instrumental elements through the development of a tool which has the features of supporting medical staff in their rescue and triage tasks.

[2] The YES/NO answers are result of a work in progress assessment. These answers may change as the development of the project unfolds.

		The integration of individual components cannot be fully assessed at the time of writing. The progress will be monitored by the Ethics Advisory Board in order to provide early alarm over potential misuse emerging from the process.
Could result in the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery	No	As indicated, the added value of the system proposed does not add any risks to those already existing with off the shelf technology
involves developing surveillance technologies that could curtail human rights and civil liberties	No	No surveillance techniques will be developed. The only factor which could be associated with surveillance, but not involving the development of new techniques, is the potential tracking of patients after triage by the emergency system through data registered in the system and eventually bar-code or QRcode bracelets. These do not represent surveillance or tracking beyond what happens in standard pre-hospital and hospital procedures and is limited to a minimal set of data linked to the identity of the patient and the triage code. Besides the systems will be GDPR compliant and provide sufficient data security guarantees. Where UAVs are concerned, no tracking issues are relevant because the aerial data collection feature will not collect any personal data but only identify situations where rescuers are most needed.
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	No	
materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced.	No	As indicated, the added value of the system proposed does not add any risks to those already existing with off the shelf technology
Could the materials/methods/technologies	No	ibid

or knowledge concerned physically or in any other way harm people, animals or the environment, by themselves or if modified or enhanced?		
Could the materials/methods/technologies or knowledge concerned, physically or in any other way, have direct negative impacts on the security of individuals, groups or states?	No	ibid
Could the unauthorised disclosure of the materials/methods/technologies or knowledge concerned prejudice the interests of the European Union or of its Member States?	No	ibid
Does the activity involve the development of surveillance technologies?	No	ibid
What would happen if they ended up in the wrong hands?		The outputs of the Project would not represent a danger of misuse because they are only aimed at developing more efficient protocols and tools for delivering aide and rescue to persons or populations hit by mass casualties or emergencies. The aim of the output is also that of facilitating a harmonisation in the rescue and triage methods in particular throughout Europe. However, any risks identified during the development phase and the planning of the validation activities will be carefully assessed,
Could they serve any purposes other than the intended ones? If so, would that be unethical?	No	The case under assessment, where UAVs are concerned, does not add anything new to what is available and already developed except for the customisation for rescue purposes.
Does the activity involve minorities or vulnerable groups or activities involving the	No	

development of social, behavioural or genetic profiling technologies?		
Does the activity generate knowledge, materials and technologies that could be used for criminal or terrorist purposes?	No	ibid
Could the activity result in the development of chemical, biological, radiological or nuclear (CBRN) weapons or any method for their delivery?	No	ibid
Could the activity result in misuse of data from Cyber-attacks or cybercrimes by states or illicit entities?	No	The protection measures are calibrated to a high protection level as described in D8.3 (POPD – Requirement No. 3) with regard to personal data and in D8.4 (NEC – Requirement No. 5) where the control of import/export of data involving non-EU countries is concerned.

1.6.10 Essentials on potential misuse

In the light of this assessment of risks that the outcomes of the Project could promote or serve unethical or malevolent purposes, it emerges that the risk level may be low, however applying relevant legal framework, deontological standards, continuous monitoring, these risks can and will be mitigated. The results of the assessment will outlast the duration of the project itself. Other than monitoring that the outlasting duration of their low risk level persists, and the observance of the security measures already adopted by the Consortium, no further measures appear to be necessary. As mentioned, periodic review of adopted measures by Consortium management based on information inputs from all partners will ensure safety of data and safety from misuse. Special safeguards to secure data in accordance with national laws and GDPR and EU Commission Implementing Decisions also represent mitigating factors from misuse. Any additional needs will be identified and acted upon to ensure the highest level of protection against misuse and under the principle of due diligence.

1.7 Conflict of interest

A conflict of interest (CoI) is a situation in which a person or organization is involved in multiple interests, financial or otherwise, and serving one interest could involve working against another. Article 35 (1) of the GA states the obligation to avoid a conflict of interests.

"The beneficiaries must take all measures to prevent any situation where the impartial and objective implementation of the action is compromised for reasons involving economic interest, political or national affinity, family or emotional ties or any other shared interest ('conflict of interests'). They must formally notify to the Agency without delay any situation constituting or likely to lead to a conflict of interests and immediately take all the necessary steps to rectify this situation. The Agency may verify that the measures taken are appropriate and may require additional measures to be taken by a specified deadline"

In the case that any consortium organization becomes aware of a situation of conflict of interest, the following procedure is to be adopted:

1. Immediately inform the coordinator and/or the Project Board in writing;
2. The coordinator and/or consortium governing bodies will immediately inform the Ethics Advisory Board and the Independent Ethics Advisor who will jointly assess if the case makes up for a conflict of interest. In case a unanimous decision is not reached, the opinion of the IEA will prevail;
3. in the light of the mentioned assessment, the Coordinator and the Project Board will adopt all necessary measures to halt the situation of conflict of interest and to limit potential consequences;
4. the coordinator will notify the EU (through the competent Agency) the case and the corrective measures adopted

1.8 Equal opportunities and non-discrimination

Article 33 (1) of the GA (Obligation to aim for gender equality) states that

"The beneficiaries must take all measures to promote equal opportunities between men and women in the implementation of the action. They must aim, to the extent possible, for a gender balance at all levels of personnel assigned to the action, including at supervisory and managerial level"

In compliance with European regulations and recommendations, the Consortium adheres to the principles of equality between women and men and to non-discrimination on account of sexual orientation and gender identity. Actions will be taken to promote the involvement of staff with fair distribution between genders at all levels. Hence, the activity inside the Project considers and takes into account the gender perspectives in establishing the project policies and programs, recommending specific and concrete actions in favour of female staff. To this extent, the Treaty of Lisbon which formalizes the gender commitment and the gender mainstreaming process at the European level is considered as fundamental reference, as it mentions explicitly two aspects among the tasks and objectives of the Community: the elimination of inequalities and the promotion of equality between women and men. The EU legislation and the country specific implementation measures have contributed to sharpen consciousness and foster the creation of structures for greater gender-fairness. The consortium considers as a priority the issues of equality in employment,

offering equal opportunities to women and men, and will take appropriate actions to avoid gender discrimination and discrimination towards sexual orientation. For this purpose, the following actions will be prompted:

- encouraging junior and senior female employment participation in the different project activities;
- sensitizing project participants on equal opportunities in the projects contents;
- promoting female staff in relevant disciplines and at all levels of responsibility;
- enforcing due provisions guaranteeing options to obtain part-time and flexible employment
- according to the requirements of personnel with family and time constrains, with simple and fair procedures
- adopting appropriate measures in the extremely unlikely situation in which a case of discrimination may be recorded

An Equal Opportunities Checklist is provided in Annex 2 for self-assessment by partners.

2 Monitoring procedures

The ethics monitoring procedures are conducted by the Ethics Advisory Board, supported by the leader of Task 7 (Ethical, privacy and security office) UCSC and by the Coordinator ICCS who is Leader of WP7. The monitoring activities will be supported by all collective functions and functional roles according to the area and issues observed. The Independent Ethics Advisor has and external supervisory and control role.

2.1 Monitoring governance

Collective functions

- Project Board
- Project Executive Board
- Security Advisory Board
- Ethics Advisory Board
- User Advisory Board

Functional roles

- Project Coordinator (ICCS)
- Technical Manager (ASTRIAL)
- Integration Manager (INTRA)
- User Advisory Board Coordinator (ESTES)
- End User Partners Coordinator (UPO)
- Risk and Mitigation Planning Manager (INTRA)
- Quality Manager (EXUS)
- Ethical, Privacy and Security Issues Manager (UCSC)
- Legal, Societal and Humanitarian Aspects Manager (IDC)
- Exploitation and Innovation Manager (LDO)
- Dissemination Manager (CCL)

Independent

- Independent Ethics Advisor

2.1.1 Ethics Advisory Board and Independent Ethics Advisor

The Ethics Advisory Board (EAB) and the Independent Ethics Advisor (IEA) have different roles but concur - together with the Coordinator ICCS, the task leader of T7.6 Ethical, Privacy and Security Office UCSC and the whole Project Consortium - to the same objective: ethics compliance of the Project's procedures and outcomes. The aim is that of not only ensuring compliance but of providing a wider range ethics contribution to the research community at large.

The **EAB** is an "internal" board (composed of members of the Consortium namely ICCS, UCSC, ESTES, APHP-SAMU, INTRA) in charge of supervising ethics related issues and activities as defined per content and methodology in the DoA. The EAB will monitor and provide recommendations on such issues: to this end it will be supported by the Coordinator and the Task Leader of T7.6. Given activities or dossiers may be attributed to individual members of the EAB who will then report their findings to the Board in collegial composition for information or approval.

In particular the EAB will be charged with:

- outlining risks within key research activities where research with human subjects will take place;
- conducting discussions with appropriate WP leaders to identify and discuss ethical considerations and measures to meet such considerations;
- creating and implementing the ethics handbook;
- ensuring that the consortium abide by the handbook throughout the duration of the project;
- ensuring the consortium obtain, where applicable, ethical clearance and gain appropriate permission from data protection authorities and ethical committees;
- reporting on the ethical monitoring exercise throughout the project.
- taking into consideration all deliverables and outcomes from WP8 – Ethics Requirements.

Last but not least, Security aspects will be supervised, in collaboration with the SAB, and critical input will be provided when and if there is deviation from common standards, directives and best practices.

The IEA is an external expert who will have general and independent supervisory role on ethics and on the activities of the EAB and will interact both with the EAB and the Project Coordinator and Leader of T7.6.

The following specifically mentioned tasks, common for the EAB and the IEA, are requirements set forth in the Ethics Appraisal Report:

- Full involvement in the ethics monitoring of the project

In particular
  - ✓ where data collection and protection are concerned
  - ✓ in drafting the unexpected/incidental findings policy
  - ✓ in monitoring the overall ethics compliance of the final tool

MAIN SOURCES OF INFORMATION FOR MONITORING METHODOLOGY AND OUTCOMES

- Deliverables
- Contacts with consortium partners involved in research and development and with the Coordinator and Leader of T7.6
- Non deliverable documentation

FREQUENCY OF MEETINGS

The EAB will meet 4 times a year. Teleconference mode is admitted. At least 2 times the IEA will participate.

REPORTING

The activities of the EAB and IEA will be reported as deliverable in D8.8 (at M12), D8.9 (M24) and D8.19 (M36)

2.1.2 Security Advisory Board and monitoring of sensitive deliverables

NIGHTINGALE might handle security and ethical sensitive information as it unfolds; hence a Security Advisory Board (SAB) has been formed, comprising experts on security issues that are responsible to screen project's outcomes and activities ensuring that no security or sensitive content is publicly disclosed and to assess whether deliverables include any such information and propose timely measures (including eventually an upgrade of the dissemination level) to prevent any form of misuse of such information. The SAB is composed of experts on security issues, including end-user representatives.

According to the Security Scrutiny recommendations, particular attention should be given to two deliverables (these are indicated in section 6.3.2 of the DoA) and are not mentioned in this deliverable due to its public dissemination level.

To effectively and efficiently perform its task, the SAB not only monitors as a distinct entity the Action's outcome but closely follows the Project's Board activities and collaborates on handling security sensitive implementations. Additionally, the SAB is actively engaged to the mechanisms for approving deliverables. In more detail, a dedicated section will be introduced in the peer review process in which the deliverables' authors and reviewers will provide a notification to the SAB about the inclusion of potentially security sensitive material, thus triggering the SAB for exhaustive screening of such material and ultimately provision of recommendations for such information handling.

Furthermore, the SAB is regularly updated by the PB on the Action's progress whilst closely following internal and external information exchanges, supporting the ethics monitoring process in particular where ethics and security monitoring may provide their joint competence, e.g. where there may be potential misuse issues. The SAB's synthesis features security experts from the Action's partners. As such it will be comprised of a representative of ICCS on the Project Coordination side, of ASTRIAL on the technical management side, of UCSC being the Legal, Ethical and Security Issues Manager, of IDC being the Legal, Societal and Humanitarian Aspects Manager, of ESTES being the User Coordinator.

At the time of writing all deliverables have confidential (for Consortium members and Commission/Agency services) or public dissemination level. The SAB will monitor if any dissemination level requires being upgraded.

2.2 Quality Assurance

The QA process to which deliverables are subject before submission includes an ethics, privacy and security assessment. Reviewers will notify the Coordinator who, in turn, will consult the Ethics Advisory Board and/or the Security Advisory Board in the case any relevant issue is recorded. Deliverables identified as sensitive by the pre-Grant Security Scrutiny (as mentioned in par. 2.1.2)

will be reviewed by the SAB in order to verify if information contained is compatible with the provisions applicable to the indicated dissemination level.

2.3 Support methodology

The Project provides a mechanism to provide ethics support to project partners and to provide early identification of potential issues in the framework of the monitoring process. Identifying an issue when an activity or task is already running may cause greater problems (e.g. delay, major efforts and costs, changes to original plans etc.) than if the issues are identified and fixed in a more timely and preventive way. The Nightingale Ethics Helpdesk is available for any support which may be required by project partners. An early identification approach is at the core of the monitoring activity through interaction between the EAB, the T7.6 task leader, the IEA, the WP leaders and the project governing bodies.

2.3.1 Helpdesk

An Ethics Helpdesk acts as a contact point for any ethics issues. It is managed by the Leader of Task 7.6 (UCSC) and may be contacted to get support for ethics, protection of personal data and security issues. The ethics helpdesk staff will provide support and, when requested by the sender of if advisable in the case of a specific issue, will invest the coordinator and competent governing bodies with the request.

2.3.2 Early alarm mechanism and Ethics Systematic Monitoring Scheme

To implement the monitoring activities and in particular the early alarm mechanism, an Ethics Systematic Monitoring Scheme will represent a control panel instrument, or dashboard, which provides an all-in-one overview of the project, ethics risks, corrective measures and opinions of relevant governing bodies which can be regularly updated. Please see Annex 1.

2.3.3 Reporting

Reporting will be provided in Deliverable 8.8 (at Month 12), D8.9 (at Month 24) and D8.10 (at month 36). These are reports by the Ethics Advisory Board and the Independent Ethics Advisor.

References

[1] Ethical management of incidental findings in emergency care: A critical interpretive, Iskander R and Ells C, literature review, Canadian Journal of Emergency Medicine – Volume 22, Supplement S1, May 2020

[2] Incidental Findings on CT Scans in the Emergency Department, Thompson RJ, Wojcik SM, Grant WD, Ko PY, Emergency Medicine International, 10.1155/2011/624847

[3] Suicidal Ideation, Harmer B, Lee S, Duong TVH, Saadabadi A.2021 Aug 6. In: StatPearls [Internet]. Treasure Island (FL): StatPearls Publishing; 2021 Jan–.PMID: 33351435 Free Books & Documents. Review.

[4] Frequency and follow-up of incidental findings on trauma computed tomography scans: experience at a level one trauma center, Munk MD, Peitzman AB, Hostler DP, Wolfson AB.J Emerg Med. 2010 Apr;38(3):346-50. doi: 10.1016/j.jemermed.2008.01.021. Epub 2008 Sep 19.PMID: 18804935

[5] Frequency of incidental findings on computed tomography of trauma patients, Devine AS, Jackson CS, Lyons L, Mason JD.West J Emerg Med. 2010 Feb;11(1):24-7.PMID: 20411070 Free PMC article.

[6] The trauma pan scan: what else do you find?, Baugh KA, Weireter LJ, Collins JN.Am Surg. 2014 Sep;80(9):855-9.PMID: 25197870

[7] Incidental CT findings in trauma patients: incidence and implications for care of the injured, Paluska TR, Sise MJ, Sack DI, Sise CB, Egan MC, Biondi M.J Trauma. 2007 Jan;62(1):157-61. doi: 10.1097/01.ta.0000249129.63550.cc.PMID: 17215748

[8] Lesson by SARS-CoV-2 disease (COVID-19): whole-body CT angiography detection of "relevant" and "other/incidental" systemic vascular findings, Rea G, Lassandro F, Lieto R, Bocchini G, Romano F, Sica G, Valente T, Muto E, Murino P, Pinto A, Montesarchio V, Muto M, Pacella D, Capitelli L, Bocchino M.Eur Radiol. 2021 Oct;31(10):7363-7370. doi: 10.1007/s00330-021-07904-y. Epub 2021 Apr 16.PMID: 33864140 Free PMC article.

[9] Three Medicolegal Cases of Searching for the Stone: Lessons Learned Along the Journey, Jacobson AA, Sakamoto AE, Moore GP, Boie ET.Clin Pract Cases Emerg Med. 2020 Nov;4(4):505-508. doi: 10.5811/cpcem.2020.9.48652.PMID: 33217257 Free PMC article.

[10] Incidental Findings in CT and MR Angiography for Preoperative Planning in DIEP Flap Breast Reconstruction, Wagner RD, Doval AF, Mehra NV, Le HB, Niziol PA, Ellsworth WA, Spiegel AJ.Plast Reconstr Surg Glob Open. 2020 Oct 23;8(10): e3159. doi: 10.1097/GOX.0000000000003159. eCollection 2020 Oct.PMID: 33173675 Free PMC article.

[11] Appropriate use of CT for patients presenting with suspected renal colic: a quality improvement study, Himelfarb J, Lakhani A, Shelton D.BMJ Open Qual. 2019 Dec 2;8(4):e000470. doi: 10.1136/bmjoq-2018-000470. eCollection 2019.PMID: 31909206 Free PMC article.

[12] Incidental findings on whole-body computed tomography in trauma patients: the current state of incidental findings and the effect of implementation of a feedback system, Kumada K, Murakami N, Okada H, Toyoda I, Ogura S, Asano T.Acute Med Surg. 2019 Mar 27;6(3):274-278. doi: 10.1002/ams2.410. eCollection 2019 Jul.PMID: 31304029 Free PMC article.

[13] Incidental CT findings in Trauma patients: incidence and implications for care of the injured, Paluska TR, Sise MJ, Sack DI, Sise CB, Egan MC, Biondi M, Western Journal of Emergency Medicine. 2007;62(1):157–161. – PubMed

[14] The prevalence of incidental findings on abdominal computed tomography Scans of Trauma Patients, Ekeh AP, Walusimbi M, Brigham E, Woods RJ, McCarthy MC. Journal of Emergency Medicine. 2010;38(4):484–489. - PubMed

[15] IAPP Data Protection Policy template. https://iapp.org/resources/article/sample-data-protection-policy-template-2/

[16] Enisa best practices and techniques for pseudonymisation (December 3, 2019 update). https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation

[17] The ENISA Pseudonymisation techniques and best practices report. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices

[18] ULD - ENISA Workshop: Pseudonymisation and relevant security technologies. https://www.enisa.europa.eu/events/uld-enisa-workshop/uld-enisa-workshop-pseudonymization-and-relevant-security-technologies

[19] EU Dual Use Research guidance-draft version for Targeted Consultation, EU compliance guidance for research involving dual-use items. https://trade.ec.europa.eu/consultations/documents/consul_183.pdf

[20] United Nations Inter-Agency Network on IANWGE Women and Gender Equality, Minimum requirements checklist for integrating gender equality in the implementation of the un framework for the socioeconomic response to COVID-19, (online) https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/IANWGE-Minimum-requirements-checklist-for-integrating-gender-equality-in-COVID-19-response-en.pdf

[21] Directive 89/391/EEC - OSH "Framework Directive (update: 17/02/2022), European Agency for Safety and Health at Work, https://osha.europa.eu/en/legislation/directives/the-osh-framework-directive/1

Annex 1 – Ethics Systematic Monitoring Scheme

ESMS - Ethics Systematic Monitoring Scheme

PHASES of NIGHTINGALE	Leader	duration	Risk Code	Description of risk	Probability of occurring	Potential impact	Mitigation	Task 7.6 Leader Comments	ERB Comments	IEA Comments	Coordinator comments
WP1: Practitioners Needs & Toolkit Architecture and Design	**UPO**	**1-34**									
T1.1: Triage Protocols, Damage Control, Prehospitalization processes: Common Denominators and New Paradigm for Trauma Care	UPO	1-34									
T1.2: Social, Legal and Ethical Landscape for MCIs handling and Action's Impact Assessment	IDC	1-11									
T1.3: Technology Watch for EMS - Gaps and Limitations	MDA	1-5									
T1.4: Overarching scenarios, Definition of use cases and testing and validation activities specific	APHP-SAMU	2-9									
T1.5: Definition of functional and non-functional user requirements	UPO	2-9									
T1.6: Technical Requirements, Specifications and Toolkit Architecture	ASTRIAL	2-10									
T1.7: User and Technical Validation Protocol, KPIs and Plan	INTRA	2-10									
WP2: Upgrading Triage	**ICCS**	**3-34**									
T2.1: Component definition/application sheet, deployment specifics and ruggedisation	UPV	3-12									
T2.2: Development & Prototyping of a novel Triage System (HW, App, Frontend & Functions)	ICCS	3-34									
T2.3: Development & Prototyping of Rapid and Wide area Triage Services in the air and on the ground (HW, App, Frontend & Functions)	LDO	3-34									
T2.4: Development & Prototyping of Volunteers based participatory, inclusive and rapid Triage (HW, App, Frontend & Functions)	INOV	3-34									
WP3: Pre-hospitalisation enhancement and Continuous Triage enablers	**INOV**	**3-34**									
T3.1: Component definition/application sheet, deployment specifics and ruggedisation	INOV	3-12									
T3.2: Field data analysis and preparation for AI training (Assets, Resources and Vitals continuous monitoring, track and tracing ML-based algorithms)	FOI	3-34									
T3.3: Semi-autonomous tasking and optimal routing ML-based algorithms	CERTH	3-34									
WP4: Multi-agency collaboration and Information Management, Augmenting the Common Operational Picture and Training Engine	**ASTRIAL**	**3-34**									
T4.1: Multi-source Information Fusion and Expert Reasoning (Interoperable Data Lake)	CERTH	3-34									
T4.2: Development and prototyping of AR functions	ASTRIAL	3-34									
T4.3: Scenario Digitalisation and Execution / Triage Digital Scenario Engine (TRIDEN)	EXUS	3-34									
T4.4: Multi-agency Incident Management and Command and Control	ASTRIAL	3-34									
T4.5: Citizen to EMS interaction - PSAP to IMS	DW	3-34									
WP5: Toolkit Integration, Testing & Field Validation and Knowledge Capitalisation	**INTRA**	**11-36**									
T5.1: Laboratory Integration and testing (LITs, TTXs)	INTRA	11-34									
T5.2: Field integration and testing in small scale deployments (SSXs)	INTRA	12-35									
T5.3: Field integration and testing & Full scale field validation in operational conditions (FSXs)	INTRA	16-35									
T5.4: LITs, TTXs, SSTs, FSXs Knowledge capitalisation: Systematic Training, Evaluation and Lessons	UPO	16-36									
T5.5: User familiarisation on the operation of the tools	CCL	13-36									
WP6: High Impact Creation, Dissemination, Communication, Awareness and Exploitation	**CCL**	**1-36**									
T6.1: Brand Strategy & creation of first class communications collateral	CCL	1-36									
T6.2: Implementation of High impact Communications activities & Outreaching Events (Workshops, Conferences, DEMOs, Seminars)	CCL	1-36									
T6.3: Identification of stakeholders and business cases & Networking with key actors from the Emergency Medicine community	ESTES	1-36									
T6.4: Exploitation plans and Business Strategy	LDO	1-36									
T6.5: Standardisation, IPR and Data Management Plans	ICCS	1-36									
WP7: Consortium Management &R-I Development Coordination	**ICCS**	**1-36**									
T7.1: Overall Project and Financial Coordination & Planning	ICCS										
T7.2: Technical Management & Integration Assurance and Risks	ASTRIAL	1-36									
T7.3: Innovation Management and Exploitation Potential	LDO	1-36									
T7.4: Overall Quality Criteria Management and Assurance	EXUS	1-36									
T7.5: Practitioners Management and Advisory Board	ESTES	1-36									
T7.6: Ethical , Privacy and Security Office	UCSC	1-36									
T7.7: Social and Legal Aspects	IDC	1-36									
WP8: Ethics Requirements	ICCS	1-36									

	RISK CODES
H	Humans
POPD	Protection of Personal Data
NEC	Non European Countries
DU	Dual Use
M	Misuse
GEN	General
SEC	Security
	PROBABILITY OF OCCURRING AND POTENTIAL IMPACT
LOW	
MEDIUM	
HIGH	
EAB	Ethics Advisory Board
IEA	Independent Ethics Advisor

Annex 2 – Gender equal opportunities checklist

	Y/N	Comments (for internal use of the organization)
Does your organization have an equal opportunities and non-discrimination policy?		
If no, have you adopted specific measures to implement equal opportunities and non-discrimination?		
Does your organization promote equal opportunities and non-discrimination actively (e.g. through training and/or specific documentation)?		
Specifically, in the framework of the Nightingale project, has your organization actively worked towards the inclusion of female researchers (both at a senior and junior level)		
Does your organization, e.g. when collecting data requiring to declare if male or female, provide fields for Male, Female, Non Binary and Not Declared?		
Would your organization benefit from a specific training session in the Nightingale framework?		
Further questions or doubts? Please share them with nightingale@ethics-heldesk.eu		