Social, Legal and Ethics Report

01.09.2022

NIGHTINGALE

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	Social, Legal and Ethics Report – First Response in Mass Casualty Incidents and NIGHTINGALE Actions' Impact Assessment- Preliminary		
Work Package	WP1		
Deliverable type	Report and Annexes	Dissemination Level	Public
Due Date of Deliverable	31.08.2022	Actual Submission Date	01.09.2022
Deliverable Identifier	D1.3	Deliverable Version	Final
Lead Beneficiary	IDC		
Authors	Yael Vias Gvirsman (IDC)[1]		
Co-authors	Lorenzo Marchesi (UCSC) on Ethics		
Reviewers	Itamar Ashkenazi (ESTES), Daniele Gui and Sabina Magalini (UCSC)		
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.

[1] I would like to thank Ms. Gabriele Kuchenbecker for research assistance at the initial stages of the project.

HISTORY OF CHANGES

Version	Date	Changes
0.1	15/07/2022	Table of contents
0.2	27/08/2022	First draft
0.3.	29/08/2022	Reviewer comments
0.4.	31/08/2022	Version integrating reviewer comments
0.5.	31/08/2022	Coordinator approval/comments
1.0	01/09/2022	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	Definition
BHR	Business and Human Rights
DoA	Description of Action
ESG	Environmental and Social Governance
EU	European Union
E/PIA	Ethics and Privacy Impact Assessment
FR	First Responder
GA	General Agreement
GDPR	General Data Protection Regulation (EU Reg. 2016/679)
HRDD	Human Rights Due Diligence
M	Month
MCI	Mass Casualty Incident
MS3	Milestone 3
NIT-MR	Novel Integrated Toolkit for Emergency Medical Response
OECD	Organisation for Economic Co-operation and Development
UAV	Unmanned Aerial Vehicle
UN SDGs	United Nations Sustainable Development Goals
WP	Work Package

Executive Summary

This document is the preliminary output from the Social, Legal and Ethics landscape exercise accomplished from M1 to M11 of the project and a preliminary impact assessment within Task 1.2 *Social, Legal and Ethical Landscape for MCIs handling and Action's Impact Assessment* (deliverable 1.3. due M11). It will be followed by periodic review and a final report toward the end of the project (D1.4.). D1.3. feeds from deliverables in WP1, WP2, WP3, WP4, WP5, WP7 and WP8. It identifies relevant Actions in the project to be taken into account in view of their impact on social, legal and ethical aspects, possible risks and the need to mitigate risk through an early-stage preparedness and on-going impact assessment from design to training and use.

Social or societal boundaries exist in relation with (1) **advanced technology**- an under-regulated sphere in a rapidly developing environment with potentially far-reaching effects on fundamental human rights, (2) **first response to and in mass casualty incidents and disasters** that occur in complex humanitarian settings characterized by uncertainty, emergency and the necessity to act fast, life threatening settings and the aim to preserve life, personal (physical and mental) integrity and human dignity, and (3) training and including volunteers and broader public to first responders. Successful integration of advanced technology accessible for the use of FRs or a broader public requires trust-building, transmitting accurate, truthful coherent information, transparency. Addressing societal concerns at the initial phases of the project (designing process and building training material) will increase the potential success of the project objectives. Communication and outreach to professional and broader public needs to be done conscientiously and intentionally, while ensuring an on-going monitoring and engaging process with designated affected population.

The legal landscape of MCIs generally and of the meeting point between MCIs and Advanced Technology can be a minefield, between uncertainties on how to implement existing regulation and an inherent vacuum of an under-regulated field, as well as by differences in domestic regulation (laws, guidelines, protocols).

As a rule, task 1.2. and task 7.6. on the legal, societal, humanitarian and task 7.7 on ethical aspects of the project takes a rights-based approach. On the one hand the different relevant deliverables set out *existing, binding rules* and obligations affected by integrating advanced technology to first response in MCIs. These include international or European human rights law, namely non-discrimination, right to life, right to bodily integrity, right to dignity and the right to privacy and family life. On the other hand, whereas the implementation of existing regulation or where regulation is still in development or inexistent, the legal approach takes a rights-based and risk-based approach. Humanitarian principles (e.g. do no harm, preserve life, integrity, dignity, non-discrimination) and the Business and Human Rights field provide the main anchors and guidelines for best practices. It also takes into account proposed legislation within the EU framework relating to each potential advanced technology integrated in the NIGHTINGALE toolkit (e.g. draft EU Artificial Intelligence Act). This framework has several advantages and is based on a 'means liability' (apply the correct means, caution in advance and preparedness, monitor compliance, actively intend to reach outcomes) as opposed to a 'result liability'. This does not mean that partners that comply with their obligations as to 'means' are released from liability for results. It does mean that if an ex post facto (judicial) review occurs of results, and perhaps possible harm, than there is a track-record of the means, caution and therefore indication of intent of partners when complying with their obligations or in following best practices.

Partners are obliged to apply precautions to mitigate risks and to report on how they acted to mitigate those risks. This creates a responsible environment based on awareness, open communication, mutual (sometimes expert) support and transparency. How this is achieved is summarised by Annexes I-IV to this report, namely with consent forms (Annex I); the Human Rights Due Diligence 'checklist' (Annex II) updated with an Environmental and Social Governance (ESG) approach (compared Annex I of D7.5. the Legal, Societal and Humanitarian Handbook); Incidental research findings checklist (Annex III); and finally, the Ethics and Data Protection Impact Assessment (E/PIA) checklist (Annex IV).

Ethics and data protection landscape: As reflected in deliverables mentioned above, partners are bound by several principles relating to avoiding conflict of interest, ethical obligations in human research (e.g., collateral or incidental findings) and to data protection, namely in relation to 'sensitive data' as defined by the GDPR, including patient or medical data. Principles of minimizing data to strict necessary, anonymisation of data where possible, pseudonymisation where needed, authorized access where required.

Table of Contents

LIST OF FIGURES

Introduction

The NIGHTINGALE's project main objective is to enhance first medical prehospital response (triage, primary treatment and evacuation) in challenging and large emergencies by taking a twofold approach: (a) integrating specifically designated, advanced technology to emergency response, referred to in the NIGIHTINGALE project as the Novel Integrated Toolkit for Emergency Medical Response (NIT-MR), for 'conventional' First Responders (FRs) (e.g. Emergency Medical Staff (EMS), firefighters, police)and (b) enhancing medical response by boosting the medical capabilities of medical staff, non-medical first responders and volunteers. It is agreed by all NIGHTINGALE partners and specified in the General Agreement that this substantive objective cannot be achieved without complying with legal, ethical obligations or good practices and without an awareness to societal boundaries that may exist in relation with integrating advanced technology in first response to medical emergencies, either mass casualty incidents (MCIs) or disasters- man-made or natural- herein addressed generally as MCIs.

Main risks number 21 and 29 identified in the Description of Action (DoA) – Annex I to the Amended General Agreement (GA) (see p.57 therein) are particularly relevant to the present report. Risk number 21 states: "NIGHTINGALE is not aligned with EU core values and citizen expectations". Risk number 29 states: "NIGHTINGALE meets its technical goals, yet fails to address legal, ethical, social, privacy and security issues."

The proposed solution to mitigate the risks are respectively, "Societal, legal and ethical concerns are taken into account at an early stage and constantly communicated to all partners." Furthermore, "[d]edicated tasks to address and comply Toolkit design with legal/ethical/security/social/privacy requirements and establish a relevant framework governing integration, implementation and evaluation."

The Social, Legal and Ethics Report (deliverable 1.3.) addresses these concerns and feeds first from deliverables in WP7: D7.1. (Project Management Guidebook); D7.4., (Ethics, Data Protection and Gender Handbook- see attached as Annex II of this report), D7.5. (Legal, Societal and Humanitarian Handbook- see attached as Annex I of this report); WP8 – deliverables D8.1-D8.7, followed shortly by D8.8 (due M12); as well as Milestone 3 (MS3) on ethics and data integration or E/PIA processes (Ethics and Privacy Impact Assessment) due M11; alongside: WP1- namely deliverable 1.1.; WP2, WP3, WP4 and WP5. While most deliverables in these WPs are due after the submission of this report, the report reflects preliminary discussion between partners and conclusions, as well as work in progress.

The report will serve partners leading the WPs to integrate social, legal and ethics considerations into their set of responsibilities within the NIGHITNGALE project from an early stage. It should be noted that at this stage of the project, the NIT-MR is still in design, as well as related deliverables such as the exercise of mapping of the current state of affairs in MCIs (e.g. D1.5. and other); the design and architecture of the NIGHTINGALE toolkit with functional and non-functional components, KPIs to be achieved and how to test them (task 1.7.)- all of which are the result constituting the development process in the encounter between practitioners (technology) and users (medical emergency) partners of NIGHTINGALE project. Finally, training actions of the project are also represented below in a preliminary impact assessment to which the human rights due diligence checklist is also relevant.

ACTIONS of NIGHTINGALE to which the report is specifically addressed include the distinct technical phases of the NIGHTINGALE project such as, design, development, integration, testing,

demonstration, training, and validation. Among these phases, specific care is given to data processing and the development of training material involving volunteers and possibly bystanders.

Admittedly, *FRs in MCIs and Disasters* operate within a given setting of challenges, namely the 'fog of war' and uncertainty, the need to act under pressure and emergency, limited resources and more. Equally and generally speaking, the world of *Advanced Technology* encompasses internal challenges relating namely to its accuracy (relevant to all technology), shielding from human error, inherent biases and discrimination (e.g. AI), danger of misuse- need to protect from malicious attacks (e.g. biometrics and facial recognition, tracking and tracing technology), and dual-use whereby the same technology can serve both civil and military purposes (e.g. UAVs)- the NIGHTINGALE project has exclusively humanitarian and civilian objectives.[2] Specific technology is identified as especially prone to danger, or negative effects on individual rights. This includes the use of biometrics and facial recognition, the need for transparency in decisions based on Artificial Intelligence (analysing data, learning, providing results) and inherent biases; man v machine liability and more. The report below is structured as follows: Chapter 1 sets out the inherent challenges First Responders (FRs) face in MCIs and specific needs advanced technology can address. This provides a preliminary impact assessment of the project itself on enhancing First Response in complex emergencies; Chapter 2 maps the social, legal and ethics landscape and risks; Chapter 3 provides proposed solutions to social, legal and ethics concerns.

The report is submitted at an initial stage of the 3-year project in view of the understanding that early preparedness, a risk and rights-based approach, ethics and law in design- assist in ensuring better outcomes and preventing violations partners wish to and must avoid in compliance with commitments under the General Agreement and applicable laws and best practices.

[2] Notwithstanding this fact, Emergency Medical Response may occur in 'peacetime' or in 'armed conflict' whereby different legal norms apply. Under all settings, humanitarians are protected from attack and must be allowed to perform their duties, under required conditions.

1 Inherent challenges First Responders (FRs) face in MCIs and specific needs advanced technology can address- preliminary impact assessment of the NIGHTINGALE project

1.1 FRs in MCIs face several inherent challenges (see Chapter 2 of the Legal, Social and Humanitarian Handbook for further information)

FRs operate under 'a fog of war' with greater uncertainties than certainties, as to the needs, number, identity and medical history of casualties. They operate often in insecure environments- either for natural reasons: e.g. an earthquake and recurring explosions, terrorist attacks with the need for security forces to secure the scene first. Furthermore, scarcity of resources is one of the main givens of FRs operating in MCIs and disasters. There are usually more needs than the FRs can attend. Medical needs must be identified as quickly as possible in order for available resources to be used optimally. Medical needs will indicate which treatment will be available for each of the casualties. It will also determine the evacuation from the scene, including transport priorities and destination. Moreover, FRs work in a highly stressful environment. Time means lives saved or lost, decision-making must be sound and reasonable given the circumstances- an achievement that can be reached given the correct training and preparedness done in advance. And still, human error will exist. Another angle to take into consideration in view of preparedness is that different environments present different challenges- an urban setting will require a different response than a rural, less populated and more remote from hospitals environment, for instance.

Workshops, discussions and exchange between the partners reveal (work in progress) the specific needs that technology should address when enhancing different stages of first response in MCIs and Disasters (the WHAT); and HOW designated technology can address the needs. For instance, technology that provides the answers needs also to be easily mobile (compact?), have a long enough life-span without recharging (e.g. flight capacity of UAVs), be resilient to very cold or very hot temperatures, smoke and other environmental factors. Also, the data-communication capabilities between different ACTORS and TECHNOLOGIES during an MCI or disaster are also an ACTION to take into account in relation with possible risks (See D.1.8. in progress).

1.2 A preliminary assessment of needs to enhance FR capability in MCIs (see Chapter 2 of the Legal, Social and Humanitarian Handbook for further information)

1.2.1 A preliminary assessment of needs to enhance FR in complex emergencies and where the NIGHTINGALE Toolkit (advanced technology) can have impact

A preliminary assessment of needs to enhance FR capability in MCIs and that technology may address reveals, at a preliminary stage (to be completed by D1.5., D1.10 and developments throughout the project):

- the need for quicker and better precision in the ability to localise the MCI (or disaster);
- the need to channel the information flow correctly and to avoid an overflow of data that would burden FRs' capacity to respond;
- the need to enhance triage for optimal treatment and evacuation, throughout the MCI scene;
- In order for technology to enhance FR capacity rather than burden it, FRs need to have free hands able to deal directly with the casualties.
- Technology resilience: technology that is fragile to blood stains, extreme weather or similar features will not be useful to FRs.
- FRs need simple to employ, easy to carry means of identifying patients and tracing them throughout the MCI scene.
- the need for homogenous protocols between different FRs in the same jurisdiction and among different jurisdictions – in case of a multi-national FR team;
- dealing with psychological strain of FRs: the need for training in advance (ab initio) and debriefing ex post facto.
- consent: this includes both the need to get consent from participants in the research project; in training and integration exercises; and the inability to get consent in an MCI from casualties and patients as a factor to take into account also in the design of technology.
- involvement of bystanders and volunteers in assisting FRs responding to MCI. Involvement of bystanders and volunteers should be meaningful, within the limits of the law, and should take into account their safety.

1.2.2 How the Novel Integrated Toolkit for Emergency Medical Response (NIT-MR) impacts needs

Advanced technology considered within the NIGHTINGALE project, both as means and methods to enhance First Response in MCIs and complex emergencies can serve before, during and after such emergency arises. Admittedly the design and architecture of the NIT-MR is in development. However, the general lines of impact consist in the following: Before an MCI or other complex emergency occurs, advanced technology can enhance preparedness, namely of FRs (medical and non-medical, staff and volunteers) through training; and can also maximize and optimize resource management by recording quality, quantity and location. During an MCI Nightingale toolkit can provide rapid and reliable localisation of MCI scene; identification of cause of MCI; identification of number of affected individuals; help perform triage: prioritizing patients for treatment and evacuation; monitoring change in prioritizing according to patients' evolving needs and available resources; and, enhance communication capability on different levels: communication from the scene outside the immediate MCI scene and identifying available adequate resources, enhancing the management of the emergency; communication providing FRs (including bystanders) the means to communicate reliable information relating to casualties and to the scene (e.g. METHANE information) to the central communication center managing the MCI/hospital evacuation from the scene and general response.

Seeing the NIT-MR is still in design, the legal, social and ethics impact assessment will develop from providing an overall framework of guidelines to specific and general questions that arise- to a case specific assessment. The assessment will be done from M12 to M36 and will be reflected in the final report D1.4.

2 Social, Legal, and Ethics Challenges: Landscape and Risks at the meeting point of MCIs and Advanced Technology Preliminary Impact Assessment

Keeping in mind that technology holds great potential for a greater good, when designed and used for the better of humanity, for enhancing FRs in MCIs and other complex emergencies, and assisting them in their humanitarian mission- saving life, preserving body and mental integrity and preserving human dignity; technology also holds risks to fundamental human rights, risks of discrimination, violation of the right to privacy; misuse and dual-use.

This reality presents the challenge of striking the balance between opportunity and risk. Correctly addressing the social, legal and ethics risks embedded in the two fields (medical emergency and advanced technology) as well as the specific risks arising from their meeting point, allows to lower the threats of derailing, and to ensure reaching the intended humanitarian objectives of the project, including as a lucrative initiative. A more conscientious (public and) private sector is also arguably more susceptible of reaching success. It also better reflects social realities around the world and especially in the Nightingale partner's specific societies and jurisdictions, within or outside the European Union. This is true while taking into account, the NIT-MR is designed for MCIs or disasters also outside the EU territory. Applying the NIT-MR in developing countries, facing both MCIs and disasters and other complex emergencies, may present additional or different challenges and may require adaptation at different levels. While, all NIGHTINGALE testing and integration of the NIT-MR is done within the EU (or Israel) settings, specific adaptation will be needed on a case by case basis, including after the lifespan of the project. Before proposing the solutions (Chapter 3), this Chapter sets out the main social, legal and ethics risks, respectively.

Alongside risks that have been identified in relevant Handbooks listed above, additional risks entail impact on the environment of the NIT-MR that all practitioners should take into account. This concern relates to the question of: what carbon imprint do your companies and technologies within the NIT-MR make on the environment and how do you address this concern?

2.1 Social

Social barriers to the achievement of NIGHTINGALE main objectives (summarized in the DoA – Annex I of GA) are related to social expectations and possible concerns in case the project actions would not be aligned with EU core values and citizen expectations.

Nevertheless, a note should be made to culture-specific, cultural diversity social barriers within specific communities, whereby social barriers to NIGHTINGALE will be different in one society compared to another. For instance in some societies the “triage” need to separate a mother from her children in an MCI if they belong in different categories will be acceptable, whereas in other societies this will not be acceptable. Another example having impact may be the need to keep patients’ identities and medical information completely secret, or the acceptability to physically examine women in the field by male responders. In some societies, priority will be given to the young

over the old. In others, the influential old will receive priority. These issues may be sensitive and complex to deal with and will require a culture-sensitive approach, possibly with the need to involve experts (e.g. social workers) or community leaders in the efforts invested in building social acceptance to the humanitarian objectives of enhancing FR capacity in complex emergencies by integrating advanced technology. Internal acceptance is much more prone to success than a solution imposed from what may be perceived as 'external' entities.

Notwithstanding the above, it must be stressed that cultural sensitivity does not come at the expense of fundamental rights such as the right to life and the right to bodily integrity. Some human rights are 'erga omnes' (applicable to all) and 'jus cogens' (i.e. suffer no exceptions, derogations or limitations) (e.g. the prohibition of torture). Otherwise, human rights (e.g. the right to assembly, freedom of expression) are balanced with other human rights and may be limited under specific conditions (e.g. in emergencies, in view of preserving life, dignity, preventing harm; for a limited time and in a proportionate manner- whereby the means do not exceed the legitimate end).

While freedom of conscience and religion are fundamental human rights, they come in balance and may be limited in view of ensuring life, bodily integrity and human dignity- human dignity being the most difficult fundamental right to strike a balance with freedom of conscience and religion- seeing that if it were possible to ask for consent, arguably, in some societies, individuals would choose the right to religion over the right to life in the name of human dignity- for example. Nevertheless, in liberal societies based on the rule of law and democracy, immediate humanitarian objectives and the sanctity of life are prioritized.

Citizen expectation (in an EU setting) from emergency medical response is that all Actors and Technologies align with legal, ethical and humanitarian values, best practices, norms or obligations. Therefore, social risks of rejection are closely intertwined with the legal and ethical standards applied throughout the project from design to integration.

Alongside this reality, today, there is a concern from the use of advanced technology, precautions using artificial intelligence responsibly, designing and applying technologies indiscriminately, addressing biases, protecting data, especially private data (e.g. personal details) data and sensitive data (e.g. patient data), in accordance with the rule of law and democracy. Ways in which advanced technology and data processing is protected from misuse and dual-use (i.e. ensuring the technology developed will be used exclusively for civilian, humanitarian purposes, especially in relation with tracing and tracking technology- also known as 'surveillance technology'), will also increase or decrease social acceptance of the NIT-MR and its use by medical, non-medical staff and volunteers and even bystanders.

2.2 Legal

The legal risks related to NIGHITNGALE Actions relate to non-compliance with existing legal obligations, uncertain or non-homogenous legal obligations, specific notice on non-discrimination, inclusiveness (e.g. taking into account the need to include disability in medical emergency response also when using advanced technology); obligation to protect from misuse (e.g. of data) or dual-use (civilian use entailing different legal obligations than military use, which requires specific certification and unless the military is involved in the FR to MCIs and other complex emergencies, is excluded from civilian actors).

Surveillance technology can affect rights to privacy, freedom of expression or freedom of movement. AI systems can restrict an individual’s autonomy, quality of life, or deny important benefits –

especially if leaked or used in a setting different from the one the AI was designed for. Finally, AI systems can increase barriers for people with disabilities if they are designed without considering accessibility.

AI systems can be biased or discriminatory against individuals on the grounds of race, age, disability, sex, family structure or other protected grounds. Bias in an AI system can also intersect across multiple grounds at once. Equally troubling, bias is often embedded, unexpected, undetected and coupled with the perception that machines are objective.

Specific caution must be applied as to technology aimed at Tracing –tracking, using biometrics (e.g. facial recognition), private and sensitive data under the GDPR, communication of data between different actors, technologies, or even exporting data outside the EU.

Processing data must allow take active measures to protect sensitive and private data at the risk of violation of the right to privacy.

Uncertainty as to liability (civil or even criminal), shared liability- between designer of technology, user of technology or other, liability between man and machine, differences in liability regimes in different jurisdictions. The NIGHITNGALE ambition to integrate lay volunteers into the emergency response is especially relevant here. Different jurisdictions apply different norms as to the responsibility of lay volunteers or bystanders acting or omitting to act to save lives. The question of training lay volunteers may influence the legal setting, so will potential institutional affiliation creating responsibility over the training of lay individuals. It is more cautious to express the absence of institutional affiliation by training or in the absence of an explicit mention of the existence of institutional affiliation. In rough lines, the applicable domestic liability laws will be those of the nationality of the volunteer, the nationality of the institution providing training, delivering technology or of affiliation wherever institutional affiliation exists, or/and the territory whereby the intervention occurs, possibly creating a conflict of applicable laws to be determined by the courts. Wherever possible, training brochures and programs and technology instructions must include information as to applicable laws, supported by consent forms, thereby creating an agreement and an expectancy of the applicable law. This is true, while not shielding entirely from domestic laws seeking to implement liability for malicious acts (under civil and/or criminal responsibility) or for negligence: omitting to act whereby action was obligatory by law/ or acting and creating damage whereby this damage was avoidable under the circumstances.

2.3 Ethical

Emergency medical response, advanced technology, researching in and with humans, training volunteers – all entail ethical issues. Specific risks relate to data collection and protection, use of research participants (with special emphasis on their safe conditions and on voluntariness), unexpected/incidental findings, and in complying with medical deontology, human dignity, gender equal opportunity at all levels of the Project, gender neutrality of research outcomes, non-discrimination (racial, religious, gender-orientation etc.) and overall ethics compliance issues of the tools in the NIT-MR and their use.

Also, it should be stated, NIGHITNGALE Actions are bound by GDPR (Legally binding EU regulation relating to data protection) and as such, an assessment of elements which, if relevant, would make the DPIA (Data Protection Impact Assessment) an obligation on all NIGHTINGALE partners. For more information see Annex II of this report- the Ethics, Data Protection and Gender Handbook.

2.4 Conclusion on Social, Legal and Ethical Risks

The three arms, social, legal and ethical, are interlinked. Complying with legally binding obligations, ethical standards and best practices will ensure social acceptance, legal and ethical compliance and greater chances of success for the NIGHTINGALE project as a whole and enhancing the world of Emergency Medical Response by Integrating the NIT-MR and involving broader publics (volunteers, bystanders). Of particular interest is the flexible boundary between Regulatory and best practices, where often Regulatory "delegates" to the latter an important role.

While the objectives are ambitious and entail social, legal and ethical risks, the Leads on these topics within the project offer a comprehensive monitoring and communication framework aimed at mitigating risks- as will be examined in Chapter 3.

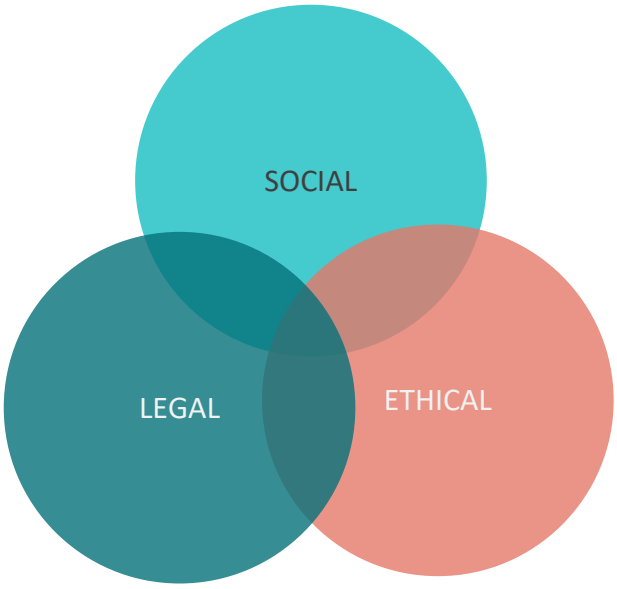

Figure 1 Social, Legal and Ethical Risks and Mitigating them are intertwined

3 Proposed solutions

The overall approach to mitigating the risks mentioned above is multiple. The social, legal and ethical managers provide a comprehensive framework to relevant issues, propose checklists, communicate obligations and guidelines throughout the project and are an integral part of the exercises of the project and of debates (see Annexes I-IV below). Also, different partners with relevant responsibilities, for example in training or communication, in developing technology and in using technology are directly solicited when necessary or approach the legal, ethics or security experts, including also the project Advisory Boards, who are at the project partners availability.

The main features of the proposed solutions are developed below.

3.1 Providing definitions for common grounds

Project partners define common denominators in the emergency medical response world and in the designated advanced technology as part of the project objectives. Notwithstanding this fact, at an early stage of the project, the need to provide common definitions was raised.

Common and clear definitions are also necessary in order to address social, legal and ethical risks. This is true seeing the Emergency Medical Response world entails different actors, different protocols and guidelines, and different solutions to the same problems in different jurisdictions.

Equally so, the field of Advanced Technology is under-regulated. Discussions exist today between lawmakers throughout the world, including the European Union and individual European or non-European State Members on whether and how to regulate the fast-paced world of advanced technology. This is also true in relation with the private business sector and creating corporate responsibility, especially in view of Business and Human Rights- i.e. relating to fields that have a specific effect on fundamental human rights, such as the field of emergency medical response and advanced technology.

To this existing setting, the NIGHTINGALE project, encompassing a multitude and interdisciplinary set of expert partners, providing clear definitions at an early stage of the project seems essential in view of ensuring a coherent social, legal and ethical framework reflecting EU values and citizen expectations.

Definitions relating to the complex emergency field as well as to data protection under the GDPR, advanced technology under any existing or in-development legislation (or guidelines) has been provided in the Legal, Societal and Humanitarian Handbook (LSHH) in Chapter 2 of the LSHH with 38 definitions (8 of which were taken from the NIGHTINGALE Medical Glossary and the NIGHTINGAL Technical Glossary, work-in-progress).

3.2 Abide by social, legal and ethical laws and guidelines applicable in your own national jurisdictions and to universal norms

Wherever there are different applicable protocols and heterogeneous legislations among partners, each partner must first abide by his/her own national/domestic settings. In this case, the presumption is that by complying with domestic legislation, the partner is complying with EU legislation and guidelines. Wherever non-EU Member States are involved, i.e. Israel-based partners; the EU has mutual recognition mechanisms and cooperation agreements including in terms of data protection, export of data and so forth. Foremost, all NIGHTINGALE Partners are from rule of law based democracies, either from EU Member States or from Associated States and are also members of the OECD which also develops relevant guidelines and to which states from which partners operate are bound.

The overall golden rule from all Partners is to do no harm and comply with the humanitarian objectives of the NIGHITNGALE Project and the Emergency Medical Response in MCIs and Disasters or other complex settings, namely, preserving the right to life, bodily and mental integrity and human dignity. These objectives are to be achieved without discrimination based on ethnic, religious, political, national, racial, gender origin or on any other factor other than the well-being of the patient in need of life saving emergency medical response.

3.3 Social

Specifically on the social front, alongside the legal and ethical aspects, solutions entail communication based on outreach to broader public, raising awareness to the humanitarian objectives of the project, possible risks and ways in which these risks are being mitigated. An active effort is necessary to receive feedback and create a communication flow or even community, relating to the field.

Communication also enables to ensure the transparency of the project and strengthen democratic acceptance and to manage citizen expectations.

Training material for partners and volunteers is also developed within the project. Such training material takes into account consent forms, information about legal and ethical obligations, namely human rights (e.g. non-discrimination, the right to privacy…).

The legal and ethics managers accompany the development of training, the publication of deliverables, and other communication to ensure compliance with social, legal and ethics aspects.

Specific Consent forms have been developed within the project from an early stage (see Annex I). Checklists relating to Human Rights Due Diligence (See Annex II), Data Protection Impact Assessments or E/PIA (see Annex IV), including concerns from fundamental human rights to the right to privacy, gender, and recently environmental concerns have been developed and disseminated among Partners

3.4 legal framework to mitigate risks: Human Rights Due Diligence

Alongside legal obligations of all NIGHTINGALE Partners under their respective jurisdictions, the proposed legal framework to mitigate risk and ensure compliance draws from the Business and Human Rights (BHR) field based on the UN Guiding Principles for Business and Human Rights, the

OECD Guidelines and relevant EU legislation or even draft legislation (e.g. the EU AI Act which adopts a risk-based approach).

The Business and Human Rights applied within the context of the NIGHTINGALE project entails a 'means responsibility' for corporate and public entities, which is a rights and risk-based approach, embodied by a 'Human Rights Due Diligence' checklist (See Annex II).

The field of Business and Human Rights consists in mapping corporate obligations to respect human rights, state obligations to protect human rights and enforce binding laws, and victims' rights for effective remedy in case of violation. An effective setting for Business and Human Rights entails processing Impact and also ensuring what is commonly referred to today as ESG compliance, aka Environmental and Social Governance, and abiding by UN Sustainable Development Goals (SDGs).

The process of early-preparedness aims to prevent violations, create awareness; create a rights environment at the early stages of design of technology or training of volunteers. The responsibility chain runs through all ACTIONS of the NIGHTINGALE project as specified in the DoA and summarized in the Introduction above. This may entail questions of liability and need of outreach and training to the public of methods of response in MCIs (e.g., civil training at schools, youth organisations, as a condition to acquiring a driver's licence and so forth. For instance integrating use of METHANE data or monitoring of patient condition (triage) in an MCI scene in emergency medical response training).

The proposed legal framework maps the comprehensive legal framework where legal obligations exist (e.g European Charter of Human Rights, GDPR…) and sets out a Human Rights Due Diligence checklist relating to existing obligations, diligent approach where non-binding or uncertainties or gaps in regulation exist, including impact and ESG (ESG which relates to the internal policies of public and private entities, such as non-harassment at work, gender equality, etc.).

Non-discrimination, protection from misuse and alertness to dual-use is specifically addressed.

3.5 Ethics and Data Protection

Ethics obligations entail legally binding and non-legally binding norms. The proposed solutions in relation with the overall ethics and data protection issues are ensured by the Ethics Manager and the Ethics Advisory Board and Independent Ethics Expert Advisor, as reflected in confidential non-public deliverables, namely in WP8.

Deliverable 7.4. the Ethics, Gender and Data Protection Handbook (Ethics Handbook) provides in-depth guidance as to ethical risk assessments and partner obligations.

In view of drawing the main lines of the Ethics folder of the project, Ethics policy include: minimization of data (process only necessary data), anonymization of data wherever possible, pseudonymisation of data wherever for instance, patient data is necessary (therefore anonymization is non-applicable); limiting sensitive data (patient data) to authorised personnel only, codifying sensitive data wherever needed; avoiding digitalizing personal data wherever this is avoidable and notifying National Data Protection Authorities (NDPA) wherever authorization is required (See Ethics Handbook for detail).

Furthermore, an Incidental Findings Policy was developed and includes a comprehensive checklist (Annex III below).

Additionally to the guidelines included in public deliverables (D7.4.) and in confidential deliverables D8.1-D8.7, Ethics Management also added a E/DPIA Checklist (Annex IV below).

Specifically on GDPR responsibility between partners and Consortium and on the applicable legal framework and necessary consent forms : The Consortium's activities must comply with GDPR because the activities imply collection and processing of Personal Data. For Example, even the collection of names, e-mail addresses and affiliation information for the participation in a workshop and sending out communications or updates constitutes Personal Data collection and processing.

The borderline between the responsibility of the Consortium and that of each beneficiary acting within the framework of the project must be explained.

Each Partner (beneficiary) is responsible for its own GDPR related actions and policy (such as data collection or processing, even if fulfilling Consortium activities) and, eventually, for any breaches or negligence. Eventual penalties will be directed towards the single Partner by the relevant Authorities.

The Consortium which is responsible towards the EU and the EC for the correct implementation of the Grant Agreement, on the other hand, is obliged to ensure that NIGHTINGALE related activities are in compliance with GDPR. Non-compliance even of a single Partner (in NIGHTINGALE related activities) may result in a Grant Agreement breach.

All Partners (beneficiaries) being SMEs, Universities, Research Organizations, Public Institutions etc. most probably, and independently from their being beneficiaries of the NIGHTINGALE project, will have adopted necessary compliance policies, such as nominating a Data Protection Officer and a series of compliance measures which to abide by.

The principal implications involving the NIGHTINGALE project are represented by:

Information to be provided and informed consent.

GDPR strictly disciplines the type of information to be provided and how consent must be obtained for collection and processing of personal data. The cases could be summarized into five sub-categories:

1. Workshops/meetings – information sheet must be provided and verbally explained and the consent form signed when there is a workshop/meeting in which questionnaires/surveys are administered or personal information is collected;
2. Questionnaires remotely administered – this is the case of questionnaires sent out by e- mail to recipients. The contents of the information sheet must be sent out together with (or in) the message and the consent form must be sent back with the filled-out questionnaire;
3. Qualitative data collected through different methods of research, e.g., via observations or interviews from case study participants;
4. SurveyMonkey - where the questionnaires on SurveyMonkey (or other online service) which do not imply collection of Personal Data nor the possibility of identifying the individual, no informed consent is required; SurveyMonkey Europe UC in any case results to be the Controller for eventual personal data;
5. By keeping a database with names, e-mail addresses and info such as affiliation or telephone numbers, you have collected and processed data. Therefore, unless you have already obtained a consent specific for NIGHTINGALE, you must contact the data subject (e.g., practitioners or stakeholder) by e-mail or other means of which record must remain, to inform them of the scope and to ask and obtain consent.

Conclusions

Social, Legal and Ethical concerns relating to the NIGHTINGALE project are an integral part of the project's chances of success. Reaching technological goals with addressing potential social concerns and expectations, legal and ethics obligations and guidelines will prevent the project from succeeding.

Early integration of Social, Legal and Ethics guidelines have been integrated into the project from the beginning, starting with the D7.1. Project Management Guidebook for example, which also address social, legal and ethical concerns and main principles.

Review of relevant legal frameworks (including the GDPR, Charter of Fundamental Rights of the European Union 2009), principles exposed in relevant privacy frameworks and guidelines (i.e. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 20134 , APEC Privacy Framework 2005 5 , Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 19856) and any relevant EU legislation on Advanced Technology has been incorporated into the relevant deliverables amounting the present preliminary report to be followed by a final report on how the guidelines have been streamlined and implemented by partners.

Wherever specific technologies contain high or medium risks, these are being addressed. Overall, seeing the humanitarian objectives of the project (Emergency Medical Response) and the engagement of its partners, the risks are low or are being addressed from design to subsequent stages of the project.

Nevertheless, it must be remembered that sensitive data (patient data) and private or personal information is being processed, raising specific obligations under the GDPR. Furthermore, even reliable technology, such as AI, entails biases; biometrics and facial recognition can be misused or have a dual-use – therefore specific precautions apply.

Finally, a strong drive on identifying issues before they become an issue is represented by an Ethics by Design and a Privacy by Design Approach, as outlined in D7.5 Legal, Societal and Humanitarian Handbook and in D7.4. Ethics, Data Protection and Gender Handbook.

The aim of Ethics by Design is to make people think about and address potential ethics concerns, while they are developing a system. An assessment of the potential ethics risks must be made in the very early development phases of design of a product and solutions must be foreseen and discussed with developers and ethics experts. The implementation can be represented by the proactive transposition of identified ethics principles in the system requirements. Inspirational for this approach are the six principles contained in the document published in November 2022 by the EC "Brandt DAINOW and Philip BREY: Ethics By Design and Ethics of Use Approaches for Artificial Intelligence".

Privacy by design, or its variation data protection by design, a multifaceted concept – as described by ENISA - involving various technological and organisational components, which implement privacy and data protection principles in systems and services is also at the centre of the Projects efforts.

The adoption of Ethics by Design and of Privacy by design, besides being a necessary instrument for compliance with European and national standards, represents also a winning approach because products or services which implement ethics and privacy by design will have a wider acceptance in a

world which is more and more sensitive to the stakes and will reduce costs of providing compliance ex-post.

Ensuring a high social, legal and ethics standard is an on-going process and will develop alongside substantive deliverables and exercises of the project. Most of all, legal, social and ethical aspects must not be perceived as separate or 'sterile' entities- they must be integrated holistically into all substantive actions and objectives of the project. Once partners of the project demonstrate embracing and compliance with legal and ethical standards, the same standards will be more accessible to external entities.

References (Heading 1)

INTERNATIONAL TREATIES, RESOLUTIONS, GUIDELINES (UN Bodies)

[1] UN Sustainable Development Goals, https://sdgs.un.org/goals

[2] UN General Assembly Resolution 45/95 of 14 December 1990, A/RES/45/95 14 December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm

[3] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, http://www.refworld.org/docid/3ddcafaac.html

[4] UN General Assembly Resolution 45/95 of 14 December 1995 adopting the Guidelines for the Regulation of Computerized Personal Data Files

[5] the International Standards on the Protection of Personal Data and Privacy (The Madrid Resolution) adopted by the ICDPPC in Madrid in 2009

[6] UN 2012 Guiding Principles for Business and Human Rights

[7] 1996 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

[8] International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands 2015, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-and-International-Humanitarian-Action.pdf

[9] WHO, Code of Conduct for Responsible Research 2021, https://www.who.int/docs/default-source/documents/ethics/code-of-conduct-for-responsible-research-pamphlet-en.pdf?sfvrsn=93f07bc9_2

[10] International Conference on Data Protection and Privacy Commissioners, International Standards on the Protection of Personal Data and Privacy, https://icdppc.org/wp-content/uploads/2015/02/The-MadridResolution.pdf

[11] Resolution on Data Protection and Major Natural Disasters adopted by the ICDPPC in Mexico City in 2011

[12] Resolution on Privacy and International Humanitarian Action adopted by the ICDPPC in Amsterdam in 2015

[13] The UNHCR Policy on the Protection of Personal Data of Persons of Concern to UNHCR (2015)

[14] The IOM Data Protection Manual (2010)

EUROPEAN, EU and OECD LAW (DIRECTIVES, REGULATIONS and GUIDELINES)

[15] The OECD Privacy Framework (2013), https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm

[16] OECD, Artificial Intelligence in Society, 2019, https://doi.org/10.1787/eedfee77-en

[17] the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), including the Additional Protocol

[18] EU General Data Protection Regulation 2016/679 (GDPR)

[19] EU Recommendation 02/2020 on Essential Guarantees in Surveillance, https://edpb.europa.eu/our-work-tools/our-

documents/recommendations/recommendations-022020-european-essential-guarantees_en

[20] The European Code of Conduct for Research Integrity, 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/european-code-of-conduct-for-research-integrity_horizon_en.pdf

[21] EUI, President Decision No. 10/2019 of 18 February 2019: Regarding Data Protection at the European University Institute, https://www.eui.eu/Documents/AboutEUI/Organization/DataProtection/PresDecision10-2019-DataProtection.pdf

[22] 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

[23] European Commission, Proposal for a Regulation on a European approach for Artificial Intelligence, 2021/0106 (COD), See in particular: recital 27, 2021/0106 (COD), https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence

[24] European Parliament, Legislative Train, Artificial Intelligence Act, https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

[25] EU Dual Use Research Guidance - Draft, 2021, https://trade.ec.europa.eu/consultations/documents/consul_183.pdf

[26] European Commission, Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe, 2021, https://digital-strategy.ec.europa.eu/en/library/study-supporting-impact-assessment-ai-regulation

[27] Ethics By Design and Ethics of Use Approaches for Artificial Intelligence (Nov. 2021, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/ethics-by-design-and-ethics-of-use-approaches-for-artificial-intelligence_he_en.pdf)

[28] ENISA – European Union Agency for Network and Information Security, Privacy and Data Protection by Design – from policy to engineering, December 2014, (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design)

EUROPEAN COURT OF JUSTICE CASE LAW

[29] ECJ, ' Schrems I ' Judgement 2015, https://eur-lex.europa.eu/legal - content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=en

[30] ECJ, ' Schrems II ' Judgement 2020, https://eur-lex.europa.eu/legal - content/EN/TXT/?uri=CELEX%3A62018CJ0311

HANDBOOKS

[31] Marelli and Kuner , Handbook on Data Protection in Humanitarian Action, 2017, https://rm.coe.int/handbook-data-protection-and-humanitarian-action-low/168076662a

[32] Inter Agency Standing Committee (IASC) of the Operational Policy and Advocacy Group (OPAG), Operational Guidance: Data Responsibility in Humanitarian Action, 2021, https://interagencystandingcommittee.org/resources?og_group_ref_target_id=19568&sort_by=field_published_date_value&sort_order=DESC&og_subspaces_view_all=1&og_subspaces_view_parent=0&f%5B0%5D=resource_audience_label%3AOperational%20Response&f%5B1%5D=resources_authored_on%3A1995-

05&f%5B2%5D=resources_authored_on%3A2000-09&f%5B3%5D=resources_authored_on%3A2008-10&f%5B4%5D=resources_authored_on%3A2011-09&f%5B5%5D=resources_authored_on%3A2013-07&f%5B6%5D=resources_authored_on%3A2015-03&f%5B7%5D=resources_authored_on%3A2016-06&f%5B8%5D=resources_authored_on%3A2020-10&f%5B9%5D=resources_authored_on%3A2021-02&s=

[33] UN Office for the Coordination of Humanitarian Affairs (OCHA), Building data responsibility into humanitarian action, 2016, https://datacollaboratives.org/static/files/framework.pdf

[34] DSEG, A Framework for the ethical use of advanced data science methods, 2018, https://www.humanitarianresponse.info/sites/www.humanitarianresponse.info/files/documents/files/dseg_ethical_framework_april_2020.pdf

[35] WHO, A Guidance Document For Medical Teams Responding To Health Emergencies In Armed Conflicts And Other Insecure Environments, 2021, https://apps.who.int/iris/bitstream/handle/10665/341858/9789240029354-eng.pdf?sequence=1

[36] OCHA, Guidance Note Series, Data Responsibility in Humanitarian Action, Note 4: Humanitarian Data Ethics,2020, https://reliefweb.int/sites/reliefweb.int/files/resources/guidance_note_ethics.pdf

[37] Sydney University, Research Code of Conduct 2013, https://www.sydney.edu.au/dam/corporate/documents/news-opinions/research_code_of_conduct_2013.pdf

[38] A Framework for the Ethical Use of Advanced Data Science Methods in the Humanitarian Sector, 2020, https://www.hum-dseg.org/dseg-ethical-framework

ICRC

[39] The ICRC Rules on Personal Data Protection (2015)

[40] the ICRC Professional Standards for Protection Work (2013)

[41] ICRC Humanitarian Charter and Minimum Standards in Disaster Response 2004, https://www.refworld.org/pdfid/3d64ad7b1.pdf,https://www.icrc.org/en/doc/resources/documents/misc/64zahh.htm

ONTARIO LAW COMMISSION

[42] The Law Commission of Ontario Report, "Accountable AI", released 17 June 2022, https://www.lco-cdo.org/wp-content/uploads/2022/06/LCO-Accountable_AI_Final_Report.pdf

SCHOLARSHIP- ACADEMIC PUBLICATIONS, ARTICLES, BLOGS, BOOK CHAPTERS

[43] Ashok Hans and Reena Mohanty, Disasters, Disability and Technology, Development, Volume 49, Number 4, December 2006, pp. 119-122(4)

[44] Gwynnyth Llewellyn, Dale Dominey-Howes, Michelle Villeneuve and Alexandra Lewis-Gargett, Disability and Disaster Risk Reduction, Emergency Preparedness, Scoping Review, November, 2016 The University of Sydney's Centre for Disability Research and Policy (CDRP) and Asia Pacific Natural Hazards and Disaster Risk Research Group

[45] John Twigg, Maria Kett and Emma Lovell, Disability inclusion and disaster risk reduction, Overcoming barriers to progress, July 2018
[46] Disability Inclusion In Disaster Risk Management Promising Practices And Opportunities For Enhanced Engagement, World Bank Group and Global Facility for Disaster Reduction and Recovery, 2017
[47] Ben Weisner, Disability and Disaster, REsearchGate, 2012
[48] A´lvarez-Garcı´a C, Ca´mara-Anguita S, Lo´pez-Hens JM, Granero-Moya N, Lo´pez-Franco, MD, Marı´a-Comino-Sanz I, et al. (2021), Development of the Aerial Remote Triage System using drones in mass casualty scenarios: A survey of international experts. PLoS ONE 16(5):e0242947. https://doi.org/10.1371/journal.pone.0242947
[49] Sarah Soliman, Tracking Refugees With Biometrics: More Questions Than Answers, War on the Rocks Blog, 9 March 2016, https://warontherocks.com/2016/03/tracking-refugees-with-biometrics-more-questionsthan-answers/
[50] Ethical Guidance for Disaster Response, Specifically Around Crisis Standard of Care: a systematic review. Am J. of Public Health. Leider J.P., De Bruin et al 2017; 107(9)
[51] Johnson AM, Cunningham CJ, Arnold E, Rosamond WD, Zègre-Hemsey JK. Impact of Using Drones in Emergency Medicine: What Does the Future Hold? Open Access Emerg Med. 2021;13:487-498, https://doi.org/10.2147/OAEM.S247020
[52] Cliem, N. and McKenzie, A-M., Digital Dignity in Practice: Existing digital dignity standards, pursuing digital dignity and current gaps in digital dignity, 2019, https://www.alnap.org/help-library/digital-dignity-in-practice-existing-digital-dignity-standards-pursuing-digital-dignity
[53] Repine, The Dynamics and Ethics of Triage: Rationing Care in Hard Times, 2005, https://mercyhighered.org/wp-content/uploads/2020/04/Dynamics-and-Ethics-of-Triage-Rationing-Care-in-Hard-Times.pdf
[54] 'Chatham House Rules', UK Royal Institute of International Affairs, June 1927, Chatham House official website: https://www.chathamhouse.org/about-us/chatham-house-rule?gclid=Cj0KCQjwrs2XBhDjARIsAHVymmTWZ5V4CGbjTE4NBEWJpmmfChOH4JlJ-7BoBl5qA5ZWeVJHbw-66GsaAjKiEALw_wcB
[55] Koskimies et al, The informational privacy of patients in prehospital emergency care—Integrative literature review, 2020, https://onlinelibrary.wiley.com/doi/abs/10.1111/jocn.15481
[56] White, Lo, A Framework for Rationing Ventilators and Critical Care Beds During the COVID-19 Pandemic, 2020, https://jamanetwork.com/journals/jama/article-abstract/2763953
[57] Albahri et al, Systematic Review of Real-time Remote Health Monitoring System in Triage and Priority-Based Sensor Technology: Taxonomy, Open Challenges, Motivation and Recommendations, 2018, https://link.springer.com/article/10.1007/s10916-018-0943-4
[58] Stewart, Dwivedi, Artificial intelligence and machine learning in emergency medicine, 2018, https://onlinelibrary.wiley.com/doi/abs/10.1111/1742-6723.13145
[59] De Stefani, Using social media in natural disaster management: a human-rights based approach, 2017, http://phrg.padovauniversitypress.it/2017/2/3
[60] Burkle, Advanced Triage Management for Emergency Medical Teams, 2019, https://www.researchgate.net/profile/Frederick-Burkle/publication/338489109_Advanced_Triage_Management_for_Emergency_Medical_Teams/links/5e1b71e392851c8364c8d5e8/Advanced-Triage-Management-for-Emergency-Medical-Teams.pdf

[61] Winn et al, Medical Volunteers during Pandemics, Disasters, and Other Emergencies: Management Best Practices, 2021, https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjel11&div=13&id=&page=
[62] Jaskula, Siuta, Simple Emergency Triage (SET) the new perspective on mass casualty incident triage, 2020, https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/263940/jaskula_siuta_simple_emergency_triage_set_2020.odt?sequence=2&isAllowed=y
[63] Nielsen, Utilitarian Triage in Disasters, 2021, https://heinonline.org/HOL/LandingPage?handle=hein.journals/byulr46&div=8&id=&page=
[64] Hodge et al, Volunteer health professionals and emergencies: assessing and transforming the legal environment, 2005, https://pubmed.ncbi.nlm.nih.gov/16181044/
[65] Perate et al, The Use of Simulation in Disaster Medicine Preparedness, 2020,https://www.semanticscholar.org/paper/The-Use-of-Simulation-in-Disaster-Medicine-Perate-Rodgers/762735daa8bce9b431c624f97414dcc59afe98ff
[66] Alvares-Garcia et al, development of the Aerial Remote Triage System using drones in mass casualty scenarios: A survey of international experts, 2020, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242947
[67] Montano et al, 'Mobile Triage Applications: A Systematic Review in Literature and Play Store,2021, https://link.springer.com/article/10.1007/s10916-021-01763-2
[68] Johnson et al, Impact of Using Drones in Emergency Medicine: What Does the Future Hold, 2021, https://www.dovepress.com/impact-of-using-drones-in-emergency-medicine-what-does-the-future-hold-peer-reviewed-fulltext-article-OAEM
[69] Merchant et al, Integrating social media into emergency-preparedness efforts, 2011, https://www.nejm.org/doi/full/10.1056/nejmp1103591
[70] Jayshree Pandya, The Dual-Use Dilemma of Artificial Intelligence, Forbes, 2019
[71] Hodge et al, The Pandemic and All-Hazards Preparedness Act, 2007, https://www.researchgate.net/publication/6388781_The_Pandemic_and_All-Hazards_Preparedness_Act_Improving_Public_Health_Emergency_Response
[72] Ebben et al, Adherence to guidelines and protocols in the prehospital and emergency care setting: a systematic review, 2013, https://pubmed.ncbi.nlm.nih.gov/23422062/
[73] Abelsson et al, Learning by Simulation in Pre-hospital Emergency Care, 2016, https://pubmed.ncbi.nlm.nih.gov/26333061/
[74] Nimmorlrat et al, Patient triage system for supporting the operation of dispatch centres and rescue teams, 2021, https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01440-x
[75] Zhang et al, Evaluative research of technologies for prehospital communication and coordination, 2020, https://pubmed.ncbi.nlm.nih.gov/32246206/
[76] Zoltowska et al, Preparedness of Health Care Workers and Medical Students in University Hospital in Krakow for Covid-19 Pandemic within the CRACoV Project, 2021, https://www.mdpi.com/2077-0383/10/16/3487
[77] Hempel et al, Allocation of Scarce Resources in a Pandemic, 2021, https://pubmed.ncbi.nlm.nih.gov/34048911/
[78] Emerging Technologies in Emergency Situations, 2021, https://www.researchgate.net/publication/353738439_Emerging_Technologies_in_Emergency_Situations_Guest_Editorial

[79] Afzali et al, The impact of the emergency medical services automation system on patient care process and user workflow, 2021, https://bmcmedinformdecismak.biomedcentral.com/articles/10.1186/s12911-021-01658-9
[80] Blank and Jensen, LOAC and the Protection and Use of Digital Property in Armed Conflict, 2021
[81] Cahane, The Right not to Forget: Cloud Based Services Moratoriums in War Zones and Data Portability Rights, 2021, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3944667
[82] Cliem, N. and McKenzie, A-M., Digital Dignity in Practice: Existing digital dignity standards, pursuing digital dignity and current gaps in digital dignity, 2019, https://www.alnap.org/help-library/digital-dignity-in-practice-existing-digital-dignity-standards-pursuing-digital-dignity
[83] Cochrane, Data Subject Access Rights and Military Agencies: A Comparative Perspective, 2020, https://csrcl.huji.ac.il/blog/protecting-privacy-and-data-protection-times-armed-conflict
[84] Crawford, The Right to Privacy and the Protection of Data in Situations of Detention in Armed Conflict', 2020
[85] Davenport, The use of Camble Infrastructure for the Interception and Collection of Data During Armed Conflict: Are There Any Limits?, 2021
[86] Hellwig, Investigation of Grave International Crimes', 2021
[87] Housen-Curiel, Managing Data Privacy Rights in Multilateral Coalition Operations' Information Sharing Platforms: Towards a "by Design and by Default" Model, 2021
[88] Oconnell, Data Privacy Rights: The Same in War and Peace', 2021
[89] Rejali, Saman and Heiniger, Yannick, The Role of Digital Technologies in Humanitarian Law, Policy and Action: Chartering a Path Forward, 2021, https://international-review.icrc.org/articles/digital-technologies-humanitarian-law-policy-action-913
[90] Ronen, The Right to be Forgotten and International Crimes, 2021,
[91] Shany and Mimran, Integrating Privacy Concerns in the Development and Introduction of New Military or Dual Use Technologies, 2021, https://openscholar.huji.ac.il/csrcl/event/yuval-shany-tal-mimran-article-36-ap1-vehicle-integrating-privacy-concerns-development
[92] Shehabi, Digital Privacy Rights, Data Protection and the Law of Occupation, 2021
[93] Van De Velde, From Telegraphs to Terabytes: The Implications of the Law of Neutrality for Data Protection by "Third" States and the Corporations Within Them, 2021
[94] Watt, NATO CCDCOE 'Rights to Privacy and Data Protection in Armed Conflict' Research Project, 2021, https://ccdcoe.org/research/data-protection-and-privacy-in-armed-conflict/
[95] West, Facial Recognition Technology use in Armed Conflict: A Case Study of the Relationship between Privacy and Precaution, 2021
[96] Dorothy Leonard-Barton, William A. Fraus, Implementing New Technology, Harvard Business Review, https://hbr.org/1985/11/implementing-new-technology
[97] Katam Raju Gangarapu, Ethics of Facial Recognition: Key Issues and Solutions, January 25, 2022 (blog guest post), https://learn.g2.com/ethics-of-facial-recognition
[98] I. Raji and G. Fried, About Face: A Survey of Facial Recognition Evaluation, 2021, https://arxiv.org/pdf/2102.00813.pdf
[99] D. Leslie, Understanding bias in facial recognition technologies, The Alan Turing Institute, 2020, https://zenodo.org/record/4050457#.YH7RdTHivD4
[100] M. Wang and W. Deng, Deep Face Recognition: A Survey, 2020, https://arxiv.org/pdf/1804.06655.pdf

[101] Tambiama Madiega and Hendrik Mildebrath, Regulating facial recognition in the EU- in-depth analysis, European Parliamentary Research Service (EPRS), Members' Research Service PE 698.021 – September 2021, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf

[102] B.Kind, Containing the canary in the AI coalmine – the EU's efforts to regulate biometrics, Ada Lovelace Institute, 2021, https://www.adalovelaceinstitute.org/blog/canary-ai-coalmine-eu-regulate-biometrics/

[103] G. Malgieri and M. Ienca, The EU regulates AI but forgets to protect our mind, 7 July 2021, https://europeanlawblog.eu/2021/07/07/the-eu-regulates-ai-but-forgets-to-protect-our-mind/

[104] N. Smuha and others, "How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act", August 2021

Appendices

ANNEX I: CONSENT FORMS

Final templates of informed consent/assent forms and information sheets (in language and terms intelligible to all participants) including personal data processing

Information sheet/informed consent template for research participants (English)

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 capacity to survive and the feeling of safety and provide affected people the 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 in a mass casualty incident scene, 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 outmoded technology. NIGHTINGALE will develop, integrate, test, deploy, demonstrate, and validate a Novel Integrated Toolkit for Emergency Medical Response (NITMR) 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-triage is the initial evaluation of sick and injured patients) by offering them the means to perform digital identification, allow traceability, support fast diagnosis and prognosis and continuous monitoring and enable accurate classification of medical condition; 2) optimising pre-hospital life support and damage control through Artificial Intelligence (AI)-based tracking, tracing, routing and utilisation 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 Programme.

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 needless to say, but 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). Personal data is 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, data concerning health, 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.

All potential risks have been assessed and all 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.

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 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 and 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 contact 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 scopes of the project, the stored personal data may be, only potentially such as when data storage space is physically located outside the EU, transferred to and from non-EU countries, in compliance with GDPR and relevant legislation.

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.

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: ……

ANNEX II: Human Rights Due Diligence (Checklist), including International Human Rights Law, namely, dignity, privacy, gender, non-discrimination and Environmental and Social Governance (ESG)

Human dignity, right to life and right to the integrity of the person		
	Y/N NA (Not Applicable)	Comments (for internal use of the organization)
Does your organisation have a code of conduct recognizing and embracing principles of human dignity, right to life and right to the integrity of the person?		
Does your organisation include human dignity, right to life and right to the integrity of the person when training personnel?		
What risks to human dignity, life and the integrity of the person is relevant in the activities of your organisation?		
Does your organisation apply any decision-making process based on algorithms?		
If yes, can this application have any effect on human dignity, right to life or right to the integrity of the person?		
Would your organisation benefit for a specific training within Nightingale on these universal principles and on how to implement them in relation to the activities of your organisation?		
For any questions please contact the project LSHM		

Right to private and family life

	Y/N NA (NotApplicable)	Comments (for internal use of the organization)
Does your organisation have a right to private and family life policy?		
How does your organisation implement the right to private and family life of its workers ?(staff or volunteers)		
How does your organisation implement the right to private and family life of its patients ?(staff or volunteers)		
How does your organisation implement the right to private and family life of its customers ?(staff or volunteers)		
Does your organisation include content on the right to private and family life in training?		
Does your organisation have an internal/or external and independent review mechanism in case of breach?		
How do you ensure the independence of the mechanism? (free from internal pressure)?		
Does your organisation have a focal point for complaints of breach ?		
For any questions please contact the project LSHM		

Right to protection of personal data

	Y/N	Comments (for internal use of the organization)
Does your organisation have a protection of personal data policy?		
If not, have you adopted specific measures to implement the protection of personal data?		
When training personnel do you include guidelines for the protection of personal data?		

Does the training or documentation policy include identifying when and what personal data is processed?		
Is there an awareness in your organisation of what personal data is and that it includes sensitive data (e.g. patient data)?		
Does your protection of personal data policy include special measures for the processing of personal data? (anonymization, pseudonimisation, minimisation of data policy…)		
Is access to personal data secured by passwords? Restricted to authorized personnel? Include regular refreshment of passwords and similar safeguards		
Does your organisation have a Data Protection Officer (DPO)?		
Does your organisation have an internal review mechanism and focal point to prevent breach and in a situation of breach?		
Would your organization benefit from a specific training session in the Nightingale framework?		
Further questions or doubts? Please share them with the LSHM		

Gender equality and non-discrimination policy[3]

	Y/N	Comments (for internal use of the organization)
Does your organization have an equal opportunities and non-discrimination policy?		
If not, 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		

[3] Extracted from D7.4 Ethics Handbook.

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		

Anti- harassment and non- sexual or gender based violence or any other form of violence including bullying at work

	Y/N	Comments (for internal use of the organization)
Does your organisation include an anti-harassment policy and a zero tolerance to any sexual/gender-based or other form of violence?		
Do you include periodic training of this policy?		
Is there a focal point for anti-harassment and zero tolerance to any form of violence (especially sexual-based violence) in your organisation?		
Is there an internal review mechanism in case of breach?		
Would your organisation be interested in training within the framing of Nightingale?		
For any further information please contact the project LSHM		

Misuse and Dual-use Risk Mitigation

	Y/N	Comments (for internal use of the organization)

Does your organisation handle any of the following : sensitive data, large-scale data processing, drones (UAVs), biometrics, tracking and tracing software, facial recognition, automated data processing, Artificial Intelligence?		
If yes, is there a risk mitigation from misuse or dual-use policy?		
If not, are there any special measures implemented?		
If any of your relevant personnel be asked at random what does misuse and dual-use mean in the context of your activity- would he/she know to answer?		
Does your staff (including management) follow specific and periodic training on mitigating risk of misuse/dual-use?		
Is there a focal point and internal review mechanism on risk mitigation of misuse and dual-use?		
Would you and your organisation be interested in training within Nightingale?		
For any further information please contact the project LSHM		
Environmental and Social Governance (ESG)		
Does your company apply an ESG policy?		
Would you wish to receive training on ESG relating to your company products in view of NIGHTINGALE NIT-MR?		
Do you know the carbon imprint of your technology developed within the NIT-MR?		
How are you addressing carbon imprint concerns in view of complying with environmental and social governance policies within the EU?		
Are you reaching out to public audiences (outreach, training, conferences) in view of creating greater transparency as to your contribution to the NIGHTINGALE project and its humanitarian objectives? (to enhance		

Medical Emergency Response through technology, while integrating human rights due diligence, data protection impact assessments and ESG)		

ANNEX III: Incidental findings policy and checklist

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 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 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, but not 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

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 referable 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, ethics experts or panel)?	
Is there a timeframe involved indicating the urgency of the issue?	

ANNEX IV: Data Protection Impact Assessment (E/PIA Checklist)

Dissemination Risk Assessment Checklist

This checklist, to be used before any such activities, is finalized at assessing privacy, security and ethics risks deriving from dissemination and communication activities.

1)	Is any personal data contained?	
2)	Would the information to be disseminated produce harmful effects on any individual or group?	
3)	Have all risks been considered?	
4)	Is there an awareness that once disseminated or published, data will not be under the control of those responsible for the dissemination or publication?	
5)	Has the dissemination level of data to be released been checked?	
6)	Have, if required, all authorizations been obtained?	
7)	Have IPR issues been considered?	

Data Protection Impact Assessment support checklist

Does any of the following apply in your activities related to NIGHTINGALE tasks (which require you to make a Data		

Protection Impact Assessment – DPIA)?		
	A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly affect the natural person	
	Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences	
	A systematic monitoring of a publicly accessible area on a large scale	
If yes, to which aspect of the Project would this apply?		
	Questionnaires or data collection during Workshops/meetings	
	Questionnaires remotely administered (e.g., e-mail), including questionnaires finalized at the organization of the event	
	Questionnaires administered through a web service (e.g., Surveymonkey or other commercial services)	
	Maintaining a database of individuals (e.g., contat and affiliation information of experts), wether previosly collected or no	
	other	

If you had any doubts, have you consulted your Data Protection Officer for an opinion?		
Does your National regulatory require you to provide the Data Protection Authority with any communication about collection / processing of personal data applicable to the NIGHTINGALE Project?		

If you have any further doubts or questions on the DPIA please contact nightingale@ethics-helpdesk.eu