



*Platform for European Medical Support
During Major Emergencies*

D8.2 Review of Ethical Issues Affecting PULSE



Title:	Document Version:
Review of ethical issues affecting PULSE (Ethical Impact Assessment Report)	V1.0

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
31/10/2016	31/10/2016	R, PU

Responsible:	Organisation:	Contributing WP:
David Wright	Trilateral Research Ltd.	WP8
607799	PULSE	Platform for European Medical Support during major emergencies

Authors (organisation)

Lead authors: Rowena Rodrigues, David Wright, Inga Kroener (Trilateral Research Ltd.).

Contributors: Clare Shelley-Egan (Trilateral Research Ltd.), Francesco Malmignati (Leonardo Finmeccanica), Paul Kiernan, Jacinta Bourke & Karl Chadwick (Skytek Ltd.), Reinhard Hutter (CESS GmbH).

Abstract:

This document is the Ethical Impact Assessment (EIA) report and documents the research, actions taken, and recommendations resulting from PULSE work package 8 (Legal, ethical and societal impact). The report is a living document that has been regularly updated during the project. It was distributed at key stages to the project partners, the PULSE Ethical Review Committee (ERC), and published on the PULSE website for public comments. The document examines the ethical, legal and societal issues related to the PULSE platform; outlines the ethical, legal and societal issues in the context of the PULSE scenarios; presents the results of the internal and external ethical impact assessments of the PULSE tools, and addresses data protection issues. Finally, it summarises how the PULSE project integrates the EIA outcomes and presents the final conclusions and recommendations of WP8.

Keywords:

Ethical Impact Assessment, ethical, legal and societal impact, ELSI, public health ethics

<DOCUMENT> MAIN REVISIONS:

Revision	Date	Description	Author/contributor (Organisation)
0.1	2 September 2015	Draft revised and issued to Ethical Review Committee and the PULSE consortium	Rowena Rodrigues, Inga Kroener, David Wright (Trilateral Research)
0.2	September-2015	Post-ERC+Consortium meeting revisions	Rowena Rodrigues (Trilateral Research)
0.3	October-April 2016	Development of material for sections Input from technical partners	Rowena Rodrigues, Inga Kroener, David Wright (Trilateral Research) Francesco Malgminati (Leonardo Finmeccanica/Selex) Paul Kiernan & Karl Chadwick (Skytek)
0.4	May 2016	WP8 stakeholder consultations input	Rowena Rodrigues (Trilateral Research)
0.5	July-September 2016	Post-EVD trial input Post-MCI trial input	Rowena Rodrigues, David Wright (Trilateral Research)
0.6	September-October 2016	Review of document and feedback	PULSE Ethical Review Committee members (Prof. Dr. Philip Brey & Dr Javier Arias-Diaz, Ms. Zuzanna Warso) CESS, SKYTEK, Dr David Smith (Royal College of Surgeons in Ireland)
1.0	October 2016	Final revisions	Rowena Rodrigues & David Wright (Trilateral Research Ltd.)

Contents

1	Executive Summary	5
2	Introduction to the PULSE ethical impact assessment.....	13
2.1	The purpose of an EIA.....	13
2.2	Project description.....	13
2.3	EIA/LEPPI team.....	15
2.4	Terms of reference	16
2.5	Methodology.....	16
2.5.1	<i>Stakeholder engagement and consultations.....</i>	<i>17</i>
2.5.1.1	Workshops with end users	19
2.5.1.2	Interviews with external stakeholders.....	19
2.5.2	<i>Identification of ethical principles, threats, vulnerabilities, risks and mitigation measures relevant to PULSE</i>	<i>21</i>
2.6	Timeline.....	28
2.7	Components of the PULSE platform.....	28
3	The PULSE platform: ethical & legal principles and guidance	32
3.1	Protection of ethical and legal principles	32
3.2	Recommendations in EGE opinions relevant to PULSE.....	34
3.3	Other considerations in emergency preparedness and response	38
3.4	Critical infrastructure: legal and regulatory issues.....	40
3.5	Systems and information security: ethical principles	41
3.6	Data protection	47
3.7	Ethical and other issues in training	50
3.8	Legal & ethical considerations for, and during the trial exercises	51
4	PULSE pilot scenarios.....	51
4.1	Introduction	51
4.2	EVD scenario: ethical, legal and societal issues	53
4.3	MCI scenario: ethical, legal and societal issues.....	54
4.4	Resource triage and allocation: important considerations.....	55
4.5	Legal issues in public health emergency management	56
5	Ethical impact assessment of PULSE tools, technologies and procedures	57
5.1	Internal ethical risk assessment	57
5.2	External ethical risk assessment (interview-based)	58

5.3	Other results of stakeholder consultations held in April 2016	65
5.4	Addressing data protection	68
5.4.1	<i>PULSE data controller</i>	69
5.4.2	<i>Mapping of information flows in the PULSE system</i>	70
5.4.3	<i>Addressing data protection risks</i>	71
5.4.4	<i>Data protection post-project completion</i>	74
5.5	Ethical, economic, legal, political and societal (EELPS) assessment with trial exercise participants	74
5.6	Integrating EIA outcomes into the project	75
6	Conclusions and recommendations	75
	Annex 1: Ethics approvals: form and approvals	78
	Annex 2: Preliminary stakeholder identification	84
	Annex 3: Semi-structured interview guide	86
	ANNEX 4: Mapping ISO 29001 principles to threats, vulnerabilities, risks and mitigation measures	88
	Annex 5: International legal frameworks for preparedness planning and response to public health emergencies	95
	Annex 6: Updated overview of relevant EU and international critical infrastructure legislation and guidelines	98
	Annex 7: PULSE trials LEPPi checklist	99
	Annex 8: Informed consent forms – trials	100
	Annex 9: Scenario characteristics	106
	Annex 10: Internal ethical risk assessment of PULSE tools	108
	Annex 11: External risk assessment of PULSE tools – data	126
	Annex 12: Data protection guidance checklist	127
	Annex 13: EELPS questionnaire	128
	Glossary	130
	References	133

1 EXECUTIVE SUMMARY

Aim of the document

This document is the PULSE ethical impact assessment (EIA) report and documents the research, actions taken, and recommendations resulting from PULSE work package 8 (Legal, ethical and societal impact). The report is a living document that has been continually updated throughout the duration of the project, was distributed at key stages to the project partners, the PULSE Ethical Review Committee (ERC), and published on the PULSE website for public comments¹.

Structure of the document

Chapter 2 introduces the PULSE EIA. Chapter 3 examines the ethical, legal and societal issues related to the PULSE platform. Chapter 4 examines the ethical, legal and societal issues in the context of the PULSE scenarios; important considerations in resource triage; and legal issues in public health emergency management. Chapter 5 presents the results of the internal and external ethical impact assessments of the PULSE tools, and addresses data protection issues. It also summarises how the PULSE project integrates the EIA outcomes. Chapter 6 presents the conclusions and recommendations. The report's annexes contain the materials that supported the PULSE EIA process and include ethics approvals, stakeholder identification list, mapping of ISO principles, updated overview of relevant EU and international critical infrastructure legislation and guidelines, PULSE trials LEPPi checklist, informed consent forms, external risk assessment of pulse tools, data protection checklist, and the Ethical, Economic, Legal, Political and Societal (EELPS) Assessment questionnaire.

The project and aim of the EIA

PULSE is an EU-funded FP7, end-user-driven project that has developed a sustainable technical and operational platform for the health services that will provide health service stakeholders (i.e., ambulance personnel, hospitals and national agencies) with access to key data and medical information to enable them to prepare and to respond effectively during a major medical crisis. The EIA carried out in PULSE investigated and monitored the ethical, legal and societal issues related broadly to public health emergencies, and specifically to the PULSE system.

Team

Trilateral Research, the leader of WP8, functioned as the LEPPi (Legal, Ethical, Privacy and Policy Issues) officer and oversaw activities related to the legal and ethical aspects of PULSE across all work packages. Onest Solutions and UCSC contributed expertise in systems and information security, by facilitating the identification of ethical and legal factors to be considered in developing systems

¹ <http://www.pulse-fp7.com/pulse-ethical-impact-assessment-report-call-for-feedback/>

for the support of the emergency healthcare service. The technical partners (Leonardo Finmeccanica and Skytek) contributed their inputs to the risk assessment of the PULSE tools. CESS and Trilateral collaborated in the development of the ethical, economic, legal, political and societal (EELPS) assessment methodology presented more fully in the deliverables D7.1 and D7.3 of WP7.

The PULSE Ethical Review Committee (ERC) comprised three external, independent experts, namely, *Dr. Javier Arias-Díaz*, Full Professor of Surgery, School of Medicine – San Carlos Clinic Hospital, Complutense University of Madrid; *Professor Dr. Philip Brey*, Professor of Philosophy of Technology, Department of Philosophy of Technology, University of Twente; and *Ms. Zuzanna Warso*, Helsinki Foundation for Human Rights. The objectives of the PULSE ERC were to monitor ethical concerns that may arise within the PULSE project, provide ethical approvals, advice and input on key ethical issues affecting the project, and help disseminate relevant project deliverables.

Methodology

The PULSE EIA process included the following steps: (1) develop the EIA plan, (2) identify stakeholders, (3) consult stakeholders, (4) identify and analyse ethical impacts, (5) check whether the project complies with legislation, (6) identify risks and possible solutions, (7) formulate recommendations, (8) prepare and publish the EIA report, (9) implement recommendations, (10) third-party review. The LEPMI team assumed the primary responsibility for the steps in the process, supported by the PULSE consortium partners. While most of the steps were largely sequential in nature, several were repeated at various stages in the project, e.g., review of the risks and possible solutions, and consultation with stakeholders (at project events, via interviews etc.).

Stakeholder engagement

One important objective of an EIA is to engage stakeholders to help identify, discuss and find ways of dealing with ethical issues arising from the development of new technologies, services or products. Engaging stakeholders enables the assessor to identify risks and impacts that she/he may not otherwise have considered. PULSE engaged with stakeholders at two levels: internal and external.

Internal stakeholders included the consortium partners and end users who represent a variety of interests and expertise. Engagements with such partners occurred via project meetings (face to face and virtual), workshops, the project's trial exercises, and e-mails.

External stakeholders included hospitals, community health services, emergency care services, first responders, international health organisations, civil society organisations, policy-makers, industry and ethicists. The PULSE project consulted with such stakeholders by various means, notably project workshops with end users (i.e., direct users of the services, procedures and applications resulting from PULSE; managers with decision-making roles etc.), interviews with internal

and external stakeholders conducted via telephone or Skype or other similar means, e-mails and attendance at third party events. A major part of external stakeholder engagement were the interviews conducted with external stakeholders in April 2016, which sought views on ethical, legal and social issues related to the PULSE platform to inform the project.

Ethical, legal and social principles

This deliverable contains a repository of ethical, legal and social principles (relevant to PULSE) extracted from the *Universal Declaration of Human Rights*, *EU Charter of Fundamental Rights*, *The European Convention on Human Rights (ECHR)*, *ISO/IEC 29100 Information technology -- Security techniques -- Privacy framework*, an initial literature review and discussions with stakeholders in PULSE workshops. The repository maps the principles against potential threats, vulnerabilities and risks, and outlines potential mitigation measures, based on a literature and good practice review. The repository (presented in table format) is a heuristic one that helped the PULSE consortium understand ethical principles with which it needs to comply, helped identify and locate ethical issues in consultation with both PULSE partners and stakeholders, and helped identify the corresponding potential threats, vulnerabilities and risks. The repository is designed to be transferable to other similar projects.

The key principles covered include: human dignity, right to life, right to the integrity of the person, liberty and security, respect for private and family life, personal data protection, freedom of expression and information, freedom of assembly and of association, equality before the law, non-discrimination, gender equality, protection and well-being of children, right to health, emergency derogations, confidentiality, fairness, duty to steward resources, trust, duty to provide care, protection of the public from harm, access to healthcare, reciprocity, equity and animal welfare.

The ISO ISO/IEC 29100 Information technology Standard principles covered include: consent and choice, purpose legitimacy and specification, collection limitation, data minimisation, accuracy and quality, openness, transparency and notice, individual participation and access, accountability, information security, privacy compliance.

Ethical issues in the PULSE scenarios

The PULSE framework solution was validated by two pilot scenarios, based on multiple exercises and demonstrations: (a) an emerging viral disease (EVD), i.e., a SARS-like virus epidemic in Italy and (b) a mass casualty incident (MCI) i.e., a major stadium 'crush' at a concert. The project team presented and discussed these scenarios with representatives of the core stakeholders to validate and complement the scenarios. Stakeholders included, inter alia, health care institutions, emergency services, medical personnel, industry, businesses, data protection authorities, and organisations representing citizens' interests (normally civil society organisations).

In **scenario (a)**, the identified ethical issues at stake included individual liberty, proportionality, privacy of personal information, the public right to know, duty to steward resources, trust, duty to provide care, protection of the public from harm, reciprocity and equity. The key recommendations are:

- Public health practitioners, emergency managers and policy-makers should **consider ethical values** (e.g., individual liberty, proportionality, privacy of personal information, the public right to know, duty to steward resources, trust, duty to provide care, protection of the public from harm, reciprocity and equity, fairness of distribution of medication or vaccines, prioritisation of response and treatment and respect for religious beliefs) in making decisions in a SARS-like pandemic.
- They should also **consider procedural values** such as reasonableness, openness and transparency, inclusiveness, responsiveness and transparency in making decisions regarding the allocation of scarce resources.
- **Accountability mitigation is a crucial issue** in the preparedness and response phases of major medical emergencies. Lawyers, public health practitioners and emergency managers often have to prioritise and resolve legal issues on the basis of incomplete information and guidance during emergencies.
- In some instances, the exigencies of the situation may allow for a **derogation of normal legal requirements**, particularly regarding over-triage, balancing of individual liberties, privacy or personal² and sensitive information, duty to manage resources and duty to provide care notwithstanding personal risks and accountability mitigation.

In **scenario (b)**, the identified ethical issues include how to allocate resources in a disaster situation while considering practical issues such as likelihood of benefit, change in quality of life and duration of benefit and ethical values such as fairness and justice. The key recommendations are:

- Public health practitioners and policy-makers should **set policy guidance regarding acceptable over-triage rates** as an important input into the development of tactical procedures.
- Public health practitioners and policy-makers should **support first responders in the design of processes and procedures**. They should consider legal issues relating to implementing crisis standards of care including questions concerning co-ordination of health services, liability and, where relevant, inter-jurisdictional co-operation.

Results of the internal risk assessment of the PULSE tools

In the internal risk assessment exercise in WP8, Trilateral and the technical partners Leonardo Finmeccanica (previously Selex) and Skytek collaboratively evaluated each individual tool of the PULSE platform. This exercise (carried out between November 2015 and February 2016) enabled the technical and WP8

² See Recital 4 of the General Data Protection Regulation which states that “The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.”

teams to reflect upon the risks, stimulate discussion of the mitigation measures and take steps needed in the final integration of the PULSE platform.

Annex 10 documents the full results of the internal ethical risk assessment of the PULSE tools, i.e., it highlights the threats, vulnerabilities, risks, likelihood, potential impact and recommended mitigation measures. While this exercise did not identify any risks with high likelihood, they marked some **risks as having 'medium likelihood'** including ineffective delivery of healthcare for individuals and communities; adverse impact on the relationship between patients as a group and organisations involved (such as clinical teams, hospitals), denial of service attacks, data breaches, discrimination, failure of the emergency healthcare system and the possibility of erroneous results. They highlighted **certain risks with potential serious impact** including data breaches with significant security and privacy impacts, human suffering or loss of life, amplification of effects of the crisis, and legal prosecution of, and adverse impacts on crisis managers (both individuals and organisations).

Results of the external risk assessment of the PULSE tools

Additionally, PULSE partners discussed some key risks, their likelihood and the potential impacts of the PULSE tools with external stakeholders in interviews carried out in April 2016. We briefly summarise the results here.

The level of the likelihood of the **information confidentiality and system security risks** depends on how confidentiality and security are handled; if the system is open to breaches, then the risk would be high.

The likelihood of the **risks of human suffering, amplification of crisis effects** is low if the platform works well. The potential impact would be negligible if effects are effectively addressed.

The risk of **adverse impact on decision-makers' abilities** was stated to depend on the structure, implementation and integration of the platform. The risk would also be low if addressed in training.

The **risk of mis-assessing the crisis or emergency**, both the risk likelihood and potential impact, depends on how the system is integrated, and its level.

The risk of **ineffective co-ordination and management of the health emergency events** is a function of training and management, i.e., poor co-ordination equals high risk; if it is dealt with, it has low risk.

Both the likelihood and potential impact of the risk of **ineffective delivery of healthcare for individuals and communities** depend on how the system is integrated, its level and the resources that are available. There might be a problem if doctors rely more on data and the system than on their intuition.

The risk to privacy and personal data depends on the type of personal data collected, handled and shared. This risk might not be applicable in an emergency scenario.

The potential impacts of the risk of **violation of intellectual property rights (IPRs)** depend on how IPR are addressed; there might be a potential negative impact if proprietary information is used.

The risk of an **adverse impact on relationships between patients (as a group) and organisations involved** depends on the organisations of teams, training and communications with, and awareness of patients. Its likelihood depends on whether the system duplicates existing efforts.

The risk of **surveillance via profiling and geotagging** might have a negative impact. If people will be tracked, they must be informed. If people don't accept tracking, there might be an infringement of their rights. The risk likelihood is high due to a risk of misuse outside emergency context; the potential impact would be serious if people decide not to use the system due to surveillance concerns.

The risk of psychological and other unforeseen harms is also real; for example, if people are transferred outside their country and culture in a public health emergency, then they may become distraught. This risk likelihood may also depend on who can access their images and medical information.

The **risk of discrimination in relation to treatment of patients** depends on the criteria of prioritisation. It will be low if international standards are followed. If other criteria that aren't based on high ethical standards are used, then the risk likelihood will be high, and potential impact could be catastrophic.

The risk of the **irrelevance and future redundancies of the PULSE training tools** is low if the PULSE tools are continually updated.

The risk of **unethical and unprofessional actions by trainees** is always likely, but has a low level of likelihood if proper training is provided. If not, the likelihood of the risk is high, with a corresponding serious impact.

Stakeholders interviewed suggested the risk of **harm to vulnerable groups and individuals** was low. For example, international regulations and guidelines make provisions for overriding of consent in emergency, and deal with circumstances under which consent is difficult to obtain (e.g., disease).

Data protection

PULSE partners nominated data protection officers for their organisations to foster data protection compliance across the consortium by bearing responsibility for ensuring that their organisation complies with data protection law, PULSE WP8 and Ethical Review Committee advice, and recommendations on data protection.

The consortium consulted with data protection authorities, i.e., PULSE contacted the Irish Data Protection Commissioner's Office in July 2016 to verify if there was a need for notification. The Irish Data Protection Commissioner's Office reviewed the PULSE informed consent form for the Cork trial in August 2016 and made

useful recommendations, following which the partners revised and finalised the form.

As a critical step in data protection, the PULSE team mapped the flows of personal information within the PULSE (future fully implemented) system so that these flows can be readily understood by the project and decision-makers. This deliverable specifically assesses three sets of data protection risks i.e. risks to individuals, risks to organisations using the PULSE system, and data protection compliance risks, and presents recommendations to mitigate these risks. To support good practice both in PULSE and other similar projects, Annex 12 contains a data protection checklist.

Conclusions and recommendations

Listed below are the key recommendations that emerged from the work carried out in PULSE WP8 – these also reflect the views of the various stakeholders with whom PULSE engaged.

Recommendations for policy-makers

- Policy-makers should foster **respect for fundamental rights in the implementation of public health emergency measures**.
- Member States should **monitor public health emergency measures**, particularly those implemented by private companies and agencies, to ensure they are bound by the same **legal and ethical obligations**, and should put in place mechanisms to **monitor compliance** with such obligations.
- Public health emergency policymaking should pay attention to the **following principles**: provide care notwithstanding personal risks, accountability mitigation, privacy of personal and sensitive information, and over-triage or under triage.
- If the PULSE project proceeds to commercialise its system, stakeholders involved in the commercialisation should promote and create **buy-in** from senior people, national leaders, healthcare delivery leaders at the government and ministerial level (including different DGs of the EC).
- Industry and policy-makers should collaborate in the development of **effective, shared strategies and promote discussion on reducing potential legal complications** in cross border cooperation and collaboration in emergencies.

Recommendations for the implementers and end users of the PULSE system

- Stakeholders involved in implementing the PULSE system should ensure it is done in a **co-ordinated manner** – considering the complexities and practicalities of the public health emergency management.
- The PULSE system managers **should share knowledge** with users and the public, ensuring **transparency** of the system.
- **The PULSE system users should respect the purpose limitation principle**, i.e., using the system only for its designated purpose, demonstrating legitimate use and minimising the potential for misuse of the system outside an emergency context.

- The PULSE system implementer should support training for operators, and employees on how to manage ethical issues.
- Health managers **should be accountable for how they use or process personal data.**
- PULSE system end users should have a **good understanding** of the differences in healthcare practices and priorities across jurisdictions; they consult relevant authorities to develop this understanding.
- **PULSE system end users should** create better media and **public awareness** about the usefulness of the system and the way risks will be managed.

Recommendations for designers and developers of similar systems

- Designers and developers of similar systems should **consult the PULSE EIA and EELPS assessment results as a reference point**, and review the recommendations of other relevant projects that have considered ethical, legal and societal aspects.
- They should **conduct a privacy impact assessment and/or ethical impact assessment** (e.g., using the tools such as EELPS assessment proposed in PULSE) in consultation with relevant stakeholders.
- They should consider, address, review and improve (as technology progresses) the **security and integrity** of the system, and **protect it against internal compromises and external attacks**. They should use strong encryption and optimise access controls.

2 INTRODUCTION TO THE PULSE ETHICAL IMPACT ASSESSMENT

This chapter first introduces the purpose of an ethical impact assessment (EIA). After this it describes the project, the EIA/LEPPI team, outlines the PULSE EIA terms of reference, the methodology followed, timeline and the describes the components of the PULSE platform.

2.1 THE PURPOSE OF AN EIA

New technologies, projects, products, services, policies and programmes may raise ethical and social issues ranging from privacy concerns to issues relating to asymmetries of power and fairness.³ For these reasons, there is a need to conduct an EIA in the early stages of development and the entire lifecycle of a new technology or system, in order to assess the risks and in turn to adopt measures to mitigate those risks.⁴ An EIA is a process by which an organisation (or project consortium, as is the case with the PULSE project⁵), together with stakeholders (including end users), considers the ethical issues or impacts posed by a new project, technology, service, programme, legislation, or other initiative, in order to identify risks and solutions.⁶ An important part of an ethical impact assessment process is the preparation of a report, which includes: a description of the EIA process, a risk assessment, and recommendations for the implementation of the recommendations.

This document is the PULSE ethical impact assessment report and documents the research, actions taken, and recommendations resulting from of PULSE work package 8. The EIA report (a living document) has been distributed at key stages to project partners, in addition to stakeholders, and published on the PULSE website for public comments⁷. All partners of the PULSE project are expected to be familiar with the report and aware of the ethical/legal/societal issues highlighted in the report. The EIA was updated on an ongoing basis during the project duration.

2.2 PROJECT DESCRIPTION

PULSE is an end user-driven project that aims to develop a sustainable technical and operational platform for the health services. This platform will provide stakeholders within the health services (i.e., ambulance personnel, hospitals and national agencies) with access to key data and medical information to enable them to prepare and to respond effectively during a major medical crisis. The PULSE project aimed to:

- To develop a standardised approach to improve preparedness, response and decision making across Europe for major medical emergencies.

³ Wright, D., "A framework for the ethical impact assessment of information technology", *Ethics Inf. Technol.*, Vol. 13, 2011, pp. 199-126.

⁴ Ibid.

⁵ <http://www.pulse-fp7.com>

⁶ Wright, op. cit., 2011.

⁷ <http://www.pulse-fp7.com/pulse-ethical-impact-assessment-report-call-for-feedback>.

- To provide an operational and technical framework (suitable for the EU level) to enable risk managers to undertake a threat analysis, situation assessment and forecast and to react accordingly with effective decision making, resources and logistics planning, assignment and control.
- To develop innovative technology and tools to support preparedness, response and decision making and present a common operational picture to emergency personnel.
- To analyse the measures planned to deal with a major health incident, their social acceptance, legal and ethical implications (for technology and procedures).
- To develop a set of technologies and tools meant to improve the preparedness and reliability of European states to manage a major medical crisis.
- To provide validated procedures adequate to improve the operation and success of the healthcare system in challenging disaster situations where combined operations are required at local, regional, cross border and international levels.
- To support key decision makers, by integrating a suite of models/simulations and analysis tools able to provide insights into the collective behaviour of the Health Service.

The PULSE framework solution was validated by two pilot scenarios, based on multiple exercises and demonstrations: (a) a SARS-like virus epidemic in Italy and (b) a major stadium 'crush' at a concert. The project team presented and discussed these scenarios, with representatives of the core stakeholders to validate and to complement the scenarios. Stakeholders include, inter alia, health care institutions, emergency services, medical personnel, industry, businesses, data protection authorities, and organisations representing citizens' interests (normally non-governmental organisations).

The EIA carried out as part of PULSE investigated and monitored the ethical, legal and societal issues related to emergency management affecting various stakeholders. The activity focused on ensuring that key ethical and legal issues relating to the two scenarios were identified and understood. Specifically, a repository⁸ of legal, ethical and social issues associated with a stadium crush and SARS-like virus crisis will ensure that stakeholders and policy-makers unfamiliar with such crises can seek guidance on issues such as possible human rights infringements and resource allocation issues. In addition, the study of the legal and ethical impact of the tools and technologies, developed in the project, will help ensure that they are compliant with both national and European regulations and developed in an ethically responsible manner.

The main objectives of the EIA for the PULSE project are:

- To investigate the critical infrastructure (and the critical infrastructure information system) that will form the physical framework conditions for the development of the PULSE platform, specifically regarding legal and regulatory concerns and data security and data protection issues.

⁸ See Appendix 1, Deliverable 8.1. Plan for Ethical Impact Assessment 2.
http://www.pulse-fp7.com/pdfs/D8_1_Review_of_Ethical_Issues_Affecting_PULSE.pdf

- To conduct an ethical impact assessment of the tools, technologies and procedures developed in the PULSE project to ensure that they comply with ethical standards as well as relevant national and European regulations regarding security of information systems, privacy and data protection and confidentiality.
- To review ethical principles relevant to systems and information security and facilitate the identification of ethical factors to be considered in developing systems for the support of the emergency healthcare service
- To investigate EU policy initiatives in the field of protection of ethical principles and in the field of major emergency management and analyse and assess how these two sets of initiatives might impact on each other.
- To consider ethical issues arising from the two pilot scenarios, with a focus on allocation of resources.

The EIA has been conducted both in relation to the PULSE tools and the system. The EIA exercise engaged with the pilot scenarios, as the tools, technologies and procedures were tested in the scenarios. As mentioned above, a preliminary ethical, legal and societal analysis was first carried out on the specific features of the scenarios themselves.

2.3 EIA/LEPPI TEAM

Expertise for the EIA can be found within the consortium. Partners have the following responsibilities:

- TRI functioned as the LEPPI (Legal, Ethical, Privacy and Policy Issues) officer and oversaw activities on legal and ethical aspects of PULSE across all PULSE work packages.
- Onest Solutions and UCSC contributed expertise in systems and information security, by facilitating the identification of ethical factors to be considered in developing systems for the support of the emergency healthcare service.
- Technical partners contributed their inputs to the risk assessment of the PULSE tools.
- CESS and TRI collaboratively developed a methodology for the analysis of ethical, economic, legal, political and societal impacts in the trial exercises.

PULSE has an Ethical Review Committee (ERC) comprising three external, independent experts:

- *Dr. Javier Arias-Diaz*, Full Professor of Surgery, School of Medicine – San Carlos Clinic Hospital, Complutense University of Madrid
- *Prof. dr. Philip Brey*, Professor of Philosophy of Technology, Department of Philosophy of Technology, University of Twente
- *Ms. Zuzanna Warso*, Helsinki Foundation for Human Rights.

The objectives of the PULSE ERC were: to monitor ethical concerns that may arise within the PULSE project, provide ethical approvals, advice and input on

key ethical issues affecting the project and help disseminate relevant project deliverables.

The LEPPi Officer provided a copy of the draft EIA report (Deliverable 8.2) to the ERC in early September 2015 and held a joint ERC plus Consortium meeting on 28 September 2016 via GoToMeeting. Following this, Deliverable 8.2 was revised in line with the ERC recommendations. The consortium sent *Deliverable 7.1 Trials Definition* to the ERC on 4 May 2016 for ethical approval (Annex 1 contains the ethical approval form and responses). The consortium took the ERC recommendations into account both in the final version of the Deliverable and in the trial exercises. The LEPPi Officer issued a final draft version of D8.2 to the ERC on 23 September 2016 for comments, after which the PULSE consortium organised a final WP8 meeting with the ERC and consortium on 17 October 2016. Following this, the LEPPi team finalised the Deliverable for submission to the Commission.

2.4 TERMS OF REFERENCE

In a normal EIA, the EIA team formulates an EIA plan, which includes its terms of reference. It is very important that the EIA team's terms of reference are explicitly agreed between the EIA team and senior management. In the case of the PULSE EIA, the project's Description of Work (DoW) prescribed its terms of reference. The DoW forms part of the contract between the PULSE consortium and the European Commission. In line with its mandate, PULSE conducted a legal, ethical and societal impact assessment in WP8 which engaged project partners and external stakeholders to help assess any impacts or risks that might directly or indirectly arise from the project, and to identify possible solutions to the identified risks.

2.5 METHODOLOGY

The steps in Wright's ethical impact assessment⁹, guided the EIA process in PULSE. The PULSE process followed the steps illustrated below:

⁹ Wright, David, "Ethical Impact Assessment", in J. Britt Holbrook and Carl Mitcham (eds.), *Ethics, Science, Technology and Engineering: A Global Resource*, 2nd edition, Macmillan Reference, Farmington Hills, MI, USA, 2015, pp. 163-167.

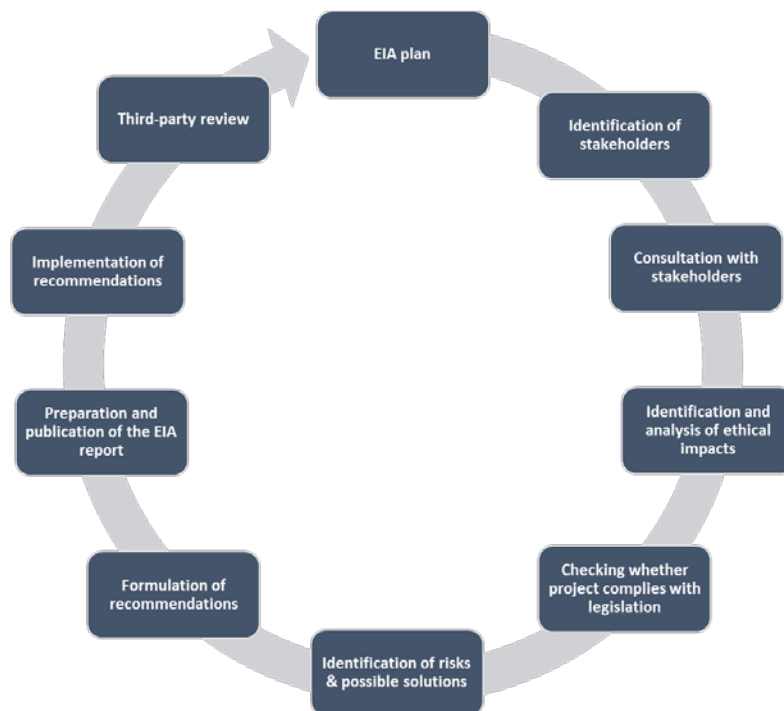


Figure 1: PULSE EIA process

The LEPPi team assumed the primary responsibility for all the steps in the process, supported by the PULSE consortium partners. While the steps were largely sequential in nature, many of these were repeated at various stages in the project e.g. review of the risks, and possible solutions, and consultation with stakeholders (at project events, via interviews etc.).

2.5.1 Stakeholder engagement and consultations

One important objective of an EIA is to engage stakeholders to identify, discuss and find ways of dealing with ethical issues arising from the development of new technologies, services or products. Engaging stakeholders enables the assessor to identify risks and impacts that she/he may not otherwise have considered. A good EIA includes consultation with internal and external stakeholders.

Internal stakeholders (in the case of PULSE) include the consortium partners/end users who represent a variety of interests and expertise:

- **Skytek Ltd (co-ordinator):** software development company that develops information and operation-based software tools.
- **CESS GmbH (Centre for European Security Strategies):** supports public, private and multinational decision-makers with the development of scenarios and expertise to meet strategic threats, and offers strategic, operational and technical security and risk management expertise.
- **ONEST Solutions SRL:** Romanian R&D SME offers engineering and system integration services, hardware and software products development, and project management and consultancy.
- **Trilateral Research:** SME research and advisory consultancy, focussed on privacy and data protection; security and surveillance; crisis & disaster management; data science, and ethics and human rights.

- **Universita Cattolica Del Sacro Cuore (UCSC):** The School of Medicine of UCSC (focussed on research, training and healthcare) provides healthcare at the Policlinico Universitario “A. Gemelli” in Rome, with 1,400 beds and a turnover of 70,000 patients annually, providing all clinical specialties.
- **Leonardo – Finmeccanica (i.e. previously SELEX ES SPA):** has expertise in electronic and information technologies for defence systems, aerospace, data, infrastructures, land security and protection and sustainable ‘smart’ solutions.
- **Health Services Executive (HSE)/Inter Agency Emergency Management Office (IAEMO) Ireland:** whose responsibilities include the support of agencies in the planning and preparation for their response to major emergencies in the Cork and Kerry Area, review and issuing of the completed major emergency plans to Principal Response Agencies (PRAs) and the preparation of pre-test planning, public consultation, testing and reviewing of the 14 Upper Tier COMAH¹⁰/SEVESO sites in the region.

The following diagram illustrates PULSE external stakeholders:



Figure 2: PULSE stakeholders

The PULSE project consulted with stakeholders by various means, notably as follows: project workshops with end users (i.e. direct users of the services, procedures and applications resulting from PULSE; managers with decision making roles etc.), interviews with internal and external stakeholders conducted via telephone or Skype or other similar means, e-mails, and attendance at third party events.

¹⁰ Control of Major Accident Hazards involving Dangerous Substances.

With the intent of contributing to future health and emergency management policies and legislative developments regarding ensuring preparedness and response during a major crisis, the PULSE LEPPI team kept a watch on policy consultations at the EU and select national level that were relevant to PULSE.¹¹ The LEPPI team participated in Westminster Health Forum¹² Keynote Seminar on *Electronic patient records and IT in the NHS*, held at Glaziers Hall, London on 9 February 2016 attended by healthcare industry representatives, academia, government agencies such as the Cabinet Office, department of health, media, ICO, NHS England, patients4data, GPS, first responders, MHRA, and NHS trusts. PULSE provided a short contribution to the briefing document of the event based on research in WP8.

2.5.1.1 Workshops with end users

PULSE convened end user workshops in PULSE work packages where user requirements of various stakeholders were considered. The consortium organised the following workshops at which members of the end user groups and other key stakeholders were invited to contribute crucial inputs to the project:

- Workshop 1 Validation of preliminary user requirements with users group (Rome, 18 July 2014¹³)
- Workshop 2 Validation of PULSE First Prototype Users Group/EVD trial exercise (Rome, 30 June- 1 July 2016¹⁴)
- Workshop 3 Validation of PULSE Second Prototype Users Group and general public/MCI trial exercise (Cork, 15 September 2016¹⁵)

Note, that during the first 18 months of the PULSE project, UCSC, CESS, ONEST conducted interviews for end-user requirements, interviews with stakeholders, and a preliminary usability testing with end users that will use the PULSE platform during the table top exercise.

2.5.1.2 Interviews with external stakeholders

The PULSE WP8 (LEPPI) team conducted interviews with external stakeholders in April 2016.¹⁶ The aim of the interviews was to seek external stakeholder views on ethical, legal and social issues related to the PULSE platform to inform the project.

¹¹ The LEPPI team subscribes to the European Observatory on Health Systems and Policies Observatory e-Bulletin, follows Public Health England via Twitter, and is involved with the work of International Association for Information Systems for Crisis Response And Management (ISCRAM).

¹²A policy makers' engagement forum.

¹³ This workshop had 13 participants (10 end-users and 3 partners with end-user experience or role).

¹⁴ This exercise involved around 20 key actors with responsibilities into the management of the emergency situations from WHO, ECDC, national and regional authorities and representatives of hospitals.

¹⁵ This exercise had 55 participants including emergency first responders (fire, police, health care).

¹⁶ <http://www.pulse-fp7.com/pulse-project-launches-external-stakeholder-consultations-on-legal-ethical-and-societal-issues/>

The first step in the process was the identification of a variety of stakeholders (Annex 2) in consultation with the PULSE consortium partners and the PULSE Ethical Review Committee, and the cross checking with stakeholders already consulted in other WPs of PULSE. PULSE identified a range of stakeholder contacts (around 50) during the process. The WP8 team designed a semi-structured interview guide (Annex 3), information sheet and consent form¹⁷ on input required for the project.

The WP8 team issued 50 invitations (along with the PULSE information sheet) were issued via personalised emails to a variety of stakeholders in various EU countries such as Austria, Belgium, Cyprus, Czech Republic, Germany, Greece, France, Italy, Malta, Netherlands, Slovenia, Sweden, Switzerland, (such as academic ethics centre, alliance of patients and the medical technology industry, civil society organisations, community health services, data protection authorities, emergency medical services, EU humanitarian agency, EU level and national policymakers, hospitals, international health organisations, public health authority, patient support organisations, related EU projects, national ethics committee, professional association, rescue services and research ethics committee). The WP8 team sent follow up emails. PULSE published information about the consultations (information sheet¹⁸ and semi-structured interview guide¹⁹) on the PULSE website²⁰ and the Twitter accounts of Trilateral Research Ltd (official and personal).

11 positive responses to invitations were received. Out of these, 7 interviews were conducted and 1 written response was received. The entities/organisations represented were: academic/ethical (Sant'Anna School/Institute of Law, Politics and development; The Medical School, University of Sheffield; University of Edinburgh), hospital, emergency medicine (Italian National Institute for Infectious Diseases), ethics committee (Irish Council for Bioethics/EUREC member), representative organisation of the National Associations of Medical Specialists in the European Union (i.e. Karolinska Institutet Department of Emergency Medicine, Södersjukhuset), related EU projects (EDEN, TACTIC, ECOSSIAN). The interviewees were from Belgium, Italy, Ireland, UK and Sweden.

The interviewers were senior researchers from Trilateral Research Ltd. and the interviews were conducted via phone and Skype and lasted between 30 to 45 minutes. Interviewees were provided interview guides and informed consent forms prior to the interviews. Some of the interview guides were tailored based on the field of expertise of the interviewee.

The interviewers prepared interview summaries and the data from these has fed into various sections of this Deliverable e.g. section 5.2 (ethical risk

¹⁷ Available at: <http://www.pulse-fp7.com/wp-content/uploads/2016/04/PULSE-Information-Sheet-for-Interviews.docx>

¹⁸ <http://www.pulse-fp7.com/wp-content/uploads/2016/04/PULSE-Information-Sheet-for-Interviews.docx>

¹⁹ <http://www.pulse-fp7.com/wp-content/uploads/2016/04/PULSE-questionnaire.docx>

²⁰ <http://www.pulse-fp7.com/pulse-project-launches-external-stakeholder-consultations-on-legal-ethical-and-societal-issues/>

assessment), section 5.3 (other results of the consultations) and section 7 (conclusions and recommendations). The LEPPi team communicated the data from these interviews to the PULSE consortium in a WP8 session at the PULSE Plenary meeting (Dublin, 9 May 2016) so that the consortium could take them actively into account in the development and finalisation of the PULSE system.

2.5.2 Identification of ethical principles, threats, vulnerabilities, risks and mitigation measures relevant to PULSE

The LEPPi team, in consultation with stakeholders, endeavoured to assess the impact of ethical issues on the PULSE initiatives, the kinds of risks these ethical issues might pose for the PULSE initiatives, and possible solutions to the risks. Again, the ethical risk management strategies set out below also have a heuristic function.

Based on the general ISO risk assessment methodology, this section maps these ethical principles to threats, vulnerabilities, risks and potential mitigation measures. A *principle* refers to an accepted or professed rule of action or conduct or underlying values. A *threat* is something that can exploit a *vulnerability* and cause damage. When a threat turns into an actual event, it may cause an unwanted incident. It is unwanted because it may harm the project or the organisations involved. A *vulnerability* is a weakness or gap in the project/platform/its tools. This weakness could allow it to be exploited and harmed by one or more threats. A *risk* is the uncertainty of achieving the objectives of the project, which is to provide a platform for EU medical emergencies that conforms to EU ethical values and principles. *Mitigation measures* are means of eliminating, reducing or controlling the adverse impact.

The table below contains ethical, social and legal principles (relevant to PULSE) from the *Universal Declaration of Human Rights*, *EU Charter of Fundamental Rights*, *The European Convention on Human Rights (ECHR)*, ISO/IEC 29100²¹, an initial literature review and discussions with stakeholders in PULSE workshops. It maps each of the principles against potential threats, vulnerabilities, risks and outlines some mitigation measures, based on a literature and good practice review. The table is a heuristic one intended to provide guidance to the PULSE consortium in understanding the ethical principles with which we need to comply, to help to identify and locate ethical issues in consultation with both PULSE partners and stakeholders, to help identify the corresponding potential threats, vulnerabilities and risks. The table is also designed to be transferable to other similar projects.

²¹ ISO/IEC, ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy framework.
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123. ISO/IEC 29100:2011 provides a privacy framework which specifies a common privacy terminology; defines the actors and their roles in processing personally identifiable information (PII); describes privacy safeguarding considerations; and provides references to known privacy principles for information technology.

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
Human dignity	No choice afforded to individuals	Tools/system does not afford individual participation and choice	Violation of right to human dignity	Informed consent and choice policies and procedures (unless derogation permitted)
	Insensitivity and discrimination	Tools enable discrimination between individuals.	Discrimination.	Dignity in medical care Non-discrimination policy and procedures.
	Untreated pain & poor standards of care	Difficulty in reaching patients, administering medicines.	Impact of quality of individual and social life. Loss of confidence and trust in PULSE	Improvement of access to pain treatment. Improved health policies. Training.
Right to life	Critical and widespread cases of life threatening conditions	Inability to co-ordinate and address multiple crises at once	Death Human suffering Loss of trust	Protection against arbitrary life threatening decision making. Access to life saving medication and resources. Robust multi-crisis co-ordination strategies.
Right to the integrity of the person	Lack of informed consent	No informed consent policies.	Violation of the right to integrity.	Free and informed consent for individuals to be ensured according to procedures laid down by law.
Liberty and security of the person	Unauthorised detention of individuals.	Lack of policy, procedural clarifications about medical detention policies, non-discrimination policies.	Violation of the right to liberty and security of the person.	Detention of individuals only if within the law e.g. mental illness, capability to spread infectious diseases. Restrictions proportional to harm and applied without discrimination.
Respect for private and family life	Non-consensual or compulsory medical treatment or	Consent issues are not addressed.	Violation of right to respect for private and	Private and public hospitals to adopt appropriate measures for the

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
	examination.		family life.	physical integrity of their patients, whose consent, based on a full understanding and knowledge of the consequences of an operation, should be obtained before any medical intervention is performed
	Surveillance of patients and other individuals.	Tracking of individuals. Lack of notice.	Unlawfulness of actions.	Surveillance should be authorised and consistent with EU and national laws
	Disclosure of personal information to other entities/people without consent; Unauthorised access to personal data including medical data	Slack information sharing/control policies.	Violation of right to respect for private and family life	Ensure confidentiality of medical records. Set up access management policies. Public authority to ensure interference is in accordance with the law, pursues a legitimate aim and is necessary in a democratic society.
Protection of personal data	Data falls into the wrong hands/shared across organisations	Collection and storage of medical data and other medical records;	Regulatory and public backlash.	Ensure high standard of data protection and data security is followed Lawful, or consent based processing of data. Data access and rectification policies
Freedom of expression and information	Lack of information about the decisions taken by public authorities and the rationale for	PULSE does not show how limited medical resources will be allocated/distributed to the public in a	Public confusion and lack of clarity about PULSE. Mistrust.	Show how limited medical resources will be allocated/distributed to the public in a pandemic).

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
	those decisions	pandemic)		
Freedom of assembly and of association	Restrictions on right to assembly and association in pandemic/crisis.	No free and open communication process about containment/restrictions in pandemics/crises.	Adverse economic effects or the restriction of civil rights and civil liberties	Pandemic preparedness planning and cross country co-ordinated approaches to pandemics. Public information and awareness.
Equality before the law.	Threat to specific needs of groups that generally face health challenges, such as higher mortality rates or vulnerability to specific diseases.	Lack of provision for the differences and specific needs of groups.	Discrimination of individuals. Violation of rights.	System of health protection providing equality of opportunity for everyone to enjoy the highest attainable level of health Equal and timely access to basic health services
Non-discrimination	Health care recipients might be discriminated against on ethically irrelevant grounds of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation.	Lack of provision for compliance with human rights legislation	Discrimination of individuals.	Ensure respect for Article 21 of the EU Charter and Article 14 of the ECHR. Outline non-discrimination policy.
Equality between men and women	Gender biases.	Inadequate addressing of gender-specific health risks and diseases	Discrimination between individuals and violation of the right.	Raising awareness of rights and facilitating their integration and access to

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
				education and health care.
Protection and well-being of children	Children are might be subject to high levels of trauma.	Does not address/deal with child vulnerability in emergencies	Adverse impact on child health Child mortality	Holistic treatment and adequate response to children's needs in crisis and emergencies.
Right to health	Ill treatment/lack of treatment to patients due to health status and/or other grounds.	Discrimination of patients/victims because of health status and/or other grounds	Health inequalities Worse health outcomes	Access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. Adoption of anti-discrimination policies. Provision of adequate information and support.
Derogation in time of emergency	Unwarranted declarations and extensions of emergencies	Adoption of measures not strictly required by the situation	Failure of democracy Loss of public trust and confidence Tyranny.	Fulfilment of requirements set by the treaty law, such as qualifications of severity, temporariness, proclamation and notification, legality, proportionality, consistency with other obligations under international law, non-discrimination, and lastly, non-derogability of certain rights recognized as such in the relevant treaty.
Confidentiality	Breach of confidentiality	Transfer of data to third parties	Harm to individuals	Robust confidentiality

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
	Wrongful disclosure/exposure of medical information	Unencrypted medical information	Lawsuits.	policy. Data security measures.
Fairness	Unfavourable treatment	Unfair allocation choices	Harm to individuals.	Fair crisis standards of care protocols Policies should reflect awareness of existing disparities in access to care Advance ethical guidance for medical emergencies.
Duty to steward resources	Scarcity of resources in a public health disaster	Inability to channel resources in emergency	Public tensions. Emotional and physical stress	Ethically and clinically sound policy.
Trust	Mistrust	Some users/public are more familiar with the system; others less so.	Resistance in using/accepting the system.	User and public engagement process. Existence of accountability and transparency mechanisms
Duty to provide care notwithstanding personal risks	Healthcare workers do not provide care due to imminent health risks to themselves/their families	No mechanisms in place to ease moral burden of those with the duty to care	Inadequacy in care Larger number of casualties/fatalities	Special facilities and additional safeguards to protect and care for health workers who face risks.
Protection of the public from harm	Threat to individual liberty	Constraints on individual freedom of movement (e.g. quarantine)	Loss of trust. Public confusion.	Stakeholders are made aware of (a) medical and moral reasons for public health measures, (b) benefits of compliance and (c) consequence of non-compliance.

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
				Mechanisms to review public health decisions made in emergency.
Access to healthcare	Those entitled to healthcare services do not receive them.	Geographical and other constraints	Inadequate support. Lower quality of care and poor outcomes.	Fair approaches to allocating and providing access to healthcare.
Reciprocity	Healthcare workers do not perform optimally.	No support or lack of for those facing a disproportionate burden in protecting the public good.	Those facing increased risks or burdens do not feel supported.	If healthcare workers are expected to work during a pandemic, benefiting their communities, access to recommended protective measures should be assured.
Equity	Lack of treatment for some patients	Patients in medical emergency get precedence over others needing urgent treatment for other diseases	Discrimination. Lack of procedural fairness.	Decision makers to strive to preserve equity between interests of different patients
Animal welfare	Epidemic or pandemic itself and measures to curtail them.		Possible impact on local, regional animal populations	Monitoring of pandemic. Defined quarantine procedures. Establish medical response procedures for common hazards.

Table 1: Ethical principles, threats, vulnerabilities, risks and mitigation measures

Annex 4 includes a Table that maps ISO 29001²² privacy principles relevant to PULSE to: threats, vulnerabilities, risks and mitigation measures.

²² Ibid.

Following this initial identification of ethical issues, risks and appropriate risk management strategies, the consortium has collaboratively worked towards implementation of appropriate procedures and processes to address these. However, we recognise that the use and implementation of some of the mitigation measures outlined above will lie with other stakeholders that take up the PULSE system (the end users) and with policy makers at the EU and national level.

2.6 TIMELINE

The duration of an EIA may be determined by some practical exigencies. In the case of the PULSE project, the EIA was conducted during the project. Listed below are the timings and the key milestones of the PULSE EIA.

- February 2015: Final submission of D8.1 to European Commission.
- September 2015: Draft D8.2 provided to ERC, followed by joint ERC and PULSE consortium virtual meeting (28 September 2015).
- October 2015-December 2015: Revision of D8.2 based on ERC feedback. Liaison with PULSE project partners on PULSE tools ethical risk assessment.
- January–March 2016: PULSE tools ethical risk assessment. Preparation for targeted stakeholder consultations.
- April 2016: Targeted stakeholder consultations (internal technical partners and external stakeholders).
- May 2016: Incorporation of results of targeted stakeholder consultations (external interviews) into D8.2. D7.1 sent for ethics approval to ERC. Revision of D7.1 revised in line with ERC recommendations. Ethical aspects support to trial exercises.
- June-July 2016: Feeding of stakeholder consultation results into D8.2/to partners. Publication of results on website. PULSE EVD trial exercise.
- August 2016: Revision of D8.2. EVD trial EELPS assessment & results analysis.
- September 2016: PULSE MCI trial exercise. Finalisation of D8.2. Submission of draft to ERC. Publication of D8.2 draft for public comments.
- October 2016: MCI trial EELPS assessment and results analysis. Meeting with Ethical Review Committee (17 October 2016), final D8.2 revision actions and submission to EC.

2.7 COMPONENTS OF THE PULSE PLATFORM

The PULSE Platform is made up of three high level components: software tools (WP4), mathematical models and SOPs (Standard Operational Procedures) (WP5).

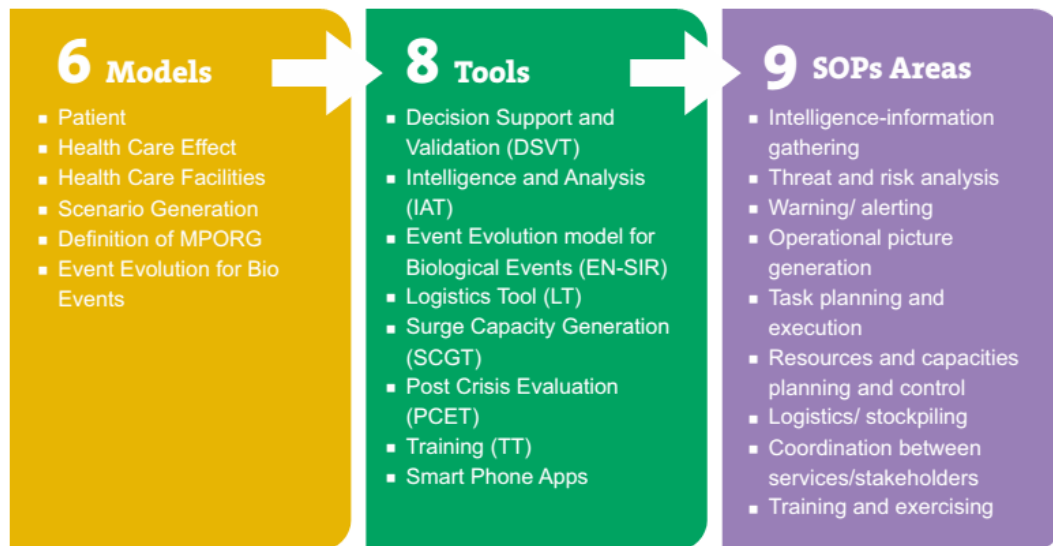


Figure 3: Components of the PULSE platform

One of the main objectives of the PULSE platform is to develop a technical and operational framework that allows the platform's stakeholders (e.g. European or National Authorities) to have access to timely key data, planning and decisions that efficiently help them to manage a major healthcare crisis. The PULSE Framework solution has been validated by two pilot scenarios: a stadium crush trial exercise in Cork, Ireland and an emerging viral disease in Rome, Italy.

PULSE Platform Architecture

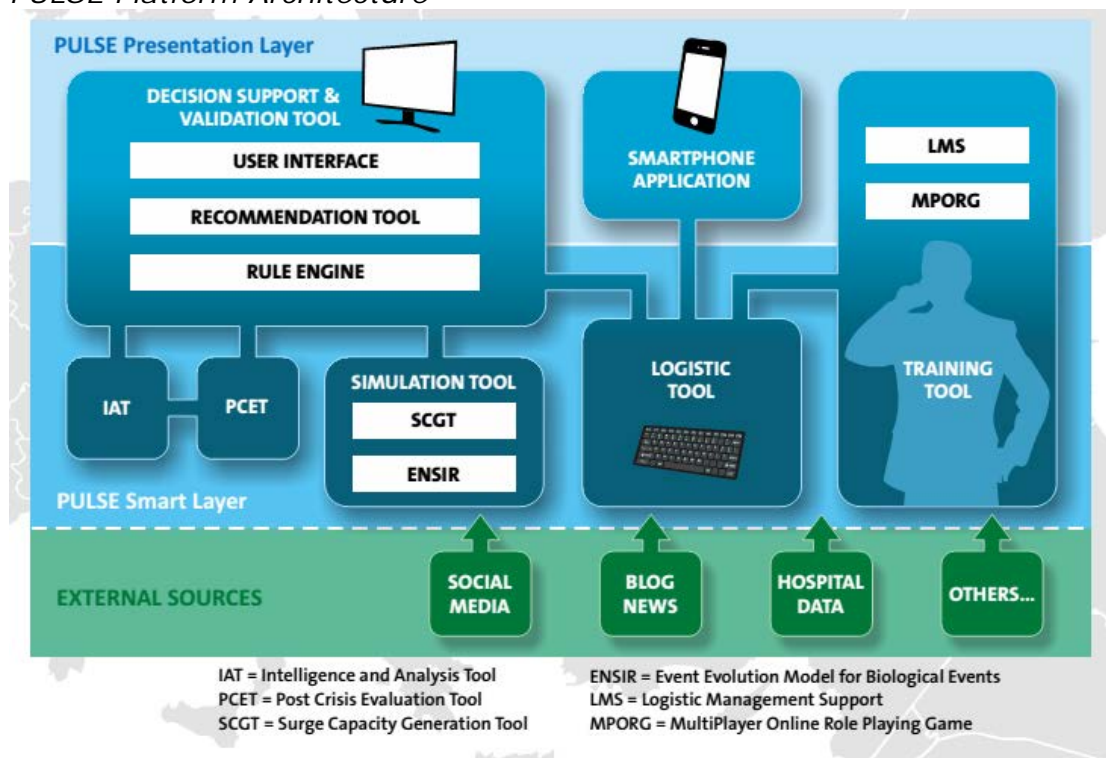


Figure 4: PULSE Platform Architecture

The PULSE tools (summarised here for the purposes of this Deliverable) are explained in detail in the Deliverables of WP4²³.

Decision Support and Validation tool (DSVT)

The DSVT provides a front-end Graphical User Interface (GUI) that is directly exploited by the platform's stakeholders in order to obtain the necessary information to handle the crisis. The *Decision support and Validation tool* provides a complete set of functionalities that allow the decision makers to efficiently handle the crisis. The DSVT assumes also an important role inside the architecture. In fact, the component resides in the platform's core and controls the communications among all the PULSE tools.

Intelligence Analysis Tool (IAT)

The IAT's objective is to provide an early warning system that is able to alert decision makers to the occurrence of an unusual biological event. The IAT in fact is able to systematically gather and analyse incoming disease-related data and to notify the presence of possible epidemic's breeding grounds. In particular, the IAT is able to extract information regarding the disease symptoms from (1) clinical records coming several selected hospitals, (2) geo-localized tweet messages generated from the Twitter platform and (3) web sites, specialized blogs, news containing disease-related information. If the number of persons suffering from these acquired disease symptoms is above a predefined threshold, then the IAT generates a weak signal.

Logistic Tool (LT)

The LT provides functionalities to manage data regarding the events, in particular with respect to the crisis management, and an optimization mechanism, able to provide an almost optimal solution that, by using the Health care facility model defined in WP3, assesses the required stockpiles of any necessary equipment, medications and vaccinations present in the different hospitals and is able to assign all the wounded to the proper hospitals using as many hospital resources as possible and sending them in the minimum amount of time.

Surge Capacity Generation Tool (SCGT)

The tool's objective is to provide support for the creation of surge capacity or, in other words, the expected evolution of some critical medical resources during a major health crisis. The tool accepts as input (1) the number of people involved in the crisis scenario and (2) a desired prediction interval. It returns the amount or resources (depending on the specified number of people) which is possible to make available within the prediction interval .

Training Tools (TT)

The training tools include a MPORG training platform for personnel involved in crisis management and a Learning Management System (LMS)/Learning Record Store tailored for the emergency and health services with access to training courses from a wide variety of browsers and mobile devices. The MPORG will be a training platform for personnel involved in crisis management and a training learning management system tailored for the emergency and health services with

²³ See PULSE Deliverables D4.1 Decision support and validation tool, D4.2 IAT tool, D4.3 Logistics tool, D4.4 Surge capacity tool, D4.5 Training tools, D4.6 Post crisis evaluation tool, D4.7 Event evaluation for biological event. Available at: <http://www.pulse-fp7.com/deliverables/>

access to training. The LMS. The LMS will be combined with a Learning Record Store (LRS) to provide support for modern tracking of a wide variety of learning experiences within the PULSE training system. The tool shall be available through an internet accessible web site and will allow for trainees to undertake remote training and self-paced training activities if they are unable to travel to the classroom based sessions or wish to perform additional preparatory training in advance of the PULSE trials.

Post Crisis Evaluation Tool (PCET)

The PCET component implements specific functionalities that allows to overcome the current unorganized manner to carry out a post crisis evaluation of the decisions taken during medical emergencies. *PCET* provides integrated features that simplify the identification of past bad choices and, in such a way, it helps to understand where to intervene for addressing critical issues in future emergencies.

Event evolution model for Biological Events (ENSIR)

This tool aims at computing the expected time evolution of the geographical spread of a biological event and it is the implementation of the mathematical model of epidemics evolution defined in T3.6 of WP3. This model is an extended version of the classical SIR (Susceptible - Infected - Removed) model. The ENSIR tool provides its functionality through a SOAP-based Web Service and the *Decision Support and Validation Tool (DSVT)*.

Smartphone application (SA)

This is the Android application can be used to access the PULSE platform.

Authentication Server (AS)

This is the tool that facilitates the authentication of the entities that attempts to access the platform. It is based on the *OAuth2* standard that assure the security protection of all the tools composing the platform.

Standard operational procedures (SOPs)

*PULSE Deliverable D5.2 PULSE SOPs*²⁴ documents the development of standard operational procedures (SOPs) for the PULSE system. Building upon a status quo analysis of national healthcare systems and international frameworks in *PULSE D5.1 Procedures and Status Quo Report*²⁵, formulates best practices to guide the further development of the functionalities of the PULSE system. It specifies detailed SoPs in a standard format for the individual use cases of the trials scenarios. The six core SOP areas of activity covered include:

- Intelligence-information gathering
- Threat and risk analysis; warning/alerting
- Operational picture generation and situational assessment
- Task planning and execution (such as movements and triage), including prioritisation; resources and capacities planning and control; logistics/stockpiling
- Training and exercising capability
- Knowledge Management

²⁴ http://www.pulse-fp7.com/pdfs/D5_2_PULSE_SOP.pdf

²⁵ http://www.pulse-fp7.com/pdfs/D5_1_Procedures_and_Status_Quo_Report.pdf

3 THE PULSE PLATFORM: ETHICAL & LEGAL PRINCIPLES AND GUIDANCE

This chapter first examines the key ethical and legal principles applicable to PULSE. It then considers recommendations in EGE opinions relevant to PULSE. It looks at other considerations in emergency preparedness and response, particularly relevant international legal frameworks for the preparedness planning and response to public health emergencies and some guidance for emergency planners and responders. The chapter also examines the legal and regulatory issues of critical infrastructure (from the PULSE perspective), identifies ethical principles for systems and information security. It highlights provisions of the General Data Protection Regulation (GDPR) applicable to PULSE. Finally, it considers the ethical and other issues in training, and outlines the PULSE strategy in addressing the legal and ethical considerations for, and during the PULSE trial exercises.

The analysis in this chapter will show that there are a variety of legal, ethical, and other principles (e.g. information security) to consider in the PULSE context. Some of these principles overlap and have some complementarities, while others might have more of 'standalone' nature. While ethics offers guidance based on moral principles, legal principles have specific penalties or consequences attached to their violation. For a wholesome appreciation of the different aspects related to public healthcare emergency management, we have chosen to adopt an approach that seeks to understand the diversity of applicable principles and issues that might arise.

3.1 PROTECTION OF ETHICAL AND LEGAL PRINCIPLES

Ethics is an integral part of research funded by the European Union, from beginning to end and ethical compliance is crucial to achieving research excellence.²⁶ The Seventh Framework Programme for Research and Technological Development was announced in 2006 by Decision No 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013).²⁷ This Decision sets out the following: "Research activities supported by the Seventh Framework Programme should respect fundamental ethical principles, including those reflected in the Charter of Fundamental Rights of the European Union. The opinions of the European Group on Ethics in Science and New Technologies (EGE) are and will be taken into account." Article 6 further sets out that "All the research activities carried out under the Seventh Framework Programme shall be carried out in compliance with fundamental ethical principles".

²⁶ http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

²⁷ <http://cordis.europa.eu/documents/documentlibrary/90798681EN6.pdf>

Within the European regulatory framework, research ethics is based on the explicit European commitment to human rights.²⁸ Compliance with human rights is firmly enshrined in the European treaties and commitment to human rights is strengthened in the Charter of Fundamental Rights of the European Union.²⁹ The Charter³⁰ describes the core values of the Union as human dignity, freedom, equality and solidarity. It outlines the rights, freedoms and principles that are relevant in the context of research.³¹ These form the basis of important ethical guidelines and support the conduct of research.³² The following articles, in particular, are relevant to the PULSE project:

- Article 1: Human dignity.
- Article 2: Right to life.
- Article 3: Right to the integrity of the person.
- Article 6: Right to liberty and security of the person
- Article 7: Respect for private and family life.
- Article 8: Protection of personal data.
- Article 11: Freedom of expression and information
- Article 12: Freedom of assembly and of association
- Article 18: Right to asylum
- Article 20: Equality before the law.
- Article 21: Non-discrimination
- Article 23 Equality between men and women
- Article 24 on the rights of the child
- Article 35 on health care

The ***European Convention on Human Rights (ECHR)***³³ and the relevant case-law of the European Court of Human Rights, especially regarding Article 8 (Right to Respect for Private and Family Life) may be an important point of reference for a legal/ethical review. This may be particularly important given the upcoming accession of the EU to the Convention. The following articles are particularly relevant to PULSE:

- Article 1: Obligation to respect Human Rights
- Article 2: Right to life
- Article 8: Right to respect for private and family life
- Article 14: Prohibition of discrimination
- Article 15: Derogation in time of emergency
- Article 17: Prohibition of abuse of rights

By being involved the discussions of the project and its research, the LEPPi team aimed to ensure that PULSE research complies with the European Charter of

²⁸ http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

²⁹ The European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union (2000/C 364/01), *Official Journal of the European Communities* C 364/1, 18 December 2000.

³⁰ http://www.europarl.europa.eu/charter/pdf/text_en.pdf

³¹ http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf

³² Ibid.

³³ Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950. http://www.echr.coe.int/Documents/Convention_ENG.pdf

Fundamental Rights and the European Convention on Human Rights, especially regarding the items mentioned above.

3.2 RECOMMENDATIONS IN EGE OPINIONS RELEVANT TO PULSE

In addition, we consider the ethical principles highlighted in the following Opinions released by the European Group on Ethics (EGE) in Science and New Technologies³⁴ to be relevant to PULSE:

- Opinion n°28 - 20/05/2014 - Ethics of Security and Surveillance Technologies
- Opinion n°26 - 22/02/2012 - Ethics of information and communication technologies
- Opinion n°13 - 30/07/1999 - Ethical issues of healthcare in the information society

We present relevant extracts feature below (these were summarised for consideration in the technical work packages):

Opinion n°28 - 20/05/2014 - Ethics of Security and Surveillance Technologies³⁵

Technologies with the potential to intrude into the privacy of individuals *and* to which they cannot consent (or cannot opt out), require specific justification. The EGE calls for a *case by case justification* for these measures.

Accountability

Member States need to ensure that those granted with powers to surveil the private sphere of citizens are acting in the public interest and are accountable for their actions. Where the State delegates security and/or surveillance tasks to private companies, they are bound by the same legal and ethical obligations and Member States should put in place mechanisms to monitor compliance with such obligations.

Accountability means that individuals have the right to be informed about surveillance technologies — even though in some cases this information may only be provided *ex post*

Personal data

The EGE affirms that the purpose limitation principle as regards personal data be the standard for both public and private organisations. Personal data should only be collected for a specific and legitimate purpose. As far as possible data should be anonymised and greater use should be made of encryption which can serve to enhance both privacy and security. Data sharing by default is to be avoided and users should be allowed to control (e.g. through access to privacy settings) and change information held by organisations about them. Profiling of individuals for commercial purposes should be subject to the individual's explicit consent. Information should be available by commercial organisations in relation to *what*

³⁴ <https://ec.europa.eu/research/ege/index.cfm>

³⁵ European Group on Ethics in Science and New Technologies, Opinion no. 28 of the European Group on Ethics in Science and New Technologies, Ethics of Security and Surveillance Technologies, Brussels, 20 May 2014. <http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJA14028/>

data are going to be collected, *by whom*, for *what purpose*, for *how long* and if data collected will be linked with other data sources.

Public awareness of data policies

The EGE reaffirms its view that there needs to be greater clarity for the public in relation to how, why and for what purpose their personal information is managed, shared and protected. Public authorities as well as corporate actors must make their policies in that regard publicly available. The EU and Member States should seek to foster public knowledge, awareness and debate on the implications for individuals and wider society of the use of security and surveillance technologies. Education programs should start at school level and should provide information and tools for citizens to safeguard their data in the digital environment

Algorithms

In the context of security and surveillance technologies, it is important to note that algorithms are necessarily selective in their design and are as subject to bias as the humans which program them. Underlying algorithms and their parameters are ethical assumptions and these should be made explicit as a mandatory requirement. Moreover, algorithms are not infallible and the data generated are contingent on the choice and quality of data input, which in the view of the EGE should be continually examined and validated. Furthermore, education on the ethical aspects in the design of algorithms should be included in the training of developers.

e-Privacy

The EGE recommends that the EC give consideration to revising the e-Privacy Directive, the scope of which currently encompasses electronic communications. Given the explosion of digital interfaces since the introduction of the Directive, the EGE considers it appropriate that VoIP — Voice over Internet Protocol, indeed IP communications, broadband communications — products and corporate private networks would be included in the remit of any revised Directive.

Privacy Impact Assessment

Privacy Impact Assessment procedures must form part of regulatory practice in Member States when new or modified information systems which process personal data are being introduced to the market. The assessment should address the potential implications of the proposed technology for personal data and if risks are identified, measures should be taken to identify processes to mitigate the risk or indeed alternatives to that which is proposed.

Designing privacy

Public and private organisations should adopt privacy-by and privacy-in design principles for development of security and surveillance technologies. The European values of dignity, freedom and justice must be taken into account before, during and after the process of design, development and delivery of such technologies. Privacy enhancing technologies should be integrated from the outset and not bolted on following implementation. In the view of the EGE, instilling a culture in organisations, where privacy is understood and reflected in practice, can be achieved through engineers, developers and experts in philosophical and ethical reflection working together in an interdisciplinary way.

Understanding and valuing privacy

Privacy is not a static concept and a fuller understanding of how European citizens conceptualise and value privacy is required, if appropriate steps are to be taken to safeguard physical and informational privacy. To this end, the EU should make

funds available for research to examine and analyse how citizens consider, and cultivate their involvement in, issues related to security and surveillance

Opinion n°26 - 22/02/2012 - Ethics of information and communication technologies³⁶

The group emphasises especially the importance of the following principles:

- **Human dignity:** The Charter of Fundamental Rights of the European Union states that 'Human dignity is inviolable. It must be respected and protected' (Article 1);
- **Respect of freedom** which secures, inter alia, the right to uncensored communication and agency in the digital era;
- **Respect for democracy, citizenship and participation** which includes, inter alia, protection against unjustified exclusion and protection against unlawful discrimination;
- **Respect of privacy** which secures, inter alia, the personal private sphere against unjustified interventions;
- **Respect of autonomy and informed consent** which secures, inter alia, the right to information and consent to the use of data or actions that are based on the data-processing;
- **Justice** which secures, inter alia, the equal access to ICT, and a fair sharing of its benefits;
- **Solidarity** among European citizens aims, inter alia, at the inclusion of everyone who wishes to participate in ICT, but also aims to secure the social inclusion of those who, for example, either cannot participate in online practices or wish to maintain alternative social interactions

In relation to the right to privacy and data protection the Opinion recommends:

Privacy by design (privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal) should be incorporated into informed consent procedures.

Transparency is a fundamental condition for enabling individuals to exercise control over their own data and to ensure effective protection of personal data. It is therefore essential that individuals should be well and clearly informed, in a **simple and transparent** way, by data controllers about how and by whom their data are collected and processed, for what reasons, for how long and what their rights are if they want to access, rectify or delete their data.

Consent should be given by any appropriate method enabling a freely given specific, informed and unambiguous indication of the data subject's wishes, ensuring that individuals are fully aware that they give their consent

Consent may always be withdrawn without negative consequences for the data subject. Data subjects should have the right to require that their personal data be erased and there will be no further processing of the data

³⁶The European Group on Ethics in Science and New Technologies (EGE), *Opinion n°26 - 22/02/2012 Ethics of information and communication technologies*.

<http://bookshop.europa.eu/en/ethics-of-information-and-communication-technologies-pbNJAJ12026/>

Children and **vulnerable adults** deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data

Opinion n°13 - 30/07/1999 - Ethical issues of healthcare in the information society³⁷

Personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive.

The principles of the European Convention of Human Rights, the rules of the Convention of the Council of Europe for the protection of individuals with regard to automatic processing of personal data and especially the European Directive 95/46/EC, for the protection of personal data, are an essential source for addressing the ethical questions of healthcare in the Information Society

Status of personal health data

Personal health data form part of the personality of the individual, and must not be treated as mere objects of commercial transaction.

Confidentiality/privacy

The Human Right to respect for private life requires that confidentiality of personal health data is guaranteed at all times. It also implies that, in principle, the informed consent of the individual is required for the collection and release of such data.

Collection of, and access to, personal health data is limited to treating medical practitioners and to those third parties (non-treating medical practitioners, healthcare and social security personnel, administrators, ...) who can demonstrate a legitimate use.

All legitimate users of personal health data have a duty of confidentiality equivalent to the professional duty of medical secrecy. Exceptions to this duty must be limited and provided for by legal rule.

Medical secrecy is central to the trustworthiness of the healthcare system, not only in the private interest of the person. Trust is a fundamental ethical value in itself.

The respect for the confidentiality of health data continues after the death of the person.

Self-determination

Health data should be collected directly from the citizen wherever possible.

Self-determination includes citizens' right to know and to determine which

³⁷ The European Group on Ethics in Science and New Technologies (EGE), Opinion n°13 *Ethical Issues Of Healthcare In The Information Society*, 30 July 1999.
http://ec.europa.eu/archives/bepa/european-group-ethics/docs/avis13_en.pdf

personal health data are collected and recorded, to know who uses them for what purposes, and to correct data if necessary.

The citizen has the right to oppose, the use of her/his data for secondary purposes not provided for by law.

The use of personal health data for the purposes from which society as a whole benefits must be justified in the context of the above rights.

Accountability

The networking of health institutions fosters new kinds of dependencies and responsibilities. This has to be reflected in new kinds of accountability.

For all parties using health data an equivalent to the accountability of health professionals should be established.

When health managers use health data for the purposes of health services planning and management, they should be accountable for such data uses.

Principle of legitimate purpose

The collection and processing of personal health data should be guided by the principle of a strict relationship between this collection and handling and the legitimate purpose to which those data are used

Third parties who do not form part of the public health system may require access to medical information for their professional purposes, such as insurers and employers. Such third parties must in no case have direct access to personal health data.

3.3 OTHER CONSIDERATIONS IN EMERGENCY PREPAREDNESS AND RESPONSE

The new EU Civil Protection Mechanism came into effect at the beginning of 2014. The revised legislation builds on an established system which was set up to enable co-ordinated assistance from 31 participating states (28 EU Member States, along with Norway, Iceland and the former Yugoslav Republic of Macedonia) to victims of natural and man-made disasters in Europe and elsewhere.³⁸ The new legislation places a greater emphasis on disaster prevention, risk management, and disaster preparedness, including the organisation of training, simulation exercises and the exchange of experts, in addition to developing new elements such as a voluntary pool of pre-committed response capacities by the Member States.³⁹ The revised legislation includes the following elements:

- A European Emergency Response Capacity which will facilitate a voluntary pool of response capacities and experts available for immediate deployment as part of a collective European intervention.

³⁸ European Commission, EU Civil Protection Mechanism.

<http://ec.europa.eu/echo/en/what/civil-protection/mechanism>

³⁹ European Commission, EU Civil Protection Legislation ECHO Factsheet, 2014.

http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_legislation_en.pdf

- An Emergency Response Coordination Centre (ERCC) which provides a full 24/7 capacity to monitor and respond to disasters ensuring that Member States are fully apprised of the situation and can coordinate regarding the provision of resources and financial and in-kind assistance.
- Member States are asked to contribute to risk management planning by sharing summaries of their risk assessments and refining their risk management planning.
- The importance of prevention and preparedness actions is now legally embedded into the EU Civil Protection Mechanism. EU assistance regarding training will be provided to enable improved inter-operability of the Member States' teams on the ground.

Annex 5 contains a list of relevant international legal frameworks for the preparedness planning and response to public health emergencies.

The UK HM Government *Data Protection and Sharing – Guidance for Emergency Planners and Responders* 2007⁴⁰ document recommends asking the following questions:

- Is it unfair to the individual to disclose their information?
- What expectations would they have in the emergency at hand?
- Am I acting for their benefit and is it in the public interest to share this information?

It also outlines the following key principles:

- Data protection legislation does not prohibit the collection and sharing of personal data – it provides a framework where personal data can be used with confidence that individuals' privacy rights are respected
- Emergency responders' starting point should be to consider the risks and the potential harm that may arise if they do not share information.
- Emergency responders should balance the potential damage to the individual (and where appropriate the public interest of keeping the information confidential) against the public interest in sharing the information.
- In emergencies, the public interest consideration will generally be more significant than during day-to-day business.
- Always check whether the objective can still be achieved by passing less personal data.
- Category 1⁴¹ and 2⁴² responders should be robust in asserting their power to share personal data lawfully in emergency planning, response and recovery situations.

⁴⁰ HM Government, *Data Protection and Sharing – Guidance for Emergency Planners and Responders*, February 2007.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf

⁴¹ Category 1 are organisations at the core of the response to most emergencies (the emergency services, local authorities, NHS bodies). Category 1 responders are subject to the full set of civil protection duties.

⁴² Category 2 organisations (the Health and Safety Executive, transport and utility companies) are 'co-operating bodies'. They are less likely to be involved in the heart of planning work, but will be heavily involved in incidents that affect their own sector.

- The consent of the data subject is not always a necessary pre-condition to lawful data sharing.
- You should seek advice where you are in doubt – though prepare on the basis that you will need to make a decision without formal advice during an emergency.⁴³

The LEPPI team also identified the principles of emergency management developed by the International Association of Emergency Managers (IAEM)⁴⁴ and widely accepted across the emergency management field as relevant for consideration, particularly in the development of the scenarios. According to the IAEM, emergency management must be:

1. Comprehensive – emergency managers consider and take into account all hazards, all phases, all stakeholders and all impacts relevant to disasters.
2. Progressive – emergency managers anticipate future disasters and take preventive and preparatory measures to build disaster-resistant and disaster-resilient communities.
3. Risk-Driven – emergency managers use sound risk management principles (hazard identification, risk analysis and impact analysis) in assigning priorities and resources.
4. Integrated – emergency managers ensure unity of effort among all levels of government and all elements of a community.
5. Collaborative – emergency managers create and sustain broad and sincere relationships among individuals and organisations to ensure trust, advocate a team atmosphere, build consensus and facilitate communication.
6. Coordinated – emergency managers synchronise the activities of all relevant stakeholders to achieve a common purpose.
7. Flexible – emergency managers use creative and innovative approaches in solving disaster challenges.
8. Professional – emergency managers value a science and knowledge-based approach based on education, training, experience, ethical practice, public stewardship and continuous improvement.⁴⁵

The LEPPI team recommended the above for consideration by the PULSE consortium.

3.4 CRITICAL INFRASTRUCTURE: LEGAL AND REGULATORY ISSUES

Critical infrastructure (CI) refers to “an asset or system which is essential for the maintenance of vital societal functions”.⁴⁶ The *European Programme for Critical Infrastructure Protection* defines it as “the physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of

Category 2 responders have a lesser set of duties - co-operating and sharing relevant information with other Category 1 and 2 responders.

⁴³ HM Government, op. cit., 2007.

⁴⁴ <http://www.iaem.com/page.cfm?p=about/em-principles>

⁴⁵ <http://www.iaem.com/documents/Principles-of-Emergency-Management-Flyer.pdf>

⁴⁶ European Commission Migration and Home Affairs, Critical Infrastructure.
http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

citizens or the effective functioning of governments in EU countries".⁴⁷ There are a number of CI-related legal and regulatory issues relevant to PULSE,

1. Cross-border dependencies "create additional vulnerabilities and a potential source of instability even for countries that have addressed these issues domestically".⁴⁸
2. While "several countries have put in place a policy for critical infrastructure protection (CIP) and critical information infrastructure protection (CIIP). However, the landscape of these national policies is still very fragmented".⁴⁹
3. Local disruptions may have an impact on many countries; the fact that global legal frameworks and institutions are lacking; and the huge administrative burden faced by global players with multinational presence when responding to fragmented national CIP policies.⁵⁰
4. There are important cultural and legal specificities that inform responses and are different across countries. This makes establishing a harmonised global approach towards C(I)IP more complex.⁵¹
5. With respect to the role of liability – "there are limits in the case of CIP, due to the difficulties in establishing causation links and the multi-party, multi-risk environment in which CIP providers operate".⁵²
6. Regulatory restrictions can have an impact on technical support.⁵³

Annex 6 provides an overview of relevant EU legislation and guidelines concerning critical infrastructure. PULSE partners have consulted this document in the development of the PULSE tools and system.

3.5 SYSTEMS AND INFORMATION SECURITY: ETHICAL PRINCIPLES

Information security refers to the protection of information and its critical elements, including the systems and hardware that use, store and transmit that information.⁵⁴ Information security aims to ensure business continuity and minimise business damage by limiting the impact of security incidents.⁵⁵ Information security is defined as being concerned with the protection of three

⁴⁷ European Commission, *European Programme for Critical Infrastructure Protection*, 2007. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260>

⁴⁸ Kaska, Kadri and Lorena Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015.

⁴⁹ Hämmerli, Bernhard (Chair), *Protecting critical infrastructure in the EU*, CEPS Task Force report, 2010. <http://www.ceps.eu/publications/protecting-critical-infrastructure-eu>

⁵⁰ CEPS Task Force report, 2010.

⁵¹ CEPS Task Force report, 2010.

⁵² CEPS Task Force report, 2010.

⁵³ CEPS Task Force report, 2010.

⁵⁴ Whitman, Michael E., and Herbert J. Mattord, *Principles of Information Security*, 2012 Course Technology, Cengage Learning, 2012.

⁵⁵ Von Solms, Rossouw and van Niekerk, Johan, "From information security to cyber security", *Computers and Security*, Vol. 38, 2013, p. 97 – 102.

aspects of data, namely their confidentiality, integrity and availability.⁵⁶ Whitman and Mattord expanded the critical characteristics of information to include accuracy, authenticity, utility and possession. The following sets out a brief description of each characteristic:

- **Availability:** enables authorised users - persons or computer systems - to access information without interference and to receive it in the required format.
- **Accuracy:** information has accuracy when it is free from mistakes or errors and it has the value that the end-user expects.
- **Authenticity:** Authenticity of information is the quality or state of being genuine or original. Information is authentic when it is in the same state in which it was created, placed, stored or transferred.
- **Confidentiality:** Confidentiality ensures that only those with the rights and privileges to access information can do so. A number of measures can be employed to protect the confidentiality of information, including information classification, secure document storage, application of general security policies and education of information custodians and end users.
- **Integrity:** Information has integrity when it is whole, complete and uncorrupted. Information integrity is the cornerstone of information systems, as information is of no value or use if users cannot verify its integrity.
- **Utility:** The utility of information refers to the quality or state of having value for some purpose or end. Information should be available in a format that is meaningful to the end user.
- **Possession:** The possession of information refers to the quality or state of ownership or control. Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality.

The components of an information system include the entire set of software, hardware, data people, procedures and networks.⁵⁷ These six components allow information to be input, processed, output and stored.⁵⁸ Each component of the information system has its own security requirements.⁵⁹

Breaches in information security and associated ethical implications

Brey identifies ethical issues connected to breaches in computer security, summarised below:⁶⁰

⁵⁶ Brey, P., "Ethical Aspects of Information Security and Privacy", in M. Petković and W. Jonker (eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer Berlin, Heidelberg, 2007, pp. 21-36.

⁵⁷ Whitman and Mattord, op cit., 2012.

⁵⁸ Whitman and Mattord, op cit., 2012.

⁵⁹ Whitman and Mattord, op cit., 2012.

⁶⁰ Brey, P., "Ethical Aspects of Information Security and Privacy", in M. Petković and W. Jonker (eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer Berlin, Heidelberg, 2007, pp. 21-36.

- **Economic harm.** When system security is undermined, valuable hardware and software may be damaged or corrupted and service may become unavailable, resulting in losses of time, money and resources.
- **Injury and death** may occur in so-called safety-critical systems, which are computer systems with a component or real-time control that can have a direct life-threatening impact.
- **Indirect life-threatening consequences** may occur in systems that are used for design, monitoring, diagnosis or decision-making, for instance systems used for bridge design or medical diagnosis.
- Compromises of the confidentiality of information may **violate intellectual property rights**. Third parties may compromise the confidentiality of information by accessing, copying and disseminating it.
- Compromises of confidentiality may **violate privacy rights** when information that is accessed includes information about persons that is considered to be private.
- Breaches of confidentiality may also cause a variety of other harms resulting from the dissemination and use of confidential information. e.g. **damage to reputation, undermines trust in the security**
- Compromises of the availability of information can, when they are prolonged or intentional, **violate freedom rights**, specifically rights to freedom of information and free speech.
- Security measures may also be discriminatory: they may wrongly exclude certain classes of users from using a system, or may wrongly privilege certain classes of users over others.⁶¹

Information security standards

Information security plays a crucial role in protecting an organisation's assets. Standards play an important role in providing examples of good practice in the area. The ISO 27000⁶² series of standards regarding information security matters are relevant to PULSE, and specifically:

- ISO/IEC 27000: 2014: Information security management systems – Overview and vocabulary
- ISO/IEC 27005: 2011 Information security risk management which provides guidelines for information security management
- ISO/IEC 29100: 2011: Information technology – Security techniques – Privacy framework
- ISO/IEC CD 29134 Privacy impact assessment methodology (under development) – methodology draft standard is also relevant.⁶³

These standards are expanded below and were circulated to the PULSE technical team for consideration in August 2015 in the development of the PULSE tools.

ISO/IEC 27000: 2014: Information security management systems – Overview and vocabulary

ISO/IEC 27000:2014 provides the overview of information security management systems (ISMS), and terms and definitions commonly used in the ISMS family of

⁶¹ Summarised from Brey, op. cit, 2007.

⁶² http://www.iso.org/iso/catalogue_detail?csnumber=56891

⁶³ http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289

standards. It is applicable to all types and sizes of organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

ISO/IEC 27005: 2011 Information security risk management which provides guidelines for information security management

ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2011. ISO/IEC 27005:2011 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security.

ISO/IEC 29100: 2011: Information technology – Security techniques – Privacy framework

This standard provides a framework for protecting personally identifiable information (PII). It defines PII as any information that can be used to identify a PII principal (a person or a “data subject”, to use EC terminology) or that might be linked to a PII principal, either directly or indirectly. It defines privacy principles in terms of PII, so the standard does not address all types of privacy. Organisations can use the framework to help define their “privacy safeguarding requirement”. The framework describes such requirements and lists privacy principles based on other well-known guidance documents. The standard can also support other privacy standardisation activities, such as privacy risk assessments and controls.

Privacy safeguarding requirements may arise whenever an organisation processes PII – e.g., in the collection, processing and storage of PII and in the transfer of PII to others, including others in third countries. The standard encourages organisations to identify privacy safeguarding requirements whenever they design an ICT system that will be used to process PII. It says the privacy risk management process comprises five main elements: • establishing the context • assessing risks • treating risks • communications and consultation • monitoring and reviewing risks and controls.

The ISO 29100 Section 5 provides a list of privacy principles that were abstracted from those promulgated by various countries and international organisations. It says the privacy principles are to guide the design, development and implementation of privacy policies and controls. ISO 27005 formulates 11 privacy principles, as follows:

- **Consent and choice** means the PII principal must have a freely given, specific and knowledgeable choice (opt-in) about the processing of her PII. A PII principal should be able to withdraw her consent without penalty.
- **Purpose legitimacy and specification** means ensuring that the purpose(s) complies with applicable law, and communicating the purpose with the PII principal before the organisation collects the information.
- **Collection limitation** means limiting the collection of PII to that which has a legal basis and to not more than necessary for the specified purpose(s). The standard says organisations should justify and document the PII they collect.

- **Data minimisation** means minimising the PII processed and the number of people who have access to such data.
- **Use, retention and disclosure limitation** means a limit to that necessary to fulfil specific, explicit and legitimate purposes, and retaining such data only as long as necessary to meet the specified purpose.
- **Accuracy and quality** mean that the data controller must ensure that the PII is accurate and relevant for the specified purpose.
- **Openness, transparency and notice** mean that the data controller should provide PII principals with clear and easily accessible information about its policies, procedures and practices in regard to the processing of PII. The data controller should also inform the PII principals about who might be provided with the PII and whom they can contact at the controller's address if they have questions or want to access their data.
- **Individual participation and access** means enabling the PII principals to access, review and correct their PII, provided their identity is authenticated.
- **Accountability** means that the organisation should document and communicate to stakeholders its privacy policies and practices. It also means that someone in the organisation is held responsible for implementing the privacy policies and practices. If the organisation transfers PII to a third country, it must ensure by means of contractual arrangements, for example, that the recipient will provide comparable privacy protection. If there is a data breach, the organisation must inform the relevant stakeholders about the breach and what it is doing to resolve it. Accountability also means there must be redress procedures in place.
- **Information security** means protecting PII to ensure its integrity, confidentiality and availability, and protect it against unauthorised access, use or loss.
- **Privacy compliance** means ensuring that the processing meets data protection and privacy safeguards (legislation and/or regulation), and enabling the conduct of audits. It also means that the organisation should conduct privacy risk assessments to ensure, among other things, that the organisation complies with laws and regulations and safeguarding requirements.

These 11 principles should be incorporated into any new organisational data protection policy or set of guidelines to provide a comprehensive framework for the protection of personal data. In the PULSE project, additional safeguards should be implemented to protect highly sensitive information, in the light of this.

Another relevant standard (under development) is the ISO/IEC DIS 29134 Information technology -- Security techniques -- Privacy impact assessment – Guidelines (target publication date 30 May 2017).⁶⁴

Some relevant health informatics standards

We also identified the following health informatics standards as relevant:

ISO 27799:2008 Health informatics -- Information security management in health using ISO/IEC 27002

⁶⁴ ISO/IEC, ISO/IEC DIS 29134 Information technology -- Security techniques -- Privacy impact assessment – Guidelines.

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289

ISO 27799:2008 defines guidelines to support the interpretation and implementation in health informatics of ISO/IEC 27002 and is a companion to that standard. ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and that will maintain the confidentiality, integrity and availability of personal health information. ISO 27799:2008 applies to health information in all its aspects; whatever form the information takes (words and numbers, sound recordings, drawings, video and medical images), whatever means are used to store it (printing or writing on paper or electronic storage) and whatever means are used to transmit it (by hand, via fax, over computer networks or by post), as the information must always be appropriately protected.

ISO/TR 21089:2004 Health informatics -- Trusted end-to-end information flows

ISO/TR 21089:2004 offers a guide to trusted end-to-end information flow for health(care) records and to the key trace points and audit events in the electronic entity/act record lifecycle (from point of record origination to each ultimate point of record access/use). It also offers recommendations regarding the trace/audit detail relevant to each. It offers recommendations of best practice for healthcare providers, health record stewards, software developers and vendors, end users and other stakeholders, including patients.

ISO/TS 14441:2013 Health informatics -- Security and privacy requirements of EHR systems for use in conformity assessment

ISO/TS 14441:2013 examines electronic patient record systems at the clinical point of care that are also interoperable with EHRs. ISO/TS 14441:2013 addresses their security and privacy protections by providing a set of security and privacy requirements, along with guidelines and best practice for conformity assessment. ISO/TS 14441:2013 includes a cross-mapping of 82 security and privacy requirements against the Common Criteria categories in ISO/IEC 15408 (all parts).

ISO/TR 22221:2006 Health informatics - Good principles and practices for a clinical data warehouse

The focus of ISO/TR 22221:2006 is clinical databases or other computational services, hereafter referred to as a clinical data warehouse (CDW), which maintain or access clinical data for secondary use purposes. The goal is to define principles and practices in the creation, use, maintenance and protection of a CDW, including meeting ethical and data protection requirements and recommendations for policies for information governance and security. A distinction is made between a CDW and an operational data repository part of a health information system: the latter may have some functionalities for secondary use of data, including furnishing statistics for regular reporting, but without the overall analytical capacity of a CDW. ISO/TR 22221:2006 complements and references standards for electronic health records (EHR), such as ISO/TS 18308, and contemporary security standards in development. ISO/TR 22221:2006 addresses the secondary use of EHR and other health-related and organizational data from analytical and population perspectives, including quality assurance, epidemiology

and data mining. Such data, in physical or logical format, have increasing use for health services, public health and technology evaluation, knowledge discovery and education. ISO/TR 22221:2006 describes the principles and practices for a CDW, in particular its creation and use, security considerations, and methodological and technological aspects that are relevant to the effectiveness of a clinical data warehouse. Security issues are extended with respect to the EHR in a population-based application, affecting the care recipient, the caregiver, the responsible organizations and third parties who have defined access. ISO/TR 22221:2006 is not intended to be prescriptive either from a methodological or a technological perspective, but rather to provide a coherent, inclusive description of principles and practices that could facilitate the formulation of CDW policies and governance practices locally or nationally.

3.6 DATA PROTECTION

The General Data Protection Regulation (GDPR)⁶⁵ entered into force on 24 May 2016, and will apply across the EU from 25 May 2018. According to the GDPR, the principles of data protection should apply to any information concerning an identified or identifiable natural person. These include the principles relating to personal data processing: lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, accountability. It further lays down conditions for: lawfulness of processing; consent; applicable to child's consent in relation to information society services; and the conditions for processing of special categories of personal data.

This section examines some of the GDPR provisions applicable to PULSE.

Personal data concerning health

The GDPR states that personal data concerning health should include “all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject”, and this includes “information about the natural person collected in the course of the registration for, or the provision of, health care services⁶⁶ to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.”⁶⁷

⁶⁵ European Parliament and the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4.5.2016, p. 1–88.

⁶⁶ As referred to in Directive 2011/24/EU of the European Parliament and of the Council.

⁶⁷ Recital 35, GDPR.

Grounds of lawful processing

The GDPR clearly states that where the processing of personal data is necessary to protect an interest which is essential for the life of a data subject or that of another natural person, it may be regarded as lawful. It clarifies that “processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis”.⁶⁸ Processing may serve important grounds of public interest and the vital interests of the data subject e.g. when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread, or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

Prohibition on processing special categories of personal data & grounds of derogation

The GDPR expressly prohibits the processing of special categories of personal data i.e., that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.⁶⁹ However, it this prohibition does not apply if: (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, (b) the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law⁷⁰, (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent, (d) the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body, and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects, (e) processing relates to personal data which are manifestly made public by the data subject (f) processing is necessary for the establishment, exercise or defence of legal claims (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law⁷¹, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union

⁶⁸ Recital 46, GDPR

⁶⁹ Article 9 (1), GDPR.

⁷⁰ In so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

⁷¹ This must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards, (i) processing is necessary for reasons of public interest in the area of public health⁷² on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; (j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

A derogation from the prohibition on special categories of personal data may be made for health purposes, including public health and the management of health-care services, especially to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. This derogation is permissible when i.e. when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health.

Further, Recital 53 states,

Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health.

Access to data concerning health

The GDPR provides that data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any

⁷² E.g. protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

treatment or interventions provided.⁷³ Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.

Processing of personal data for scientific research

Recital 157 of the GDPR recognises the value of aggregated data on medical conditions in enhancing research and enabling researchers to obtain essential knowledge. It further states, "research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services" and that "to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law."⁷⁴ Article 89 of the GDPR lays down safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. It particularly stresses that "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject". The safeguards must ensure that technical and organisational measures are in place to ensure respect for the principle of data minimisation.

3.7 ETHICAL AND OTHER ISSUES IN TRAINING

Training is an important part of public health emergency management and is an integral part of PULSE. Training, however, raises a number of ethical issues: e.g. unethical behaviour by trainers/training team; unacknowledged power dynamics; lack of informed consent; lack of understanding of cultural norms (differences); risks to personal health and safety; trainees might volunteer (or be asked) to perform tasks beyond the scope of their training; ensuring sustainable and appropriate benefits; problems in addressing ancillary benefits (overwhelmed by the needs they perceive in local communities); identification of potential burdens - costs or other for host institutions; and impact on the way local resources are utilised.

⁷³ Recital 63, GDPR.

⁷⁴ Recital 157, GDPR.

*PULSE D2.1 Requirements Analysis*⁷⁵ specifically identified the following issues that need to be included and addressed in national ethics training and personnel response training:

- protection of information (privacy);
- individual liberty;
- fairness of distribution of medication/vaccines/antidotes;
- prioritisation of response and treatment; and
- respect for cultural and religious beliefs.

3.8 LEGAL & ETHICAL CONSIDERATIONS FOR, AND DURING THE TRIAL EXERCISES

The LEPPi team provided input on the legal and ethical considerations for the trial exercises in the planning phases and the trials definition.

PULSE Deliverable 7.1 Trials Definition, section 2.5 documents the legal and ethical considerations and implications in relation to both the trial exercises. It outlines a framework for ensuring ethical research processes, and highlighted the roles and responsibilities of exercise leaders and participants. The PULSE ERC reviewed Deliverable 7.1. All three ERC members approved the deliverable subject to recommended changes being made. The Deliverable was revised in line with the ethical approvals (Annex 1) and submitted to the EC. The recommendations guided the partners in conduct of the trial exercises.

The LEPPi team created a checklist (Annex 7) to monitor that ethical aspects identified in the planning and by the ERC were adequately considered during the trial exercises in Rome and Cork. The LEPPi team created Information Sheets and Consent forms (Annex 8) for both the exercises (for the Cork trial, this was finalised in discussion with the Irish Data Protection Commissioner).

The LEPPi team also provided input on the management of ethical aspects before the trial (applicable to both Rome and Cork trials) to *PULSE Deliverable 7.2 Report on trials implementation*. TRI also provided input on the EELPS (Ethical, Economic, Legal, Political and Societal) Impact Assessment that was used as a basis for trial participants to provide their views on the ethical, economic, legal, political and societal impacts of the PULSE system. The LEPPi team also provided support in the analysis of the EELPS assessment, documented in *PULSE Deliverable 7.3 validation results*.

4 PULSE PILOT SCENARIOS

This chapter focusses on the PULSE pilot scenarios. It examines the scenarios and outlines the ethical, legal and societal issues related to them. It also discusses important considerations for resource triage and allocation and legal issues in public health emergency management.

4.1 INTRODUCTION⁷⁶

⁷⁵ http://www.pulse-fp7.com/pdfs/D2_1_Requirements_Specification.pdf

⁷⁶ Adapted from PULSE Deliverable 2.1 Requirements Specifications.

The role of scenarios in the process of developing requirements for the PULSE system is to make the requirements realistic as opposed to speculative in nature. For the purposes of the PULSE project, the term “scenario” is defined as the description of a hazardous incident, its background, occurrence and course of main events including response and other related processes of relevance. The two scenarios developed for the PULSE project follow many requirements and differ considerably in basic characteristics:

- Scenarios should emerge because of different threats or hazard sources.
- Scenarios should be representative and realistic, i.e. similar cases have occurred in the past.
- Scenarios should offer a wide spectrum of challenges and tasks to be undertaken by different entities within the health system.
- Scenarios should show basic differences in severity, time, geographic distribution and societal, political and international relevance.

The two scenarios in PULSE are: Emerging Viral Disease (EVD) – SARS-like outbreak, and a Mass Casualty Incident (MCI) – crowd crush in a stadium.

Expected role of a PULSE-like system in the scenarios

The PULSE system will be designed to fill obvious or assumed gaps in the existing EU health system. It aims to contribute to the harmonisation of response procedures, improving decision support, harmonising information management and controlling information distribution, improving training and feedback from lessons learned and enhancing information exchange between authorities and people. PULSE will provide a framework and interoperable platform and tools for a co-ordinated European response.

PULSE requirements will be formulated differently based on the specific conditions of the scenarios. The main characteristics of the EVD scenario are international propagation and collaboration and a time horizon of days to months. The stadium crush scenario is characterised by little warning, short reaction times and high local impact with limited cross-border short term collaboration.

Trilateral identified legal, ethical and societal issues for both scenarios (i.e., a SARS-like virus pandemic and a stadium crush), with a particular focus on the ethical values relevant to decision-making in a pandemic situation, ethical issues and problems in resource triage and resource allocation and issues in public health law.⁷⁷ An overview of these issues was used as input to the first end-user workshop (Task 2.1 Health service user requirements gathering and reviewing including threat analysis). As articulated by the end-users in the workshop:

- The following issues should be included in national ethics training and personnel response training: *protection of information (privacy); individual liberty; fairness of distribution of medication/vaccines/antidotes; prioritisation of response and treatment; and respect for religious beliefs.*
- *Accountability mitigation* is a crucial issue. PULSE should provide guidance

⁷⁷ See Appendix 1, PULSE Deliverable 8.1. http://www.pulse-fp7.com/pdfs/D8_1_Review_of_Ethical_Issues_Affecting_PULSE.pdf

regarding the ethical and legal issues around the mitigation of accountability and devise strategic procedures to contribute to the development of EU-wide strategy and policies for the preparedness and response phases of major medical emergencies.

- *Duty to provide care notwithstanding personal risks* is a crucial issue requiring sensitive treatment and transparency in the development of procedures.
- *Guidance regarding acceptable over-triage or under triage rates* is an important input into the development of tactical procedures.
- *Consideration of the duty to steward resources* is a key element in the development of operational procedures.
- Ethical and legal consideration regarding *the balancing of individual liberties* should be a key component of the PULSE framework. The issues of individual liberties, resource allocation and support for first responders warrant particular attention in the design of processes and procedures and tools.
- The project should adhere to legal requirements, but there may be instances (in emergencies) where the exigencies of the situation may permit a *derogation of normal legal requirements*. This particularly applies to over-triage; balancing of individual liberties; privacy or personal and sensitive information; duty to manage resources; duty to provide care notwithstanding personal risks; and accountability mitigation.

End users viewed the treatment of many ethical issues by policy-makers – duty to provide care notwithstanding personal risks, accountability mitigation, privacy of personal and sensitive information and over-triage or under triage - as inadequate. The PULSE consortium has attempted to remain sensitive to these issues in the co-ordination of activities falling under WP8.

4.2 EVD SCENARIO: ETHICAL, LEGAL AND SOCIETAL ISSUES

Scenario summary: It is holiday season in two metropolitan areas in neighbouring EU member states (MS1 and MS2)⁷⁸ with international airports, and one EU "Associated"⁷⁹ state (AS) with borders to both MS's. "Medium" alert status has been issued by the EU/WHO⁸⁰ for the whole EU healthcare systems (EHS) because of SARS-like incidents and (still few) casualties in two East Asian States. The total number of people with general infection risk in this European area is 20 Mio. Three patients are delivered to one metropolitan hospital with serious pneumonia symptoms. They have been on holidays and/or business missions in East Asia where local SARS epidemics are roaming. They have returned in 3 different fully occupied airplanes, unfortunately with stopovers in 3 different cities in neighbouring states. After 48 hours, diagnosis of a SARS-type infection is verified. EU and WHO organizations are informed. Origin from the Far East is confirmed by authorities, to have zoonotic (animal) based root. Consultation with the neighbouring countries has to be initiated and coordination measures to be planned. WHO has issued guidelines for global surveillance,

⁷⁸ e.g. Italy (Milan) and Germany (Munich).

⁷⁹ e.g. Switzerland.

⁸⁰ GORN - Global Outbreak Alert and Response Network.

control and information exchange. A total of 3 Mio people in the affected metropolitan areas are at risk. The total population to be put on alert is 9 Mio.

PULSE Deliverable D2.2 *Use case specifications*⁸¹ considers the following ethical issues and makes the following recommendations:

Ethical issues at stake: Individual liberty, proportionality, privacy of personal information, the public right to know, duty to steward resources, trust, duty to provide care, protection of the public from harm, reciprocity and equity.

Recommendations:

- Consider ethical values (e.g. individual liberty, proportionality, privacy of personal information, the public right to know, duty to steward resources, trust, duty to provide care, protection of the public from harm, reciprocity and equity, fairness of distribution of medication or vaccines, prioritisation of response and treatment and respect for religious beliefs) in making decisions in a SARS-like pandemic.
- Procedural values such as reasonableness, openness and transparency, inclusiveness, responsiveness and transparency should inform the making of decisions.
- Accountability mitigation⁸² is a crucial issue in the preparedness and response phases of major medical emergencies. Lawyers, public health practitioners and emergency managers must prioritise and resolve legal issues based on incomplete information and guidance during emergencies.
- Indeed, in some instances, the exigencies of the situation may allow for a derogation of normal legal requirements, particularly regarding over-triage, balancing of individual liberties, privacy or personal and sensitive information, duty to manage resources and duty to provide care notwithstanding personal risks and accountability mitigation.

4.3 MCI SCENARIO: ETHICAL, LEGAL AND SOCIETAL ISSUES

Scenario summary: A rock concert is taking place in a large stadium with a capacity of 60.000 visitors, located in the vicinity of a border between two EU Member States. Tickets are fully sold out with some 10% over-selling through a fake/ black market. A renowned rock-band is performing, with the schedule of 1 hr pre-performance of a local band and 2.5 hrs main performance. The main band is politically active and based on precedent experiences may attract some violence-prone groups. It is a hot mid-summer evening, but with heavy thunderstorms forecasted. Access routes to the stadium are rather limited in number, narrow and some with stairways. The access ways to the stadium are noticeably below capacity, which already before the start of the concert causes several scrambles and disputes. Visitors start fighting for seating on the bleachers and good sighting in the bottom arena where visitors are standing.

⁸¹ http://www.pulse-fp7.com/pdfs/D2_2_Use_Case_Specification.pdf

⁸²This is an issue that came up at the end-users workshop - healthcare workers and others involved in responding to disaster situations are concerned about certain situations for which they feel they cannot be held accountable and so the issue of "mitigation" becomes relevant.

This is exacerbated by the oversold number of tickets. Some groups are already drunk when entering. Alcohol is circulating and can be purchased inside the arena. Distribution of drugs is visible at many places. When the pre-performance is finished, the appearance of the main band is delayed for more than one hour. General mood becomes more and more aggressive. After the second hit performed by the main band, very suddenly a heavy hailstorm breaks out; lightning flashes follow. Within five minutes, approximately 50% of the visitors start rushing to the exits. Local private security forces are completely overrun. At three narrow exit stairways, crowds severely crush. People fall and are trampled to death. One of the stairways is a provisional metal construction. With some 100 visitors on the stairs and many trying to enter the stairs by climbing the guardrail from the side, the whole stairway collapses, sending the whole construction and the people crashing into the crowd below. After 25 minutes, most of the visitors have fled the stadium in panic leaving a horror-scene of dead, dying and injured behind. Many lightly injured find their way home or consult emergency stations of adjacent hospitals. The final balance is 32 deaths, 91 severely injured and about 250 lightly injured.

PULSE Deliverable D2.2 *Use case specifications*⁸³ considers the following ethical issues and makes the following recommendations:

Ethical issues at stake: how to go about allocating resources in a disaster situation while considering practical issues such as likelihood of benefit, change in quality of life and duration of benefit and ethical values such as fairness and justice.

Recommendations:

- Guidance regarding acceptable over-triage rates is an important input into the development of tactical procedures.
- The issues of individual liberties and support for first responders warrant special attention in the design of processes and procedures. Legal issues relating to implementing crisis standards of care include questions concerning co-ordination of health services, liability and, where relevant, inter-jurisdictional co-operation.

Annex 9 presents a comparative documentation of the scenarios characteristics.

4.4 RESOURCE TRIAGE AND ALLOCATION: IMPORTANT CONSIDERATIONS

Resource allocation and patient dispatch are major issues for end-users, i.e. matching resources with the patient situation. A resource database of the European Commission states:⁸⁴

⁸³ http://www.pulse-fp7.com/pdfs/D2_2_Use_Case_Specification.pdf

⁸⁴ European Road Safety Observatory, "Which hospital? The importance of field triage", 19 March 2015.

http://ec.europa.eu/transport/road_safety/specialist/knowledge/postimpact/pre_hospital_medical_care/which_hospital_the_importance_of_field_triage_en.htm

Different factor needs to be taken into account in the decision about the appropriate hospital for the road traffic victim such as type of injuries, services available at the hospital, comparative distances and times to reach hospitals, and regulations concerning the transport of injured people. Triage is the term applied to the process of classifying patients at the scene according to the severity of their injuries to determine how quickly they need care. Careful triage is needed to ensure that resources available in a community are properly matched to each victim's needs. Formal algorithms or protocols need to be developed to ensure that community resources are used properly to care for trauma patients; these algorithms must exist for both the pre-hospital and hospital setting. Failure to develop protocols may lead to over-triage or under-triage. Over-triage occurs when non-critical patients are sent to facilities offering the highest level of care. Under-triage occurs when critically injured patients are treated at the local level or sent to facilities that are not properly equipped to meet their needs. This may result in increased morbidity and mortality among patients with otherwise treatable injuries.⁸⁵

4.5 LEGAL ISSUES IN PUBLIC HEALTH EMERGENCY MANAGEMENT

A document by WHO/DG SANCO⁸⁶ states emergency management refers to:

A range of measures to manage risks to communities and the environment; the organisation and management of resources for dealing with all aspects of emergencies. Emergency management involves the plans, structures and arrangements which are established to bring together the normal endeavors of government, voluntary and private agencies in a comprehensive and coordinated way to deal with the whole spectrum of emergency needs including prevention, response, and recovery.

Legal issues in public health emergency management (as outlined by Hodge⁸⁷ and others⁸⁸) include:

- Creation in overlaps in authorities and confusion if laws allow multiple states of emergency to be declared for a single event.
- Lack of uniform liability protection for all responders, which creates inconsistencies.
- Potential legal complications especially in cross border cooperation and collaboration
- Legal aspects of interoperability

⁸⁵ Sasser, S., M. Varghese, A. Kellermann, J.D. Lormand, "Pre-hospital trauma care guidelines", Geneva, World Health Organization, Geneva, 2005.

⁸⁶ World Health Organization, *Emergency Medical Services Systems in the European Union: Report of an assessment project co-ordinated by the World Health Organization*, DG SANCO, WHO, 2008. <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/WHO.pdf>

⁸⁷ Hodge Jr., J. G., "The evolution of law in biopreparedness", *Biosecurity and Bioterrorism*, 10(1), 2012, pp. 38-48.

⁸⁸ E.g. Jacobson, P. D., J. Wasserman, A. Botosaneanu, A. Silverstein, & H. W. Wu, "The role of law in public health preparedness: Opportunities and challenges", *Journal of Health Politics, Policy and Law*, 37(2), 2012, pp. 297-328; O'Connor, J., P. Jarris, R. Vogt, & H. Horton, "Public health preparedness laws and policies: Where do we go after pandemic 2009 H1N1 influenza?" *The Journal of Law, Medicine & Ethics*, 39, 2011, pp. 51-55.

- Lack of legal training for local practitioners and the difficulty of obtaining clarification and consistent legal advice regarding public health preparedness
- Preparedness and capability of the legal workforce to provide legal advice in real time.

5 ETHICAL IMPACT ASSESSMENT OF PULSE TOOLS, TECHNOLOGIES AND PROCEDURES

This chapter first documents the results of the internal ethical risk assessment of the PULSE tools carried out by the PULSE project partners between November 2015 and February 2016. Next, it documents the results of the external ethical risk assessment of the key risks, their likelihood and potential impacts of the PULSE carried out through interviews with external stakeholders⁸⁹ in April 2016. Both the exercises are to be treated as separate yet complementary exercises. This chapter also addresses data protection issues, and briefly summarises the ethical, economic, legal, political and societal (EELPS) assessment with trial exercise participants. Finally, it presents how the EIA outcomes have and should be integrated into the project.

5.1 INTERNAL ETHICAL RISK ASSESSMENT

Risks can impact a project and organisations involved in the short, medium and long term. The risk assessment process involves an identification of risks followed by an evaluation or ranking of the risks.

The PULSE LEPMI team developed a template for mapping each of the individual tools developed in PULSE against the respective threats, vulnerabilities, risks, their likelihood, potential impact and mitigation measures. The team prepared the table (Annex 10) drawing on its experience of preparing impact assessment templates and methodologies, and drawing on a range of sources, including the UK Information Commissioner's approach to Privacy Impact Assessments (PIAs).

In this risk assessment exercise, each individual tool of the PULSE platform was evaluated in WP8 collaboratively by Trilateral and the technical partners Leonardo Finmecannica and Skytek. This exercise (carried out between November 2015 and February 2016) enabled the technical and WP8 team to reflect upon the risks of the tools and stimulate the discussion of the mitigation measures and any steps needed to be taken in the final integration of the PULSE platform. Annex 10 documents the results of the internal ethical risk assessment of the PULSE tools.

While no 'high likelihood' risks were identified, risks marked 'medium likelihood' include: Ineffective delivery of healthcare for individuals and communities; adverse impact on the relationship between patients as a group and organisations involved (such as clinical teams, hospitals), denial of service attacks, data breaches, discrimination, failure of the system, erroneous results. The two risks highlighted for 'serious' potential impact were: data breaches resulting in information security and privacy issues, human suffering or loss of

⁸⁹ See section 2.5.1.2 for details of external stakeholders.

life, amplification of effects of the crisis, and legal prosecution and adverse impacts on the crisis managers (both individuals and organisations).

5.2 EXTERNAL ETHICAL RISK ASSESSMENT (INTERVIEW-BASED)

Additionally, the key risks, their likelihood and potential impacts of the PULSE (see table below which contains the template used) were discussed with external stakeholders in the interviews carried out in April 2016.

Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)
Information confidentiality and system security risks		
Human suffering, amplification of crisis effects/ Risk to health and safety of people		
Adverse impact on decision makers' abilities to, when needed, find the "most-efficient" way to handle emergencies.		
Risk of mis-assessing the crisis/emergency		
Ineffective coordination and management of the health emergency events		
Ineffective delivery of healthcare for individuals and communities		
Risk to privacy and personal data		
Violation of intellectual property rights		
Adverse impact on relationship between patients (as a group) and organisations involved (such as clinical teams, hospitals)		
Surveillance via profiling and geotagging		
Psychological and other unforeseen harms		
Discrimination in relation to treatment of patients		
Irrelevance and future redundancies of the PULSE training tools		
Unethical and unprofessional actions by trainees		
Harm to vulnerable groups/individuals (due to e.g. inability to provide informed consent)		
Any other risks – please specify.		

Table 2: Risks, likelihood and potential impacts template

Only one out of the eight interviewees did not respond to this table (stating responses were too dependent on what the platform looks like). Annex 11 presents the raw data. Below we present graphical summaries documenting the views of the interviewees on specific risks, their likelihood and potential impacts.

Information confidentiality and system security risks

Feedback received suggested that the level of the likelihood depends on how confidentiality and security were handled, if the system is open to breaches then the risk would be high. The risk likelihood would depend on security implementation, use of encryption, access restriction; if this is not adequate, the risk likelihood would be high. One interviewee clarified that the potential impact of this risk would be catastrophic, depending on context.

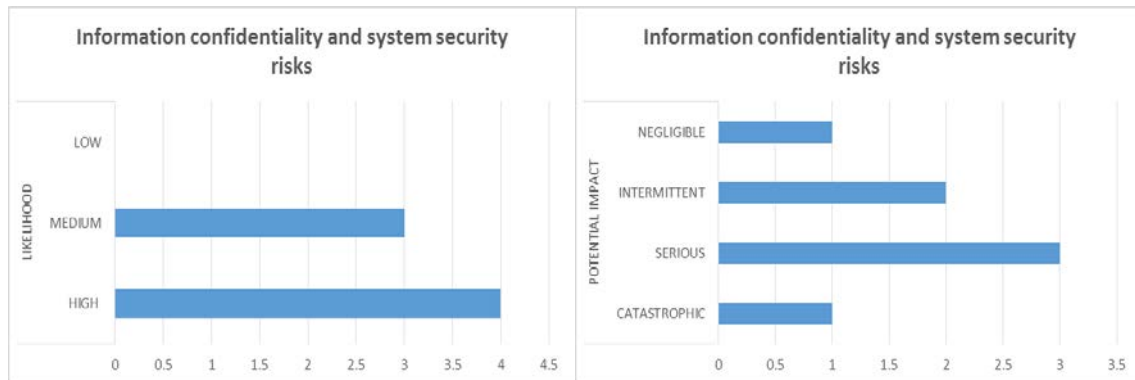


Figure 5: Stakeholder views on likelihood and impact of information confidentiality and system security risks

Human suffering, amplification of crisis effects

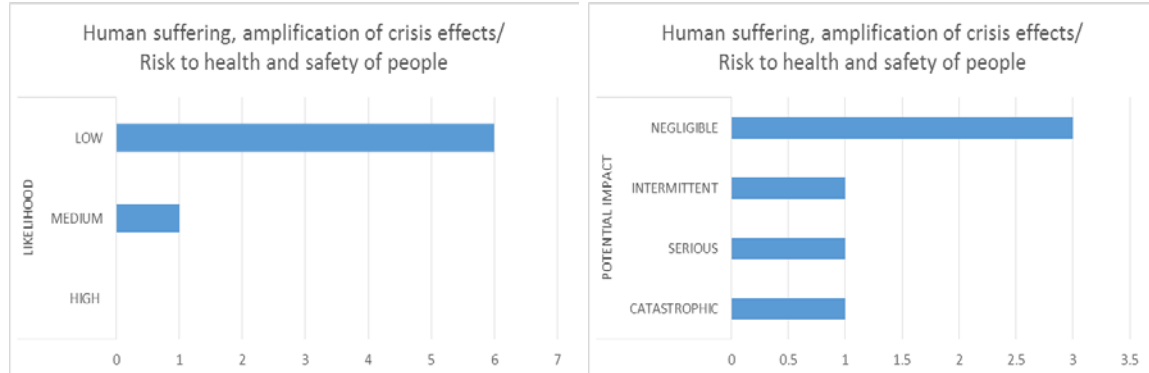


Figure 6: Stakeholder views on human suffering, amplification of crisis effects

One interviewee expressly commented that the likelihood of the risk is low if the platform works well. The potential impact would be negligible if effects were effectively addressed. One interviewee did not respond about the potential impact.

Adverse impact on decision makers' abilities

Two interviewees responded stating this depended on the structure and implementation of the platform. Another interviewee stated both risk likelihood and potential impact depended on how the system is integrated and its level. One interviewee underlined that this risk was low, if addressed in training.

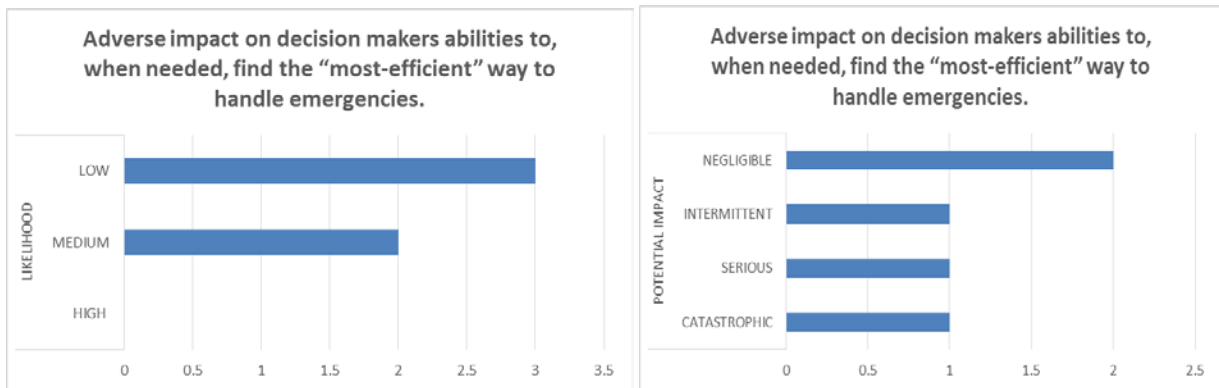


Figure 7: Stakeholder views on adverse impacts on decision makers' abilities

Risk of mis-assessing the crisis/emergency

One interviewee stated both risk likelihood and potential impact depended on how the system is integrated and its level. One interviewee did not answer this question.

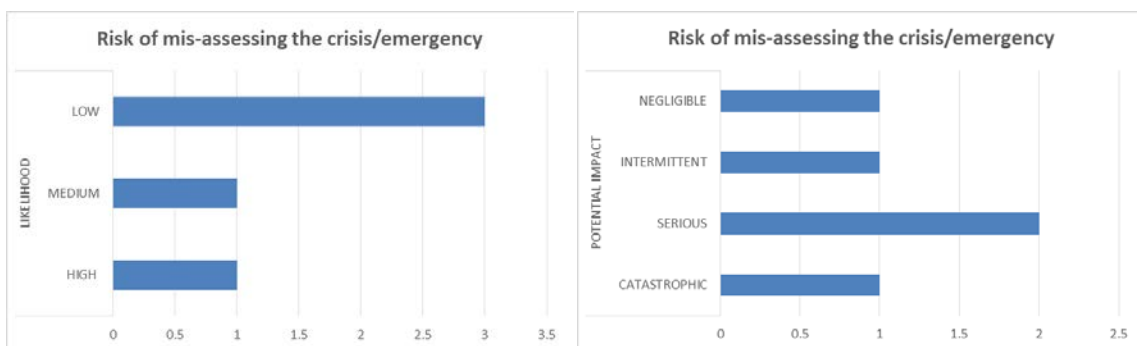


Figure 8: Stakeholder views on risk of mis-assessing the crisis

Ineffective coordination and management of the health emergency events

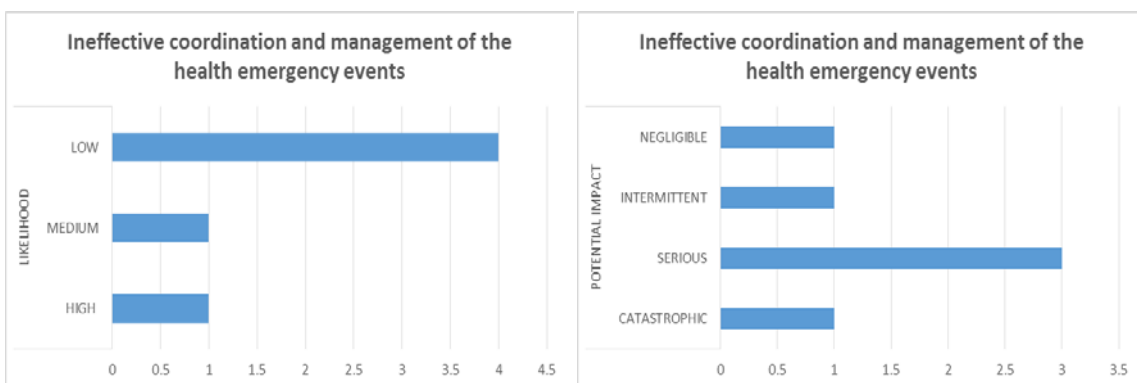


Figure 9: Stakeholder views on ineffective coordination and management of the health emergency events

One interviewee suggested this relates back to training and management i.e. poor coordination – high risk, if dealt with, low risk. One interviewee did not answer this question.

Ineffective delivery of healthcare for individuals and communities

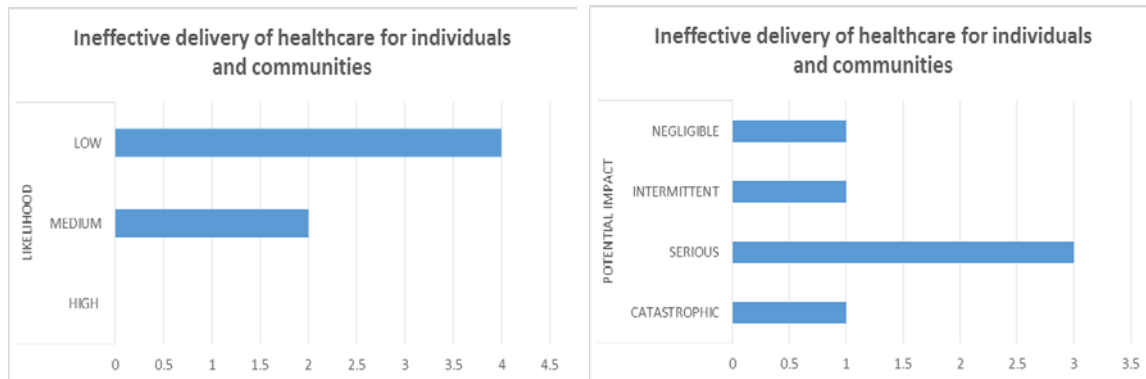


Figure 10: Stakeholder views on ineffective delivery of healthcare for individuals and communities

One interviewee said both the likelihood and potential impact depends on how the system is integrated and its level. It may also depend on the resources that are available. Another clarified that there might be a problem if doctors rely more on data and the system, than their intuition.

Risk to privacy and personal data

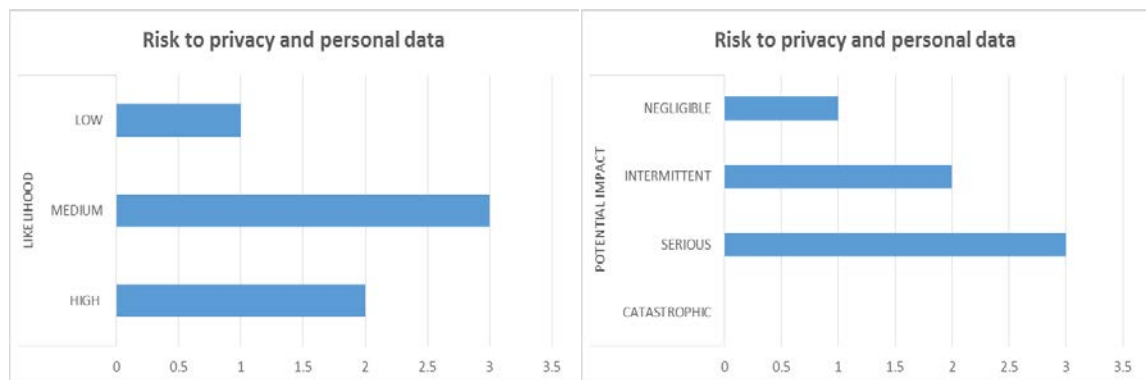


Figure 11: Stakeholder views on risks to privacy and personal data

One interviewee said it depends on the type of personal data collected, handled and shared. Also, another stated this risk might not apply in emergency.

Violation of intellectual property rights (IPRs)

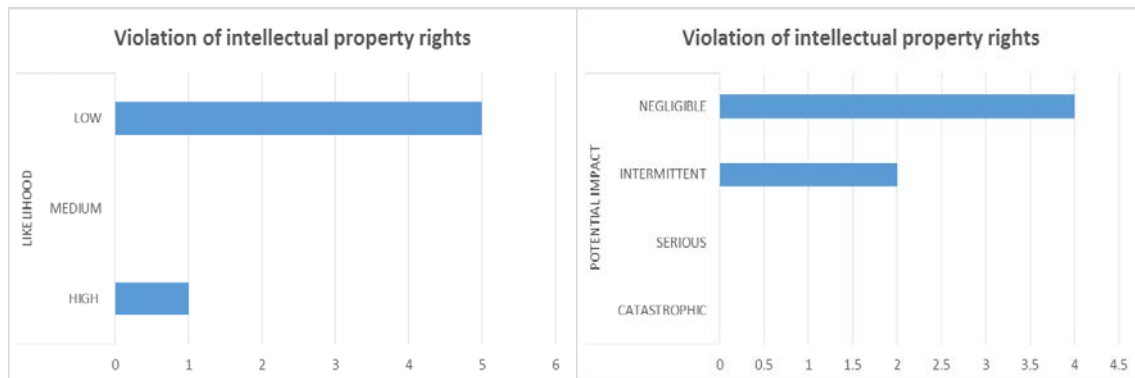


Figure 12: Stakeholder views on violation of IPRs

The potential impacts of this risk depended on how IPR were addressed. Another interviewee specifically highlighted there might be a potential negative impact if proprietary information is used. One interviewee did not respond.

Adverse impact on relationship between patients (as a group) and organisations involved (such as clinical teams, hospitals)

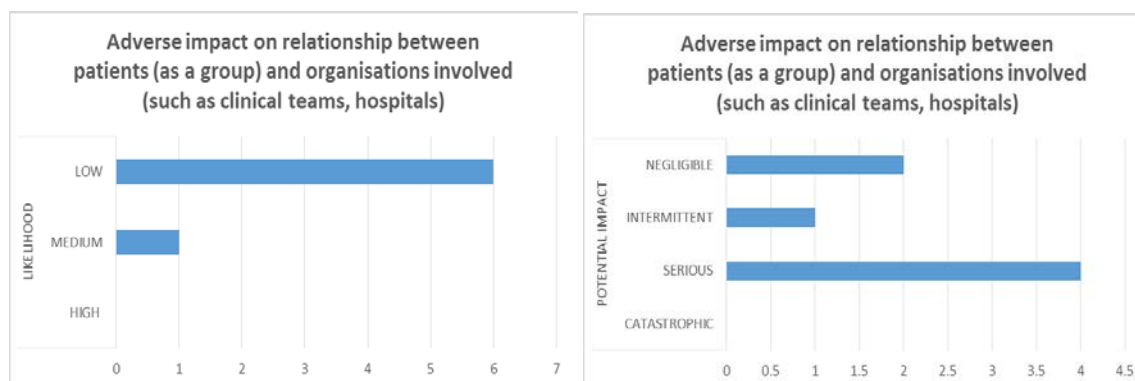


Figure 13: Stakeholder views on adverse impact between patients and organisations involved

One interviewee explained the level of this risk depended on the organisations of teams, training and communications with, and awareness of patients. Another interviewee explained that this risk likelihood depended on whether the system duplicates existing efforts, otherwise it was low.

Surveillance via profiling and geotagging

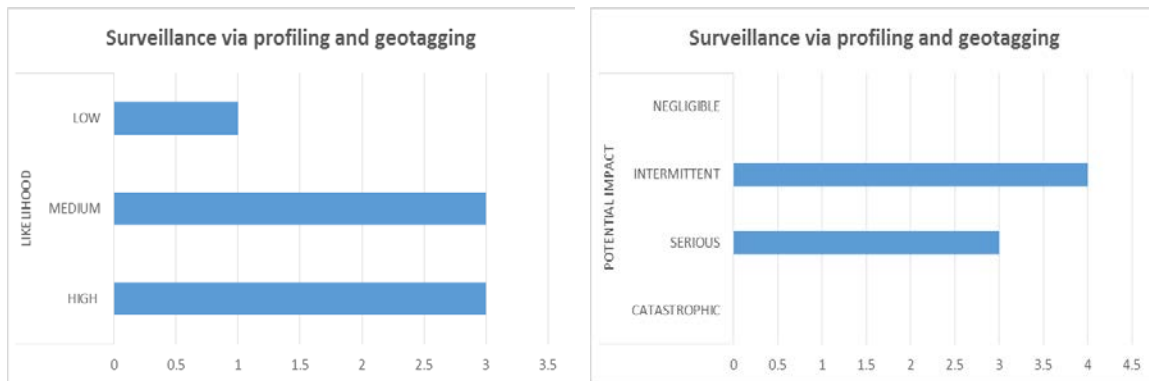


Figure 14: Stakeholder views on surveillance

One interviewee stated that there is an impact if people are tracked; they should be informed. If subjects don't accept tracking, there might be an infringement of their rights. Another interviewee underlined that the risk likelihood was high due to a risk of misuse outside emergency context; the potential impact would be serious if people decide not to use the system due to surveillance concerns.

Psychological and other unforeseen harms

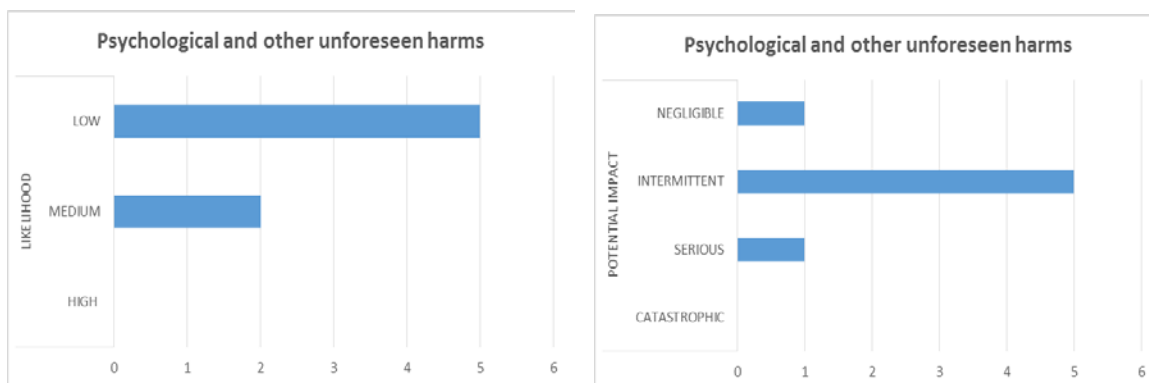


Figure 15: Stakeholder views on psychological and other unforeseen harms

One interviewee explained that if, for example, people are transferred outside their country and culture in a public health emergency, they may become distraught. If an English-speaking person is transferred to a German hospital and does not understand the language, it might lead to alienation. Another interviewee said this risk likelihood depends on who can access images, medical information.

Discrimination in relation to treatment of patients

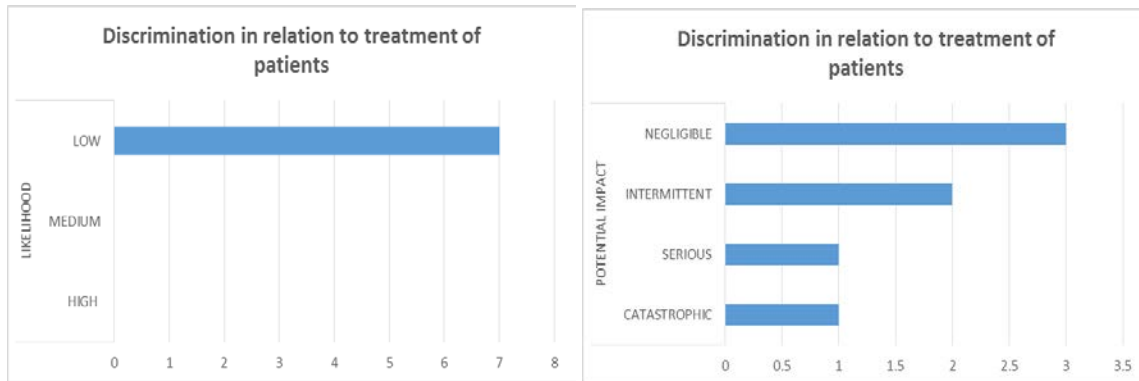


Figure 16: Stakeholder views on discrimination in relation to treatment of patients

One interviewee explained that the risk of discrimination depends on the criteria of prioritisation. It would be low if international standards are followed. If other criteria which aren't based on high ethical standards are used, then risk likelihood would be high and potential impact could be catastrophic.

Irrelevance and future redundancies of the PULSE training tools

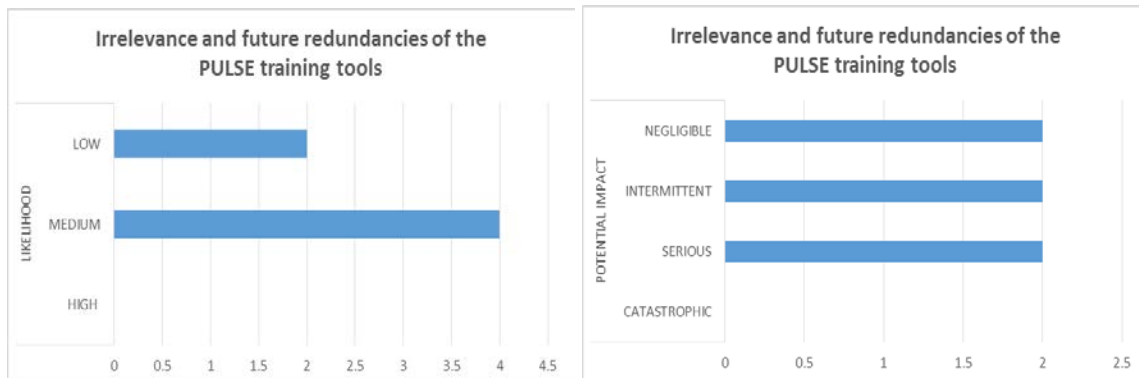


Figure 17: Irrelevance and future redundancies

Two interviewees clarified that the likelihood of this risk is low if the PULSE tools are continually updated. One respondent did not answer.

Unethical and unprofessional actions by trainees

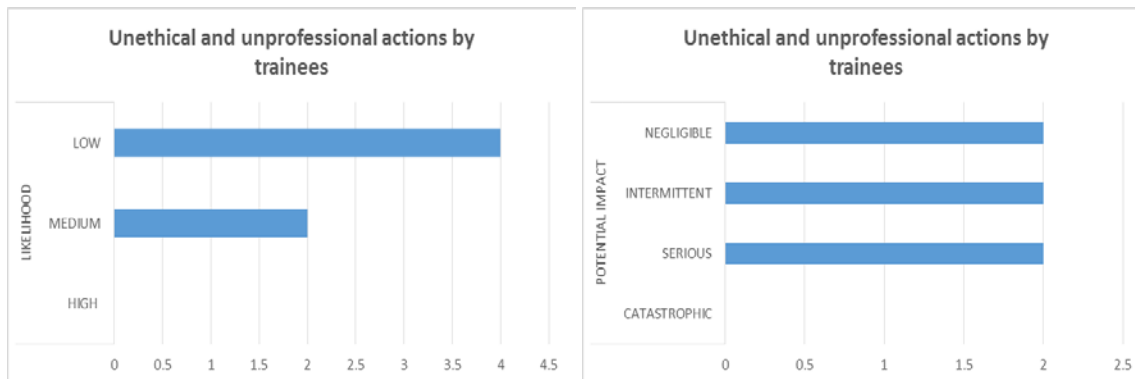


Figure 18: Unethical and unprofessional actions by trainees

One interviewee clarified that there is always a likelihood of such risk, but a low level of likelihood if proper training is provided. If not, the likelihood of risk is high, with corresponding serious impact. One respondent did not respond to this question (citing it was not applicable as it was of a purely hypothetical nature).

Harm to vulnerable groups or individuals

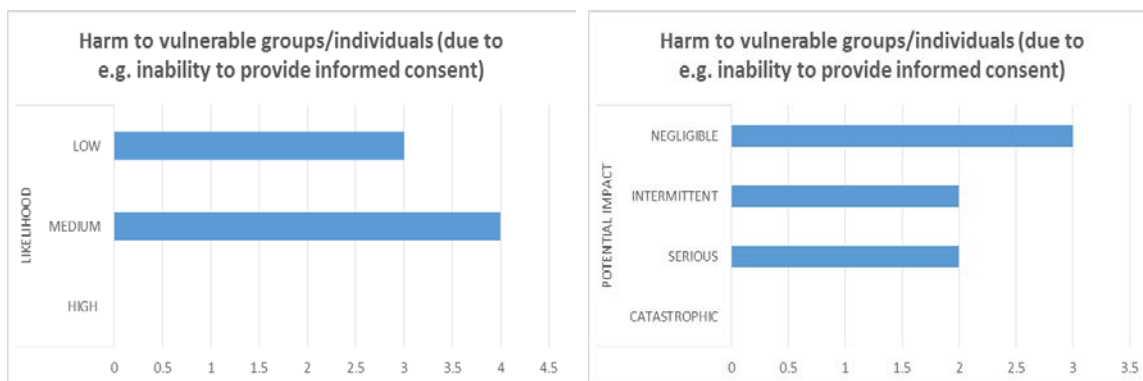


Figure 19: Harm to vulnerable groups or individuals

One interviewee (while clarifying why this risk likelihood was low) stated that in an emergency, informed consent is not an issue. International regulations and guidelines make provisions for overriding of consent in emergency, and deal with circumstances under which consent is difficult to obtain (e.g. disease).

5.3 OTHER RESULTS OF STAKEHOLDER CONSULTATIONS HELD IN APRIL 2016

This part documents the other consolidated results of the stakeholder consultations (Section 5.2 covered the risk assessment results) held in April 2016. The consortium has published these results on the PULSE website.⁹⁰

⁹⁰ <http://www.pulse-fp7.com/results-of-pulse-stakeholder-consultations-held-in-april-2016-are-now-available/>

Ethical issues raised by the PULSE Platform

The interviewees highlighted the following ethical issues in relation to the PULSE Platform:

- Dignity.
- Issues relating to the effectiveness of the platform.
- Non-identical handling of clinical scenarios in different jurisdictions; difficulties in harmonisation.
- Privacy and consent.
- Sharing of data.
- Storage and use of data
- Whether the system represents an improvement on existing structures and systems.

EU-level or national-level policy initiatives related to public health emergency management that might have an impact on the use and/or the implementation of the PULSE Platform

Interviewees highlighted the following issues when asked about whether EU-level or national-level policy initiatives related to public health emergency management that might have an impact on the use and/or the implementation of the PULSE Platform:

- Any EU developments would have to **integrate with existing national policies**.
- There are **many other platforms in different areas**: Similar programmes such as the Early Warning and Response System (EWRS) at the EU level!
- **EU-level initiatives highlighted**: General Data Protection Regulation, NIS Directive, telecoms policies.
- All countries have **national policies for emergency care** (and emergencies ranging from political emergencies to disasters (e.g. chemical disasters)).
- National health systems are **complex structures**; responsibilities of people and departments vary between countries.
- Politico-legal frameworks in different countries especially **devolved** ones are something to watch out for.

EU or national-level policy initiatives related to emergency management that might limit PULSE's effectiveness

In relation to EU or national-level policy initiatives related to emergency management that might limit PULSE's effectiveness (particularly in relation to improving the preparedness and response of emergency health services), interviewees raised the following issues:

- Who will use PULSE system? There are different implications: regional level is different from the national level.

- Confidentiality of information: treated differently at the regional level, and in different areas of the same country.
- PULSE structure is detailed and good, but the major concern is that it seems to do things that are already being done. How is PULSE adding value?
- Greater need to co-ordinate with what already exists. The threat is two or more regulatory bodies asking you to do the same thing.
- May be a LIMIT or an OPPORTUNITY.
- May be useful to look at instruments already developed and being used at the national level for information sharing, surveillance, risk assessment, national epidemiological surveillance.
- PULSE should be open and try to engage with people in various countries to try and push this forward – i.e., to harmonise across Europe and how we deal with different disasters.

EU-level burdens

When asked whether implementing the PULSE platform would impose any burdens at the EU level and what they might be, interviewees highlighted the following:

- If super-imposed = practical problems and additional burdens for participants e.g. issues related to excess paperwork, re-input of data in different systems.
- Financial and resource burdens: cost of maintenance, funding, infrastructure to make those developments and to apply the PULSE platform.
- The platform needs to work well during an emergency – needs to be well oiled and well-funded.
- There is also the issue of who is responsible for doing what – which government body, who has the responsibility – this has impacts for the system long term.
- Need to harmonise outputs of similar EU projects.

Legal or other factors might affect the cross-border implementation of PULSE

Interviewees highlighted the following legal or other factors might affect the cross-border implementation of PULSE:

- Europe is not homogenous; countries have **different laws and regulations related to health care**.
- **Diverse data protection laws** (will be alleviated with the General Data Protection Regulation).
- **Issues surrounding protection of confidentiality** and treatment of sensitive data (depends on final use of PULSE)
- **Legal differences between countries related to which healthcare professionals can do what** – roles differ from jurisdiction to jurisdiction.
- **Ethics are contextual** – e.g. prioritisation of care; this differs across countries.

Regulatory barriers

Interviewees highlighted the following regulatory barriers that might hinder the cross-border operation of PULSE-like services:

- PULSE might challenge or conflict with some plans and practices for dealing with national emergencies within countries.
- To have effect on cross-border operation, PULSE will need acceptance by Member States and approval by competent authorities.
- National level clearance for sharing sensitive information.
- Divergence in recognition of medical credentials.
- Deploying the PULSE system in countries outside the EU might be a problem (e.g. due to inadequacy of data protection in third countries).

Constraints in relation to how medical resources are allocated in public health emergencies that might affect PULSE

Interviewees identified the following constraints:

- The constraints would depend on who would be doing the allocation.
- Challenges in terms of health care budgets
- Depends on who will pay for the use of PULSE.
- Depends on cost evaluations and decisions at regional, national and local levels, and the cost of integration, interconnection between systems.

The PULSE external stakeholder consultation thus brought into focus several issues and concerns that are relevant, not only in the present project stage but also during the later use and implementation stages, during its exploitation phase. Systems that are like PULSE would also benefit from reviewing the issues and recommendations that our stakeholders have made.

The above exercises, specifically the identification of ethical issues, also suggest that ethical dilemmas might arise in the PULSE context – dilemmas arise when there is a possibility of adopting multiple courses of action.⁹¹ It is often not easy to resolve such dilemmas. The recommended courses of action to address ethical dilemmas include: gathering adequate information, referring to ethical guidelines and good practice documents, consulting with experts and colleagues.⁹² All this helps make an informed decision about the dilemma.

5.4 ADDRESSING DATA PROTECTION

This section outlines how data protection aspects have been considered in the PULSE system. This section was prepared based on research, collaborative mapping of information flows of the PULSE system with the technical partners, and consultation with the data protection authority (as outlined).

⁹¹ Lo, Bernard, *Resolving ethical dilemmas: A Guide for Clinicians*, Wolters Kluwer, Philadelphia, 2013, p. 12

⁹² Ibid.

5.4.1 PULSE data controller

Controller means the natural or legal person, public authority, agency or any other body which **alone or jointly with others determines the purposes and means of the processing of personal data**; where the purposes and means of processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community law. Data controllers are obliged to follow the rules set out in Directive 95/46/EC⁹³ i.e.

- Personal data must be processed legally and fairly;
- It must be collected for explicit and legitimate purposes and used accordingly;
- It must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed
- It must be accurate, and updated where necessary;
- Data controllers must ensure that data subjects can rectify, remove or block incorrect data about themselves;
- Data that identifies individuals (personal data) must not be kept any longer than strictly necessary;
- Data controllers must protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks. They shall implement the appropriate security measures;
- These protection measures must ensure a level of protection appropriate to the data.

In principle, all data controllers must notify their supervisory authorities when they process personal data. Skytek confirmed itself as the data controller for the purposes of the Cork trial. The LEPPi contacted the Irish Data Protection Commissioner's Office in July 2016 to verify if there was a need to notify. The Irish Data Protection Commissioner's Office reviewed the PULSE Informed Consent Form (Annex 8 contains the final approved version) for the Cork trial in August 2016 and made very useful recommendations, following which it was revised and finalised.

All the PULSE partners have nominated data protection officers for their organisation (list on file with LEPPi team). The mandate of the DPOs in PULSE was to foster data protection compliance across the entire consortium by bearing responsibility for ensuring that their organisation complies with data protection law, PULSE WP8 and Ethical Review Committee advice and recommendations on data protection.

⁹³ European Parliament and the Council of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L* 281, 23 Nov 1995, pp. 0031 – 0050.

5.4.2 Mapping of information flows in the PULSE system

To understand in greater depth the privacy and data protection impacts, we needed to understand the data processing within PULSE. Partners (technical) provided input regarding what data will be collected and processed by the eight PULSE tools and in each of the scenarios. Information flows can be recorded in whichever format meets the needs of the project (a flowchart, an information asset register, a project design brief). A good information flows map aims to provide an overview of the following:⁹⁴

- The personal data to be processed (types, nature...)
- How personal information will be collected, used, disclosed, retained, secured and disposed of (including who is responsible), how the technology will be used for each of these activities, and an explanation for what its use, from whom it was obtained and to whom it will be disclosed
- Who will have access to personal information throughout its lifecycle, for what purposes, and with what privileges. For example, who will process, browse or modify personal information, including program and IT staff, other programs providing services relevant to the project, and your partners and third parties.
- How personal information will flow through existing and planned programs, systems or processes during each associated business process.
- How and when personal information will move beyond the custody of the institution, to the custody of a third party.

The analysis aims to identify the personal information involved and determine how it will flow through the business processes and technology. If the project will change an existing program or system, it needs to determine whether it will alter the current flow of personal information. We need to map the flow of personal information in all formats, from creation or collection, until final disposition, for example, secure destruction or transfer to appropriate archives. This vital step will be the basis of privacy/data protection analysis. It is useful to develop diagrams or descriptions that are readily understood by the project and decision-makers. The following information flow table⁹⁵ (prepared in liaison with the PULSE technical partners) helps visualise the personal information flows (of the future fully implemented) PULSE system:

Types of personal information that will be collected by the system when implemented	Full name, nickname, screenname, password, home address, email, address, date of birth, birthplace, telephone number
Who will collect the information and	The PULSE system will aggregate the information from first responders and casualties through the use of the DSVT and the

⁹⁴ Information and Privacy Commissioner of Ontario, *Planning for Success: Privacy Impact Assessment Guide*, May 2015, p. 15.

⁹⁵ Adapted from Information and Privacy Commissioner of Ontario, *Planning for Success: Privacy Impact Assessment Guide*, May 2015, p. 14.

why	smartphone app. Personal information will be stored to monitor affected individuals (patient's) health status and to keep track of the first responders.
Who will use the information and why	The information will be used by the emergency coordinator (using the DSVT) or the first responder (via the smartphone app). The information will be used to perform analysis for decision support and to provide updated contextual information to the emergency coordinator using the DSVT.
How the information will be retained and for how long	The information will be stored in the PULSE internal tools repositories ⁹⁶ and will be stored securely until it is deleted ⁹⁷ .
How the information will be secured	To avoid unauthorized access to the data managed by the PULSE tool, the information will be secured by the PULSE authorisation tool that uses the OAuth2 standard to secure the communication between the PULSE tools.
To whom and how the information might be disclosed	The information will be available to the PULSE platform users through the GUI provided by the DSVT and the Smartphone app when it is necessary to get an overview on the casualties' health status and on the first responders' profiles. The information is disclosed through the DSVT and the Smartphone app to provide support to the decision makers.
How and when the information will be disposed	Information will be disposed by the Logistic tool, PCET, Authorisation tools by directly deleting the information in the repository when a DELETE request is sent to the tool e.g. when the information is not necessary anymore, or on request by an individual. Data can be deleted by a system admin.

Table 3: PULSE Information flows

5.4.3 Addressing data protection risks

This section presents commonly identified data protection risks and presents recommendations for PULSE.⁹⁸

When informed consent is mentioned, the consortium recognises that in health-related emergency situations informed consent is not always possible and exceptions to data protection obligations may come into play. The recommendations for the PULSE project listed below are recommendations in an ideal scenario. We recognise and accept that informed consent in certain contexts is not possible and that other factors such as need to provide lifesaving treatment, might take priority.

⁹⁶ The PULSE platform could be stored on cloud (public or private) or on private servers. These servers could be the property of the entity/company that decides to use the platform.

⁹⁷ The period of retention would depend on the legal, organisational information management and security policy of the entity implementing the system.

⁹⁸ The list of data protection risks included in these tables are drawn from guidance issued by the UK Information Commissioner's Office, which draws on best practice at the EU-level.

List of data protection risks to individuals	Recommendation for PULSE
Inadequate disclosure controls increase the likelihood of information being shared inappropriately.	<p>Robust (and regularly audited) policies and procedures regarding use of, disclosure of, and information sharing both internally and with third-parties.</p> <p>Robust security measures should be implemented, including authentication servers and other security mechanisms.</p>
The context in which information is used or disclosed can change over time, leading to its being used for different purposes without people's knowledge.	Data will not be used and/or processed for any other purpose than that originally specified. If data is to be used for any other purpose, specific and informed consent from data subjects needs to be sought, prior to any processing taking place.
New surveillance methods may be an unjustified intrusion on their privacy.	Methods utilised need to be proportionate to the aim of the project and/or technology. This needs to be assessed through a thorough ethical impact assessment review process. Data collected by the PULSE tool should be minimised.
Measures taken against individuals as a result of collecting information about them might be seen as intrusive.	PULSE tools should collect the minimum amount of personal data required to fulfil their task.
The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.	<p>Data should only be aggregated for specific purposes and with the consent and knowledge of individuals.</p> <p>Data should only be shared across datasets with policies in place (and audited) related to security and privacy measures.</p>
Identifiers might be collected and linked which prevent people from using a service anonymously.	Any identifiers unnecessary to the operation of the PULSE tools should be removed and/or anonymised.
Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.	The PULSE app, platform and tools should ensure that robust safety and privacy features are enabled, implemented and audited, to prevent disclosure of information to any third parties. Internally, the PULSE tools should implement authentication systems and other safeguards, to ensure that only those authorised to have access to the system, gain access to the system.
Collecting information and linking identifiers might mean that an organisation is no longer using information that is safely anonymised. Information that is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.	<p>Once data is no longer needed for the immediate purpose, the PULSE app should delete the collected information.</p> <p>The PULSE platform, tools and app, should not collect and/or store any unnecessary data. Any data that is collected and/or stored should be managed within a framework of robust privacy and security policies to mitigate the risk of duplication of records. Data should not be stored on any external devices outside of the</p>

	PULSE system. A data management plan should be developed during the project's lifecycle.
If a retention period is not established information might be used for longer than necessary	The PULSE platform will set a specific retention period for the storage of data, in line with public health emergency management practice.
List of data protection risks to organisations using PULSE system	Recommendation for PULSE
Non-compliance with data protection or other legislation can lead to sanctions, fines and reputational damage.	PULSE is the data controller and is following an ethical impact assessment process (which encompasses data protection aspects) to mitigate risks involved in non-compliance with relevant data protection legislation. The data controller remains responsible for data processing within the project.
Problems that are only identified after the project has launched are more likely to require expensive fixes.	The PULSE project is undertaking a thorough ethical impact assessment, which includes a risk assessment, to mitigate and/or minimise problems that may arise after the project has launched. The PULSE project is also conducting a live trial and desktop exercise to simulate real-life situations, assess and manage any potential problems.
The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.	The PULSE project will abide by the provisions of the GDPR, and consider the relevant guidance from the Article 29 WP ⁹⁹ (in the future, the European Data Protection Board). The policies and procedures developed for the PULSE project will address (if needed) the use of biometric data, and limitations on its usage.
Information that is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.	The PULSE platform, tools and app, should not collect and/or store any unnecessary data. Any data that is collected and/or stored should be managed within a framework of robust privacy and security policies to mitigate the risk of duplication of records. Data should not be stored on any external devices outside of the PULSE system. A data management plan should be developed during the project's lifecycle.
Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.	The PULSE project is open about the collection of personal data and its uses. The project is conducting an ethical impact assessment to identify, assess, manage and mitigate any potential issues in relation to data collection and usage.
Data losses that damage individuals could lead to claims for compensation.	Data collected on the mobile app is deleted from the device as soon as it is no longer required (and stored on a secure server)
List of data protection compliance risks	Recommendation for PULSE
Non-compliance with data protection	The PULSE EIA covers EU data protection

⁹⁹ E.g. Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, Adopted on 27 April 2012. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

law	legislation. Future implementation of PULSE must also be in line with data protection law, as applicable.
Non-compliance with sector specific legislation or standards.	The PULSE EIA has identified international legal frameworks for preparedness, planning and response to public health emergencies and relevant EU and international CIP legislation and guidelines that must be considered.
Non-compliance with human rights legislation.	The PULSE EIA encompasses human rights legislation, and the implementation of the PULSE platform should be in line with these.

Table 4: Data protection recommendations

5.4.4 Data protection post-project completion

The above data protection analysis and recommendations should be considered in the future use and implementation of the PULSE system i.e. after the completion of the project. Particularly, attention should be paid to:

- Notification/registration with the data protection authorities.
- Purpose limitation.
- Re-use of data (by third parties, etc.)
- Transfer of data
- Deletion of data
- Aggregation of data across data sets (etc.)

To support good practice both in PULSE and other similar projects, Annex 12 contains a data protection checklist.

5.5 ETHICAL, ECONOMIC, LEGAL, POLITICAL AND SOCIETAL (EELPS) ASSESSMENT WITH TRIAL EXERCISE PARTICIPANTS

To support future decision makers using the PULSE or similar systems in evaluating the system's ethical, economic, legal, political and societal (EELPS) relevance and impacts, the PULSE consortium developed the EELPS methodology and tested a sample of its criteria using questionnaires in the two PULSE trial exercises. The methodology offered is a typical multi criteria decision analysis (MCDA) tailored to the numerous specific non-quantifiable qualitative criteria relevant for security-related planning and decision making processes.

The aim of the EELPS methodology (explained fully in *PULSE Deliverable 7.1 Trials Definition*¹⁰⁰ and *D7.3 Validation Results*) is to assist in determining the ethical, economic, legal-political and societal impacts of the PULSE system. This assessment methodology is intended to be used at two levels (a) with participants at the PULSE trial exercises (b) as a guidance for future commissioners or end users of the PULSE, or of PULSE-like systems.

¹⁰⁰ Mari, Pasquale, Francesco Lauria, Reinhard Hutter, Hans Kühl, (CESS), Cian O'Brien (HSE), Peter Daly (HSE), Viorel Pecteu (OST), Francesco Malmignati, Massimiliano Taglieri, Rowena Rodrigues, *PULSE Deliverable D7.1-Trials Definition*, 31 May 2016.

As part of the PULSE trial exercises, the PULSE consortium provided a questionnaire to participants via Typeform in the Rome EVD¹⁰¹ and Cork MCI¹⁰² trial exercises. The questions were finalised based on the EELPS criteria catalogue devised for PULSE by partners CESS and TRI collaboratively under WP5, 7 and 8 collaboration. The objective of the questionnaire (Annex 13) was to determine the ethical, economic, legal, political and societal impacts of the PULSE system. There were five sets of questions focussing on the ethical (4 questions), economic (2 questions), legal (3 questions¹⁰³), political (3 questions) and societal (2 questions) aspects. There was also an open section for recommendations and remarks in the questionnaire. *PULSE Deliverable 7.3* documents the results of the questionnaire based assessment and provides an example of a full-scale application of the tool.¹⁰⁴

5.6 INTEGRATING EIA OUTCOMES INTO THE PROJECT

It is not enough to conduct an ethical and societal impact assessment; to be meaningful, it should be integrated into the project, as early on, during and even after the completion of the project (during uptake). This would support ethically sound decision making and actions. The following table briefly outlines how the PULSE EIA outcomes have been integrated into the project.

Actions taken/to be taken	Period for completion of actions	Responsibility for action
Monitoring of ethical aspects via WP8	Duration of the project	Trilateral Research Ltd.
Ethical advice and support: attendance at project meetings, support to other WPs	Duration of project	Trilateral Research Ltd., PULSE ERC
Implementation of ethical recommendations	As needed, during design, development and testing of PULSE system.	PULSE consortium partners
Consultation of the PULSE EIA and EELPS assessment results	During the future implementation and use of the PULSE system	End users of the PULSE tools and system. Emergency health policy makers.
Review of the PULSE EIA	September-October 2016	PULSE ERC, members of the public

Table 5: Integrating EIA outcomes

6 CONCLUSIONS AND RECOMMENDATIONS

This document presented the results of the ethical impact assessment WP of PULSE. Based on this multi-pronged exercise, and the feedback we have received from the various discussions with stakeholders at various stages of the project,

¹⁰¹ <https://pulsefp7.typeform.com/to/kuFoUY>

¹⁰² <https://pulsemcitrial.typeform.com/to/KlpHHJ>

¹⁰³ Note, after the Rome trial, the PULSE consortium added a question on data protection risks into the evaluation.

¹⁰⁴ Annex 1 of D7.3.

we now summarise the key recommendations (that emerged from the PULSE EIA, particularly from the discussions with stakeholders) for PULSE stakeholders. These recommendations may also be relevant for other similar systems used for managing public health emergencies.

Recommendations for policy-makers

- Policy-makers should foster **respect for fundamental rights in the implementation of public health emergency measures**.¹⁰⁵
- Member States should **monitor public health emergency measures**, particularly those implemented by private companies and agencies, to ensure they are bound by the same **legal and ethical obligations**, and should put in place mechanisms to **monitor compliance** with such obligations.¹⁰⁶
- Public health emergency policymaking should pay attention to the **following principles**: provide care notwithstanding personal risks, accountability mitigation, privacy of personal and sensitive information, and over-triage or under triage.¹⁰⁷
- If the PULSE project proceeds to commercialise its system, stakeholders involved in the commercialisation should promote and create **buy-in** from senior people, national leaders, healthcare delivery leaders at the government and ministerial level (including different DGs of the EC).¹⁰⁸
- Industry and policy-makers should collaborate in the development of **effective, shared strategies and promote discussion on reducing potential legal complications** in cross border cooperation and collaboration in emergencies.¹⁰⁹

Recommendations for the implementers and end users of the PULSE system

- Stakeholders involved in implementing the PULSE system should ensure it is done in a **co-ordinated manner** – while considering the complexities and practicalities of the public health emergency management.¹¹⁰
- The PULSE system managers **should share knowledge** with users and the public, ensuring **transparency** of the system.¹¹¹
- Specifically, the **PULSE system users should respect the purpose limitation principle**, i.e., using the system only for its designated purpose, demonstrating legitimate use and minimising the potential for misuse of the system outside an emergency context.¹¹²

¹⁰⁵ Chapter 3.

¹⁰⁶ See Section 2.5.2 Identification of ethical principles, threats, vulnerabilities, risks and mitigation measures relevant to PULSE.

¹⁰⁷ Ibid, and Chapter 4.

¹⁰⁸ This was a point made in the interviews with external stakeholders.

¹⁰⁹ Chapter 4, Section 5.3, Annex 9.

¹¹⁰ Section 5.3.

¹¹¹ Sections 3.2, 3.6, 4.2, Annex 10.

¹¹² Sections 3.2, 5.4.4.

- The PULSE system implementer should support training for operators, and employees on how to manage ethical issues.¹¹³
- Health managers **should be accountable for how they use and/or process personal data.**¹¹⁴
- PULSE system end users should have a **good understanding** of the differences in healthcare practices and priorities across jurisdictions; they consult relevant authorities to develop this understanding.¹¹⁵
- PULSE system end users should **create better media and public awareness** about the usefulness of the system and the way risks will be managed.¹¹⁶

Recommendations for designers and developers of similar systems

- Designers and developers of similar systems should **consult the PULSE EIA and EELPS assessment results as a reference point**, and review the recommendations of other relevant projects that have considered ethical, legal and societal aspects.
- They should **conduct a privacy impact assessment and/or ethical impact assessment** (e.g., using the tools such as EELPS proposed in PULSE) in consultation with relevant stakeholders.
- They should consider, address, review and improve (as technology progresses) the **security and integrity** of the system, and **protect it against internal compromises and external attacks**. They should use strong encryption and optimise access controls.¹¹⁷

¹¹³ Section 5.2.

¹¹⁴ Section 3.2.

¹¹⁵ Section 5.3.

¹¹⁶ Sections 2.5.2, 5.5.2 and Annex 4.

¹¹⁷ Section 3.5, 3.6, Annex 10.

ANNEX 1: ETHICS APPROVALS: FORM AND APPROVALS



PULSE ETHICAL APPROVAL FORM

I have considered the application for ethics approval for the following deliverable:

Project	Platform for European Medical Support during major emergencies (PULSE)
Work Package	WP7 Trials and Validation
Deliverable	D7.1 Trials Definition

Please complete the following:

1. Does the deliverable adequately address ethical issues and considerations in the definition of the trial exercises?
2. Does it address the recruitment, inclusion and exclusion criteria for prospective participants in the trials?
3. Does the deliverable outline steps to provide information to trial participants about what to expect in the trials and about the use of their data?
4. Does the deliverable include an adequate Informed Consent form?
5. Does the deliverable include details on methods used for tracking or observing participants?
6. Does the deliverable address the responsibilities of researchers and exercise leaders involved in the trials?

Please strike out what is not applicable:

I give ethical approval for this deliverable.

I give ethical approval subject to the following (please provide details):

I cannot give ethical approval for the following reasons (please provide details):

Signed:

Full name:

Date:

PULSE ETHICAL APPROVAL FORM

I have considered the application for ethics approval for the following deliverable:

Project	Platform for European Medical Support during major emergencies (PULSE)
Work Package	WP7 Trials and Validation
Deliverable	D7.1 Trials Definition

Please complete the following:

- Does the deliverable adequately address ethical issues and considerations in the definition of the trial exercises?
Yes
- Does it address the recruitment, inclusion and exclusion criteria for prospective participants in the trials?
Yes
- Does the deliverable outline steps to provide information to trial participants about what to expect in the trials and about the use of their data?
Yes
- Does the deliverable include an adequate Informed Consent form?
Yes, but I have a minor consideration: After participant has withdrawn consent, if the provided information has already been transcribed for use in the related report, it is understandable that the info can no longer be withdrawn. However, the link between that info and participant's personal data can still be destroyed. Thus, in such a circumstance, it might not be enough to handle anonymised the participant's input/feedback, but to actually proceed to an irreversible anonymization.
- Does the deliverable include details on methods used for tracking or observing participants?
Yes
- Does the deliverable address the responsibilities of researchers and exercise leaders involved in the trials?
Yes

Please strike out what is not applicable:

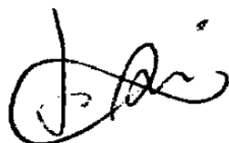
~~I give ethical approval for this deliverable.~~

I give ethical approval subject to the following (please provide details):

In case of consent withdrawal once the information has already been transcribed in the related report, the information sheet for participants should guarantee an irreversible anonymization (link destruction) of the provided input and/or feedback.

~~I cannot give ethical approval for the following reasons (please provide details):~~

Signed:



Full name:

Javier Arias-Díaz

Date: May 16, 2016

PULSE ETHICAL APPROVAL FORM

I have considered the application for ethics approval for the following deliverable:

Project	Platform for European Medical Support during major emergencies (PULSE)
Work Package	WP7 Trials and Validation
Deliverable	D7.1 Trials Definition

Please complete the following:

1. Does the deliverable adequately address ethical issues and considerations in the definition of the trial exercises?

Ethical criteria are specified in section 2.4 (pp. 10-13). However, not all of them are addressed in the definition (procedures) of the trial exercises. For example:

- There is no procedure to give information on the live exercise to members of the public in the surrounding areas of the exercise to ensure that the public do not think it is a real emergency situation.
- There are no complaints, appeals and conflict of interest procedures.
- No plans have been put in place for a real emergency or incident occurring during the trial and/or exercise (e.g., a keyword repeated three times to highlight that the trial has changed to a real emergency).
- The Stadium Crush scenario mentions the possibility of 'alternative futures'. However, these need to be mapped out prior to the exercise taking place. Trials should not encounter unforeseen/unplanned scenarios.
- There is no specification of the instructions that must be given to participants on the fairness and non-bias principles of the evaluation process and tools

2. Does it address the recruitment, inclusion and exclusion criteria for prospective participants in the trials?

No/yes. It is not specified how participants are recruited and when prospective participants must be excluded (e.g., are persons with disabilities welcome?). Only the basic types of actors are provided for each the scenarios, and the expectation is expressed that these actors are "experienced".

3. Does the deliverable outline steps to provide information to trial participants about what to expect in the trials and about the use of their data?

Yes, information on what to expect is going to be provided on the information sheet that is to be handed out to trial participants. The information has yet to be specified, however:

"The table-top exercise procedure – [UCSC to specify in brief]

The live trial exercise procedure – [Skytek/HSE to specify in brief]"

See page 48.

4. Does the deliverable include an adequate Informed Consent form?

Yes, pp. 49-50.

5. Does the deliverable include details on methods used for tracking or observing participants?

Yes

6. Does the deliverable address the responsibilities of researchers and exercise leaders involved in the trials?

Yes, in section 2.4 on the ethical criteria for the trial exercises (page 12), the responsibilities of researchers and exercise leaders are laid out:

"Responsibilities of researchers: all researchers involved in the PULSE tabletop and live exercises are responsible for knowing and following the law and the principles of good practice relating to ethics, science, information, health and safety. They will give priority to the dignity, rights, safety and well being of participants. Researchers will also protect the integrity and confidentiality of records and other data generated by the research."

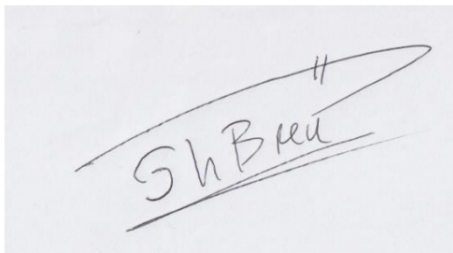
"Responsibility of exercise leaders: The exercise leaders will be directly responsible for ensuring that the exercises take place in accordance with the processes and protocols set out. The lead will take on the responsibility for the design, management and reporting of the exercise, and co-ordinating the investigators who take the lead at each site."

Perhaps these descriptions of responsibilities should be given in the outlines/plans for the individual trial exercises.

Please strike out what is not applicable:

I give ethical approval subject to the following (please provide details):

- Addressing the issues raised under questions 1, 2 and 3



Signed:

Full name: Philip A. E. Brey

Date: 05/23/2016

PULSE ETHICAL APPROVAL FORM

I have considered the application for ethics approval for the following deliverable:

Project	Platform for European Medical Support during major emergencies (PULSE)
Work Package	WP7 Trials and Validation
Deliverable	D7.1 Trials Definition

Please complete the following:

1. Does the deliverable adequately address ethical issues and considerations in the definition of the trial exercises?

Yes

2. Does it address the recruitment, inclusion and exclusion criteria for prospective participants in the trials?

Yes, however the process of how exactly participants would be sought, recruited and informed should be made clearer.

3. Does the deliverable outline steps to provide information to trial participants about what to expect in the trials and about the use of their data?

This should be made clearer – one suggestion – there should be a timeline of how the information will be provided to the (potential) trial participants, when will they be handed the information sheet, how much time (approximately) will they have to ask questions etc.

4. Does the deliverable include an adequate Informed Consent form?

I would advise that the information sheet described the goals of the project in a way understandable to a non-expert. Currently it seems it was copied from a description of the project used for different purposes.

I advise that separate Informed Consent forms were developed for the two trials and describe in more details what they will consist of.

I find the below parts problematic:

"In addition to withdrawing yourself from the study, you may also withdraw any data or information that you might already have provided up until it is transcribed for use in the related report." – withdrawal of personal data should be possible without a time limit;

"If you do decide to take part, you will be given this information sheet to keep and be asked to sign a consent form." – a clear timeline of how information will be shared with potential participants would be advisable; if the information sheet provides url links potential participants should be able to check them, so it would suggest they receive it in advance, however this is unclear at this stage.

5. Does the deliverable include details on methods used for tracking or observing participants?

I did not find relevant information in the deliverable, I would advise that the consortium makes it clear

6. Does the deliverable address the responsibilities of researchers and exercise leaders involved in the trials?

Yes

Please strike out what is not applicable:

~~I give ethical approval for this deliverable.~~

I give ethical approval subject to the following (please provide details):

Details have been provided below specific questions.

~~I cannot give ethical approval for the following reasons (please provide details):~~

Signed: *Z. Wars*

Full name:

Zuzanna Wars

Date: *23.05.2016*

ANNEX 2: PRELIMINARY STAKEHOLDER IDENTIFICATION

Stakeholder type	Name of organisation
Academia/ethical	The Medical School The University of Sheffield; Istituto Santa Ana at Pisa; University of Edinburgh.
Academic health centre	Simnova, il Centro di simulazione in medicina e professioni sanitarie dell'Università del Piemonte Orientale
Association of health law	European Association of Health Law (EAHL)
Civil society organisation/non- governmental organisation	Médecins Sans Frontières/Doctors Without Borders (MSF), Privacy International
Community health services	HSE Ireland
Emergency medical services	Ares 118 Torino (Regional EMS); GENERAL INSPECTORATE FOR EMERGENCY SITUATIONS; 118 Ares Roma; 118 Ares Milano; Emergency Response and Rescue Corps, Malta
Ethics Committee/EUREC member	Royal College of Surgeons in Ireland Department of General Practice
Humanitarian agency – EU, international	EU Humanitarian Aid and Civil Protection department (ECHO); Red Cross European Union
Fire and rescue services	Antwerp Fire Service, Belgium; London Ambulance Service
Fire and rescue services [disaster management]	GHOR- (Regional Medical Emergency Preparedness and Planning)
Government ministry	Centro de Coordinación de Alertas y Emergencias Sanitarias (CCAES); Ministerio de Sanidad, Servicios Sociales e Igualdad; USMAF
Health support service	Istituto di Rianimazione - Assistenza Stadio Olimpico di Roma; NHS Confederation Urgent and Emergency Care Forum
Hospitals	Italian National Institute for Infectious Diseases, UCSC/ Istituto di Igiene Policlinico Gemelli
Independent organisation	General Medical Council
International association of persons	European Society of Intensive Care Medicine (ESICM)

Stakeholder type	Name of organisation
International health organisation	WHO/Chair of the Commission on Social Determinants of Health
Medical accreditation organisation	Accreditation Council for Continuing Medical Education (ACCME)
Medical and travel assistance services company	HealthWatch Sa
National ethics committee	UK NHS Health Research Authority, The National Bioethics Committee, Italy
Non-profit alliance of patients, healthcare workers, academics and healthcare experts and the medical technology industry.	Health first Europe/Fipra as Special Adviser for Health and Environmental Policy
Patient support organisation	Slachtofferhulp Nederland, European Patients' Forum (EPF)
Policy maker - EU	Joint Research Centre, European Commission; ECDC - European Centre for Disease Prevention and Control; European Commission Public Health Directorate/DG SANCO Health Threats Unit
Policy maker - national	The National Coordinator for Security and Counterterrorism (NCTV), Netherlands, National Crisis Centre, Netherlands
Professional association	European Society for Emergency Medicine (EuSEM.org)
Public health authority	GGD Municipal health services
Regulator	Italian Data Protection Authority (Garante per la protezione dei dati personali); Office of the Data Protection Commissioner, Ireland.
Related EU projects	EDEN; ECOSSIAN; IMPRESS; S-HELP; TACTIC.
Representative organisation of the National Associations of Medical Specialists - EU	The European Union of Medical Specialists (UEMS)

ANNEX 3: SEMI-STRUCTURED INTERVIEW GUIDE

1. Can you think of any EU-level or national-level policy initiatives related to public health emergency management that might have an impact on the use and/or the implementation of the PULSE Platform?
2. Do you think implementing the PULSE platform would impose any burdens at the EU level? If so, what do you think those burdens might be?
3. Can you think of any EU or national-level policy initiatives related to emergency management that might limit PULSE's effectiveness (particularly in relation to improving the preparedness and response of emergency health services)?
4. Do you think the PULSE platform might have any societal, environmental or economic impacts? If so, what type? Examples include: impacts on human rights, improved or decreased health security, increased health costs, increased cooperation among health professionals, increased international technology dependencies, inefficient energy and fuel usage by ambulances, increased surveillance of individuals etc.
5. Are there any other impacts that you can think of?
6. Are there any impacts of the PULSE Platform that might be specific to the EU-level?
7. Can you think of any constraints in relation to how medical resources are allocated in public health emergencies that might affect PULSE?
8. Can you think of any legal or other factors that might affect the cross-border implementation of PULSE? E.g. national differences in critical infrastructure policies.
9. Do you know of any regulatory barriers that might hinder cross-border operation of PULSE-like services?
10. In your opinion, what do you think is the likelihood and impact of the following risks for a platform such as PULSE?

Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)
Information confidentiality and system security risks		
Human suffering, amplification of crisis effects/ Risk to health and safety of people		
Adverse impact on decision makers' abilities to, when needed, find the "most-efficient" way to handle emergencies.		

Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)
Risk of mis-assessing the crisis/emergency		
Ineffective coordination and management of the health emergency events		
Ineffective delivery of healthcare for individuals and communities		
Risk to privacy and personal data		
Violation of intellectual property rights		
Adverse impact on relationship between patients (as a group) and organisations involved (such as clinical teams, hospitals)		
Surveillance via profiling and geotagging		
Psychological and other unforeseen harms		
Discrimination in relation to treatment of patients		
Irrelevance and future redundancies of the PULSE training tools		
Unethical and unprofessional actions by trainees		
Harm to vulnerable groups/individuals (due to e.g. inability to provide informed consent)		
Any other risks – please specify		

11. Do you feel that measures could be put in place to boost the societal acceptability of the PULSE platform? If so, what type?

ANNEX 4: Mapping ISO 29001 principles to threats, vulnerabilities, risks and mitigation measures

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
Consent and choice	Individuals or external organisations may complain that PULSE provide consent and choice mechanisms	Lack of informed consent procedures	Data subjects refuse to provide personal data. Damage to PULSE reputation	Put in place consent procedures. Regular review Use of consent forms. Data protection policy and use of notices.
Purpose legitimacy and specification: ensuring that the purpose of data collection complies with applicable law, codes of best practice or other policies and procedures.	Function creep – PULSE may want to gain more value from the data it holds.	Users may ignore or are not aware that they cannot repurpose personal data (i.e., to use the data collected by PULSE for additional purposes) without seeking consent again.	Non-compliance with applicable law or codes of conduct.	Improve training and awareness of users so that they are aware that data cannot be repurposed without consent. Develop an organisational privacy and data protection policy that prohibits repurposing data without consent. Inform users of PULSE's privacy and data protection policy.
Collection limitation: limiting the collection of personal data to that which is within applicable law and strictly necessary for the specified purpose(s).	PULSE may collect more personal data than necessary for the specified purpose.	Users may not be so concerned about how much personal data they gather. Personal information is collected without a clear purpose, which increases the	Reputational risks. Additional data might create further risks. Security threats. Data quality	Specify and document the purposes for which personal information will be collected Ensure user awareness of purposes.

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
		risk of unauthorised uses and disclosures.	compromises. Profiling and surveillance	
Data minimisation: minimising the processing of personal data.	PULSE may gather more data than necessary and share it with other third parties, some of whom may not be authorised or it is not appropriate for them to have the data.	Some people may give more personal data than they need to. Some people may believe they have no choice.	Processing more personal data than necessary creates a bigger target for attackers. Some data is disclosed that was not previously identified as personal data.	Describe in the PULSE data protection policy if or how the system/tools will or might link or cross-reference separate databases. Explain why the data-matching needs to occur. Ensure each piece of data to be collected is necessary, fair and not unreasonably intrusive. Ensure that the PULSE system and processing operations are the minimum necessary for achieving their purposes and that they are transparent and fair.
Use, retention and disclosure limitation: limiting personal data to that which is necessary in order to fulfil specific, explicit and legitimate purposes.	PULSE may collect more data than needed. Users may share personal data with other organisations over which they have no control	No sufficiently adequate or regular training of staff regarding good data protection practices.	Individuals may be surprised or upset by a secondary use or disclosure of their data, resulting in	Share personal information with other organisations only if the individual has consented to such sharing and only if the other organisation has given written

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
	<p>regarding how the other organisations may use that data or further share it.</p>		<p>privacy complaints and/or negative publicity. De-identification of personal information before disclosure may not prevent re-identification</p>	<p>assurance that it will protect the information diligently. Review de-identification procedures to ensure that sufficient details are removed so that the recipient of the information will not be able to re-identify an individual, or combine it with other information to establish an individual's identity.</p>
<p>Accuracy and quality: ensuring that the personal data processed is accurate, complete, up to date, adequate and relevant for the purpose of use.</p>	<p>Data captured/collected might not be accurate.</p> <p>Data collected might become redundant due to changed circumstances</p> <p>False information is provided.</p>	<p>Lack of time to check the reliability of the information received.</p> <p>PULSE might have to rely on incomplete information or is unable to verify information.</p> <p>Insufficient resources to verify information.</p>	<p>Decisions based on incomplete, unreliable or false information</p> <p>Negative impact on assistance provided.</p> <p>Poor quality information in the PULSE increases the risk of introducing inaccuracies.</p> <p>Lack of confidence</p>	<p>Ensure a process of quality control to minimise errors or unauthorised modifications.</p> <p>Where possible, cross-check information received.</p> <p>Establish procedures to determine when and how often personal information should be reviewed and/or updated.</p> <p>Establish a procedure to notify recipients</p>

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
			in the reliability and accuracy of the information gathered by other agencies.	of data of subsequent corrections to the data.
Openness, transparency and notice: providing people with clear and easily accessible information regarding PULSE policies, procedures and practices on the collection of information.	<p>Entities may exploit the lack of availability of information about the PULSE system to attack its credibility.</p> <p>Individuals/society may not understand the benefit of the PULSE system.</p>	Strict legal and technical constraints on sharing information.	<p>Reputation damage as a result of PULSE not being sufficiently open with collaborator</p> <p>Other organisations may not share data with PULSE if PULSE does not (at least) reciprocate.</p>	PULSE policies, procedures and practices on the collection of information should be adequately described to end users and the public, in clear and easily accessible manner.
Individual participation and access: giving individuals the right to access and review their personal data, provided their identity is first authenticated	Some individuals may complain about how difficult it is to see and, if necessary, amend (or even delete) their personal data.	PULSE may not have a policy and procedure by means of which individuals can access their personal data.	Reputation damage due to complaints and bad publicity.	<p>It is sometimes (frequently) difficult to get informed consent forms signed off by individuals (victims, families).</p> <p>Mitigating the challenge or propriety or feasibility of getting a signed consent form, the PULSE home page could have a tab that links the individual</p>

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
				with an assurance that PULSE will help individuals in their requests for sight of their data.
Accountability: assigning to a specified individual within PULSE the task of implementing the privacy-related policies, procedures and practices	If no one may has the specific responsibility for safeguarding personal data, PULSE may collect and use personal data without any concerns about consequences of actions.	PULSE may not have assigned accountability to anyone for protection of the data in the PULSE system. Inadequate documentation and communication of data protection policies, procedures and practices relating to PULSE. No assigned responsibility to a specific staff member for data protection.	The credibility risk: everyone shirks their responsibility for adhering to good data protection practices.	Assign a designated person with specific responsibility for ensuring the adequacy of PULSE's policies, procedures and practices with regard to how it collects, uses, safeguards or shares personal data with third parties.
Information security: protecting personal data to ensure its integrity, confidentiality and availability against risks such as unauthorised access, destruction, use, modification,	External hackers and rogue employees may seek to exploit personal data in the PULSE system. Breaches.	Lack of information security practices or strong controls for access to PULSE system. Employees may use weak passwords or may not	Security controls of the PULSE system are breached and personal data is compromised. Lack of awareness	In consultation with stakeholders, identify what additional steps PULSE could take to improve protection of personal information, especially sensitive data.

Ethical/social/legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
disclosure or loss.		encrypt data.	about compromise. Damage to PULSE reputation. Compromised data puts lives at risk.	Robust information security policies. Develop robust access control protocols which limit access on a 'need to know' basis. Ensure clarity re who has the authority to assign, change or revoke access privileges. Ensure all accesses to PULSE are logged.
Privacy compliance: verifying and demonstrating that the processing meets data protection and privacy legislation and/or regulation by periodically conducting audits using internal or trusted third-party auditors.	Despite its humanitarian mission and good intention, PULSE may (unintentionally) violate people's privacy and misuse personal data. PULSE may transfer personal data to third countries without regulatory approval.	PULSE may not comply with privacy legislation. Because of its status, PULSE may not believe that it is or should be subject to data protection regulation, such as the EU's forthcoming Data Protection Regulation. Lack of effective oversight and enforcement	Loss of control over personal data, how it is used, to whom it is transferred. Damage to PULSE's reputation and its credibility. Regulators in Italy, Ireland and/or in the EU insist that the PULSE comply with EU	Seek legal advice to check that PULSE fully complies with (for example) the forthcoming Data Protection Regulation. Document such compliance. Do not store or transfer personal data to a third country without adequate written assurances that the third country (or other organisation) provides or will provide safeguards. Raise user

Ethical/social/ legal principles	Threat	Vulnerability	Risk	Potential mitigation measure
		of transfers of data.	data protection legislation.	awareness about data protection issues.

ANNEX 5: INTERNATIONAL LEGAL FRAMEWORKS FOR PREPAREDNESS PLANNING AND RESPONSE TO PUBLIC HEALTH EMERGENCIES¹¹⁸

International Health Regulations (IHR). WHO 2005.

Article 152 (Public health article) in Title XIII, Public Health European Parliament and Council regulation 851/2004 (ECDC).

European Parliament and Council decision 2119/1998 Network on communicable diseases

Council conclusions 17 December 2001: Informal cooperation and coordination body by Health Ministers and the European Commissioner for Health and Consumer Protection.

Council conclusions 22 February 2007: Transitional prolongation of HSC mandate 2007-09

Council conclusions 16 December 2008 (after informal Health Ministers meeting Angers, 8-9 September 2008). Provide HSC with legal basis; Legislative initiative to adopt the status of HSC to the health challenges.

Commission Decision 57/2000 Early Warning and Response System (EWRS).

Commission Decision 96/2000 list of communicable diseases and special health issues under epidemiological surveillance.

Commission Decision 2002/253 case definitions for reporting communicable diseases

Commission Decision 2004/210/EC on setting up Scientific Committees in the field of consumer safety, public health and the environment

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data

¹¹⁸ European Commission, "Annex 4:", Strategy for Generic Preparedness Planning Technical guidance on generic preparedness planning for public health emergencies, Update April 2011
http://ec.europa.eu/health/preparedness_response/docs/gpp_technical_guidance_document_april2011_en.pdf

Commission Directive 94/3/EC on establishing a procedure for the notification of interception of a consignment or a harmful organism from third countries and presenting an imminent phytosanitary danger

COM (2004)698 on Prevention, preparedness and response to terrorist attacks.

COM(2004) 701 Preparedness and consequence management in the fight against terrorism.

COM (2009) 273 CBRN package – adopted in June 2009.

Horizontal communication on strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union.

EU Action Plan containing specific measures for the individual CBRN strands (bio-preparedness, radiological and nuclear risk reduction, chemical threats) in the areas of prevention, detection and response as well as a set of horizontal actions cutting cross (Annex to the communication).

Staff working document Bridging Security and Health which presents good practices in the cooperation of law enforcement and health authorities on the response to CBRN incidents.

Directive 95/50/EC of 6 October 1995 on uniform procedures for checks on the transport of dangerous goods by road.

Seveso II Directive (96/82/EC) regarding the safety of fixed installation storing higher quantities of dangerous substances; and on the control of major-accident hazards.

Environment Impact Assessment (EIA) Directive (85/337/EEC) and Amended EIA Directive (97/11/EC)

Directive 2001/42/EC on the assessment of the effects of certain plans and programmes on the environment (SEA Directive), OJ L 197, 21.7.2001, p. 30.

Directive 2003/105/EC of the European Parliament and of the Council of 16 December 2003 amending Council Directive 96/82/EC on the control of major-accident hazards involving dangerous substances

Regulation (EC) No 648/2005 (Community Customs Code).

European Community Regulation REACH (Registration, Evaluation, Authorisation and Restriction of Chemical substances) (EC 1907/2006)

Council Decision 2007/162/EC, Euratom establishing a Civil Protection Financial Instrument, OJ L71, 10.3.2007, p. 9.

Council Decision 2007/779/EC, Euratom establishing a Community Civil Protection Mechanism (recast), OJ L 314, 01/12/2007, p.9.

Commission Decision 2008/73/EC, Euratom of 20 December 2007 amending Decision 2004/277/EC, Euratom as regards rules for the implementation of

Council Decision 2007/779/EC, Euratom establishing a Community civil protection mechanism.

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

Directive 2008/68/EC of 24 September 2008 on the inland transport of dangerous goods.

Directive on information to the public 89/618/Euratom Directive on EU Basic Safety Standards 96/29/Euratom Regulation (EC) No 1592/2002 of 15 July 2002 on common rules in the field of civil aviation and establishing a European Aviation Safety Agency.

Regulation (Euratom) No 3954/87 laying down maximum permitted levels of radioactive contamination of foodstuffs and of feeding stuffs following a nuclear accident or any other case of radiological emergency.

Council Decision on early exchange of information 87/600/Euratom

ANNEX 6: UPDATED OVERVIEW OF RELEVANT EU AND INTERNATIONAL CRITICAL INFRASTRUCTURE LEGISLATION AND GUIDELINES

- Regulation (EU) No 283/2014 of the European Parliament and of the Council of 11 March 2014 on guidelines for trans-European networks in the area of telecommunications infrastructure and repealing Decision No 1336/97/EC
- Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA
- Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC
- Decision No 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
- Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection [COM(2006) 786 final – Official Journal C 126 of 7.6.2007].
- Directive 99/5/EC on Radio Equipment, Telecommunications Terminal Equipment and the Mutual Recognition of Their Conformity. Access to control devices and control is a key issue from the viewpoint of the person
- Directive 2001/95/EEC includes the general safety requirements for manufactures and distributors. The manufacturers must put on the market products that comply with the general safety requirement. They must also provide consumers with necessary information
- Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to Electrical Equipment designed for use within certain voltage limits (repealed Low Voltage directive (LVD) 73/23/EEC)
- Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA
- Directive 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC
- Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency
- ENISA, A Good Practice Collection for CERTs on the Directive on attacks against information systems, 2013.
<https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems>

ANNEX 7: PULSE TRIALS LEPPi CHECKLIST

Item	CORK TRIAL	ROME TRIAL
Preparation for the trial exercise – ethical aspects and considerations addressed in trials definition	Complete – April-May 2016.	
Ethical approvals for trials definition – from Ethical Review Committee	Received and actioned in D7.1 and organisation of trials.	
Have Information sheets and Informed Consent forms been issued to, and collected from participants?	yes	yes
Has notice of recordings been given to participants/placed at the venue?	yes	yes
Are the exercise leaders/researchers involved operating within clearly defined constraints to ensure that when sensitive issues are touched upon (such as national security or commercial confidentiality) that neither individuals nor organisations are put at risk?	N/A	N/A
Are the participants aware that the exercise is not a real emergency?	yes	yes
Does the scenario overwhelm the participants in any way?	no	no
Has prior information been given to members of the public in the surrounding areas of the exercise, to ensure that the public do not think it is a real emergency situation?	N/A	N/A
Has safety and well-being of participants been taken care of during the exercise?	yes	yes
Has the exercise leader ensured that the exercise has taken place in accordance with the established processes and protocols (i.e. those set out/outlined in D7.1)?	yes	yes
Has the exercise leader taken on the responsibility for the design, management and reporting of the exercise, and co-ordinating the investigators who take the lead at each site?	yes	yes
Add any other relevant items		

Completed by: David Wright, Trilateral Research Ltd

Date: 1 July 2016 Place: Rome

Date: 15 September 2016, Place: Cork

ANNEX 8: INFORMED CONSENT FORMS – TRIALS

EVD trial Information sheet and consent form



PULSE TRIALS INFORMATION SHEET – TRIAL EXERCISE - Emerging Viral Disease - SARS-like outbreak

We invite you to participate in this trial of PULSE (Platform for European Medical Support during Major Emergencies (PULSE) project, funded by the European Commission. The project aims to develop tools to substantially improve the preparedness and response capabilities of the health services in major emergency situations, to mitigate the loss of life and raise the survival rates among mass casualties. Further details about the project and this trial exercise are available in your invitation letter, and will also be provided to you in the trial exercise briefing. Please read it and the following information carefully and discuss it with others if you wish. Do ask us if there is anything that is not clear or if you would like more information.

This exercise aims to perform an evaluation of the PULSE Toolset. The trial will last one day and a half and will develop through all the WHO pandemic phases, in 7 scenes. Each scene will last 60-90 minutes. At the end of the trial, a two-hour discussion will involve *actors* and *observers* all together, for a summary evaluation of the PULSE support and for evaluating, via a questionnaire about the system performance and socio-political impacts.

Your participation is entirely voluntary. You are entitled to ask questions and receive answers from the PULSE project partners before you make your decision about whether to participate. You are free to withdraw at any time and without giving a reason. In addition to withdrawing yourself from the trial, you may also withdraw any data or information that you might already have provided. In any case, your input and feedback will be handled anonymised. In case you withdraw consent after the information has already been transcribed in the related report, the consortium will ensure an irreversible (link destruction) of the provided input and/or feedback.

You will participate in the trial according to the role assigned to you. Participants will operate in previously assigned roles. While this exercise may be different to what you are used to, we kindly advise you to act in the assigned role and give your feedback for the evaluation independent of your personal preferences, and any possible bias.

If you do decide to take part, please sign the consent form and return it to the project team.



PARTICIPANT INFORMED CONSENT FORM

We thank you for your participation in research conducted for the PULSE project.

The data collected during the trial exercises will be recorded. Any information that might identify you will be removed. Only the research team undertaking the research project will be able to access them. When the information you provide is used for the writing of the report, we will remove your name and all identifying features of that information so that your identity and experiences remain confidential.

The information that we collect from you is considered as non-sensitive personal data under the current European data protection legal framework, i.e., the Data Protection Directive 95/46/EC. Under that Directive, we have obligations to inform you of the purpose of our collection, use, storage and retention of that information you provide to us. We will collect from you information that is relevant to our research, and we inform you that your information will be stored by us on our internal server, and accessible to only those involved in the research process. We will not transfer your personal information to third parties.

Consent terms	Please tick to confirm that you have read and accepted the terms listed.
I confirm that I have read the information sheet explaining the purpose of the research project and I have had the opportunity to ask questions.	
I understand that my participation is voluntary; I am free to withdraw at any time without giving any reason and without any negative consequences. In addition, should I not wish to answer any particular question or questions, or take part in any aspect of the trial exercises, I am free to decline.	
I confirm that I agree to the recording of the research in which I am participating and that any recorded data will only be used for the purpose of the preparation of the report of the trials.	
I understand that any information that I provide will be kept confidential and anonymised for the purpose of the report.	
I agree I may be contacted by the PULSE project consortium in the event of its requiring further information as a follow-up to the initial research.	
I agree that any information I provide can be used in the report of the trial produced by the PULSE consortium.	

By signing this form, you consent to this collection of information (including personal data) from you so that we may meet our commitments for the research project and its associated reports. You also acknowledge that you are aware of the reasons for our collection, the manner in which the information you provide will be used, processed and stored. You acknowledge that you are aware of who to contact in order to ask questions about the research process and/or assert your rights under the Data Protection Directive. If you have any further questions, concerns or complaints, please contact the PULSE project co-ordinator, Sarah Bourke: sarah.bourke@skytek.com or tel.: +353 6787660.

Name (please print):

Signed:

Date:



Photograph & Video Release Form

I hereby grant permission to the rights of my image, likeness and sound of my voice as recorded on audio or video tape without payment or any other consideration. I understand that my image may be edited, copied, exhibited, published or distributed and waive the right to inspect or approve the finished product wherein my likeness appears. Additionally, I waive any right to royalties or other compensation arising or related to the use of my image or recording. I also understand that this material may be used in diverse educational settings within an unrestricted geographic area.

Photographic, audio or video recordings may be used for the following purposes:

- Conference presentations, educational presentations or courses
- Project informational presentations
- Online educational courses
- Educational videos

By signing this release, I understand this permission signifies that photographic or video recordings of me may be electronically displayed via the Internet or in a public educational setting.

I will be consulted about the use of the photographs or video recording for any purpose other than those listed above.

There is no time limit on the validity of this release nor is there any geographic limitation on where these materials may be distributed.

This release applies to photographic, audio or video recordings collected as part of the trial exercise.

By signing this form, I acknowledge that I have completely read and fully understand the above release and agree to be bound thereby. I hereby release any and all claims against any person or organization utilizing this material for educational purposes.

Full Name _____

Address/P.O. Box _____

City _____

Postal Code _____

Phone _____ Fax _____

Email Address _____

Signature _____ Date _____

If this release is obtained from a presenter under the age of 18, then the signature of the participant's parent or legal guardian is also required.

Parent's Signature _____ Date _____

MCI trial Information sheet and consent form



PULSE TRIALS INFORMATION SHEET – Trial Exercise: Mass Casualty Incident (MCI) – crowd crush in a stadium

We invite you to participate in this trial of PULSE (Platform for European Medical Support during Major Emergencies (PULSE) project, funded by the European Commission. The project aims to develop tools to substantially improve the preparedness and response capabilities of the health services in major emergency situations, to mitigate the loss of life and raise the survival rates among mass casualties. Further details about the project and the trial exercise are available in your Exercise Pack, and will be provided to you in the trial exercise briefing. Please read it and the following information carefully and discuss it with others if you wish. Do ask us if there is anything that is not clear, or if you would like more information.

This trial exercise aims to perform an evaluation of the PULSE Toolset and meet the training objectives of participants' organizations in relation to Interagency MCI preparation. The exercise will last one day. The trial details are set out in the on-line multimedia instructional and informational inject, which explains the nature of the PULSE Project, describes the PULSE platform and the MCI "crowd crush" scenario, and sets out the timetable for the exercise, the nature and mechanism of the validation and the methods that will be used to gather their feed-back by way of on-line or paper based targeted questionnaires.

Your participation is entirely voluntary. You are entitled to ask questions and receive answers from the PULSE project partners before you make your decision about whether to participate. You are free to withdraw at any time and without giving a reason. In addition to withdrawing yourself from the trial, you may also withdraw any data or information that you might already have provided or any images of you that might have been video recorded.

In any case, your input and feedback will be anonymised. In case you withdraw consent after the information has already been transcribed in the related report, the consortium will ensure an irreversible (link destruction) of the provided input and/or feedback.

You will participate in the trial according to the role assigned to you. While this exercise may be different to what you are used to, we kindly advise you to act per your assigned role and give your feedback for the evaluation independent of your personal preferences, and any possible bias.

If you do decide to take part, please sign the consent form and return it to the project team.

PARTICIPANT INFORMED CONSENT FORM

We thank you for your participation in the PULSE MCI trial exercise.

The data collected during the trial exercise will be recorded. Any information that might identify you will be removed. Only the research team undertaking the research project will be able to access them. When the information you provide is used for the writing of the report, we will remove your name and all identifying features of that information so that your identity and experiences remain confidential.

The information that we collect from you is considered as non-sensitive personal data under the current European data protection legal framework, i.e., the Data Protection Directive 95/46/EC. Under the Directive, we have obligations to inform you of the purpose of our collection, use, storage and retention of that information you provide to us. We will only collect information that is relevant to our research. Personal information will be stored by us on our internal server, and accessible to only those involved in the research process. We will not transfer your personal information to third parties.

Consent terms	Please tick to confirm that you have read and accepted the terms listed
I confirm that I have read the information sheet explaining the purpose of the research project and I have had the opportunity to ask questions.	
I understand that my participation is voluntary; I am free to withdraw at any time without giving any reason and without any negative consequences. In addition, should I not wish to answer any particular question or questions, or take part in any aspect of the trial exercises, I am free to decline.	
I confirm that I agree to the recording of the research in which I am participating and that any recorded data will only be used for the purpose of the preparation of the report of the trials.	
I understand that any information that I provide will be kept confidential and anonymised for the purpose of the report.	
I agree I may be contacted by the PULSE project consortium in the event of its requiring further information as a follow-up to the initial research.	
I agree that any information I provide can be used in the report of the trial produced by the PULSE consortium.	

By signing this form, you consent to this collection of information (including personal data) from you so that we may meet our commitments for the research project and its associated reports. You also acknowledge that you are aware of the reasons for our collection, the manner in which the information you provide will be used, processed and stored. You acknowledge that you are aware of who to contact in order to ask questions about the research process and/or assert your rights under the Data Protection Directive. The data controller for PULSE is Skytek Ltd. (69 Fitzwilliam Lane, Dublin 2 Ireland). If you have any further questions, concerns or complaints, or do not wish to be contacted in the future by the PULSE consortium, please contact the PULSE project co-ordinator, Sarah Bourke: sarah.bourke@skytek.com or tel.: +353 1 678 7660.

Name (please print):

Signature:

Date:



Photograph & Video Release Form

I hereby grant permission to the rights of my image, likeness and sound of my voice as recorded on audio or video tape without payment or any other consideration. I understand that my image may be edited, copied, exhibited, published or distributed and waive the right to inspect or approve the finished product wherein my likeness appears. Additionally, I waive any right to royalties or other compensation arising or related to the use of my image or recording. I also understand that this material may be used in diverse educational settings within an unrestricted geographic area.

Photographic, audio or video recordings may be used for the following purposes:

- Conference presentations, educational presentations or courses
- Project informational presentations
- Online educational courses
- Educational videos

By signing this release, I understand this permission signifies that photographic or video recordings of me may be electronically displayed via the Internet or in a public educational setting.

I will be consulted about the use of the photographs or video recording for any purpose other than those listed above.

There is no time limit on the validity of this release nor is there any geographic limitation on where these materials may be distributed.

This release applies to photographic, audio or video recordings collected as part of the trial exercise.

By signing this form, I acknowledge that I have completely read and fully understand the above release and agree to be bound thereby. I hereby release any and all claims against any person or organization utilizing this material for educational purposes.

Full Name _____

Address/P.O. Box _____

City _____

Postal Code _____

Phone _____ Fax _____

Email Address _____

Signature _____ Date _____

If this release is obtained from a presenter under the age of 18, then the signature of the participant's parent or legal guardian is also required.

Parent's Signature _____ Date _____

ANNEX 9: SCENARIO CHARACTERISTICS

Characteristics	Scenario 1): SARS Incident	Scenario 2): Stadium Crush
Likelihood	Between likely and unlikely	Likely
Impact	Very serious to catastrophic	Very serious
Total risk class	Major emergency	Major emergency
Affected area	From local up to international	Regional/national/possibly limited international
Escalation time profile	Developing over days / weeks	Occurring quickly
Alerting of the public	Gradually progressing	No pre-alerting possible
Alerting/ instructing responder services	Long preparation & pre-alerting phase	Immediately; through emergency dispatching centres
Importance of international coordination	Very extensive	Only if event is located close to a border and/or if support is required for longer term care
Type of international coordination/ collaboration	Sharing of the <ul style="list-style-type: none"> • Identification of source of agent • Scientific investigation of the agent type • Investigation of infection route(s) • Hospital resources • Special treatment • Resources such as medications (Vaccines; antibiotics) • Sharing/mutual support in transportation of patients 	Coordination of: <ul style="list-style-type: none"> Search and Rescue-Teams; Equipment, and Know How; Logistic support for Transfer, distribution, allocation of very seriously injured persons
Political relevance	High; on local/national government to international level	Low to medium
Societal public perception	Very high	Limited
Societal reactions	Very intensive, depending on spread and seriousness of infections	Locally limited concerns

Characteristics	Scenario 1): SARS Incident	Scenario 2): Stadium Crush
Societal consequences/ impact on social order, peace	May escalate to panicking; undue withholding of medication; hoarding; looting;	Limited
Ethical and psychological implications	Broad; may cause deep doubts and mistrust against public admin. and healthcare system	Limited; psychological treatment of relatives
Economic impact	May be very serious (loss of working force, ...)	Locally limited
Environmental impact	Possible impact on local, regional animal populations (if susceptible to the disease)	None to minor
Impact on vital infrastructures	On hospitals and ambulance services Collapse of health care sector due to loss of work force on the one side and high numbers of patients in need of intensive care. Possible collapse of supply chains due to loss of work force	Local stadium and possibly some surrounding infrastructure
Priority requirements: Preparedness	Medication stocks Early warning indication system Capacity planning of... Quality of diagnosis Hospital surge capability Communication strategies International coordination regulations	Resilience of stadium and site infrastructure Quality of first responders Real-time indicator monitoring Adaptive response capability Crowd Event Planning and Guidance
Priority requirements: Response	Alerting of ... Forecasting of development and spreading Public communication Inter-services and international cooperation Monitoring of criminal escalations	Very short-term decision making On-site communication Monitoring of critical spots and events Pre-hospital care capability Fast reinforcement of security staff

ANNEX 10: INTERNAL ETHICAL RISK ASSESSMENT OF PULSE TOOLS

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
DSVT	Unauthorised access to the PULSE system	Inadequate security measures	Data breaches resulting in information security and privacy issues	Low	Serious	A dedicated tool called the Authentication Server handles the security aspects of the PULSE platform. This tool provides a layer of protection that forces users and clients to authenticate through the server prior to, for example, accessing the network, or invoking the web service interfaces exposed by the PULSE tools. This component is based on the well-known open authentication protocol OAuth2 that provides different security mechanisms.
DSVT	Ineffective or erroneous decision making e.g. unfair resources allocation choices	Automatic creation of personalised suggestions to decision makers in charge of the crisis management	Human suffering Loss of life Amplification of effects of the crisis Legal prosecution and adverse impacts on the crisis managers (both individuals and organisations)	Medium	Serious	The decision-maker has the moral and ethical responsibility for all decisions that will be taken. The PULSE platform is a Decision Support System that will provide support to the decision makers, however it will not take decision in their place.

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
DSVT	Untrustworthiness of sources of information and networks (lack of integrity of the data)	Analysing and classifying news articles from specialised official and unofficial medical sites, blogs, online newspapers and clinical records. (failure of weak signals classification)	Adverse impact on decision- makers abilities to find the most-efficient way to handle emergencies Threat to positive outcome of the crisis.	Low	Negligible	Sources of information have been validated by experts in the emergency coordination field. Some of the resources can be decided and selected by the decision-maker themselves (although this needs to consider ethical responsibility and awareness).
DSVT	Information is made available and/or disclosed to unauthorised persons, entities, or processes; and/or the unavailability of timely, accurate information about patients, resources, and environmental conditions; malfunction of the DSVT tool	Failure of DSVT functionalities, i.e. to correctly estimate the number of resources on the field, e.g. number of ambulances, first responders etc. necessary to manage an event (e.g. a big concert in a stadium) and to efficiently respond in case	Ineffective coordination and management of health-related emergency events	Low	Intermittent	The DSVT is just a support to decision-makers, therefore in case of failure, the person in charge of the emergency coordination can still take decisions according to the available field information and according to his/her experience.

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
		of an incident.				
DSVT	The credibility of the DSVT decision-making process is undermined due to a lack of transparency.	Process and/or steps followed by DSVT are not transparent	Loss of reputation of the PULSE system	Low	Negligible	The DSVT can provide a complete trace log of all the steps that have been followed to simulate the crisis. This information can be useful to the PULSE users to understand the quality of the simulation and to follow the suggested steps.
DSVT	Not taking the principles of beneficence and non-maleficence into account during the design of the tool	Reduction of complexity, or minimising the effects of cognitive biases, or other negative influences, in the decision-making process.	Adverse impacts on the autonomy of the system user as a decision maker.	Low	Negligible	The PULSE platform is intended as a decision support system without affecting the autonomy of the decision-makers, who still have the right to refuse or choose different solutions.
DSVT	The DSVT cannot	Lack of	Ineffective delivery	Medium	Intermittent	The PULSE platform has been

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
	communicate and/or work with other health systems across organisational boundaries	interoperability	of healthcare for individuals and communities			developed with up-to-date standards (e.g., REST, JSON) that ease the integration with external heterogeneous systems. Adapter can be developed for integration with health infrastructure legacy.
IAT	Collection and analysis of clinical data by PULSE IAT tool	Lack of pre-defined policy on collection and analysis of clinical data. This may increase the risk of re-purposing and further use of the data	Adverse impact on the relationship between patients as a group and organisations involved (such as clinical teams, hospitals) Data security risks	Medium	Intermittent	Participating hospitals to ensure patients are informed about, and have consented to, such use of their clinical data Data collection will be logged and justified
IAT	Collection, filtering and analysis of geo-localised tweet messages generated from the Twitter platform	Lack of consent for the collection, filtering and analysis. Unreliability and non-validation of the information derived from Twitter Tracking physical	Violation of privacy and data protection law. Breach of confidentiality Risk of mis-assessing the situation Psychological and	Low	Negligible	The likelihood is viewed as low and the impact viewed as negligible, as a twitter message can only contain GPS coordinates if the person sending the message explicitly provides consent to send his/her actual position GPS coordinates. PULSE will use only publicly shared data

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
		location of Twitter users	other unforeseen harms			<p>Twitter has its own privacy and security settings</p> <p>PULSE will specify use and define how the tool will treat such data in the SOPs and/or data protection policy targeted at the end users and the public</p> <p>Appropriate storage and security of the data.</p> <p>Data minimisation</p>
IAT	Co-relating gathered data (i.e. clinical records, geo-localised tweets and information from websites)	Data linkage	<p>Risk of privacy loss due to linking data from different sources</p> <p>Profiling</p>	Low	Negligible	Will only be conducted as necessary and lawfully authorised
LT	Storage of the information available regarding the status of crisis resources and real-time retrieval of data	Inadequate security for the stored information	<p>Denial of service attacks</p> <p>Data breaches</p>	Medium	Intermittent	<p>The Logistic Manager's RESTful interface is secured with the OAuth2 security protocol that allows only authorised clients to access the tool's functionalities. Moreover, the Logistic Tool is able to encipher the information stored into its internal repository depending on the specific data security policy of the monitored</p>

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
						resources.
LT	Critical and widespread cases of life threatening conditions; lack of treatment for some patients	Inability to co-ordinate and address multiple crises at once, and non-optimal dispatch of the casualties to the available hospitals	Discrimination Human suffering Death Loss of trust	Medium	Intermittent	The tool considers the actual resources present in the different hospitals and exploits the models defined in WP3 for assessing the required stockpiles of any necessary equipment, medications and vaccinations. The tool is then able to calculate and suggest the optimal dispatch of the casualties to the available surrounding hospitals. The optimisation algorithm is based on the fairness usage of the hospitals' resources and the minimisation of the time necessary to send the casualties to the hospitals.
LT	Surveillance of responders and victims	Tool tracks ambulances, persons, hospitals, Resources (e.g. equipment, medications and vaccinations), rescuers, and tasks	Non-compliance in relation to data protection legislation	Low	Negligible	Actions will be only as necessary and in conformity to EU and national laws.

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
LT	Disclosure of personal information to other entities and/or people without proper authorisation	Tool collects information on ambulances, persons (i.e. symptoms, health condition, required resources to be cured, GPS coordinates, full name (if available), rescuers (GPS coordinates, full name, qualification, set of medical resources at disposal, tasks), hospitals, resources and tasks.	Improper treatment of personal data	Low	Intermittent	Data will be collected only for authorised purposes and kept only for the time necessary. The Logistic Manager's RESTful interface is secured with the OAuth2 security protocol that allows only authorised clients to access the tool's data.
SCGT	Underestimation of the amount of resources (depending on the specified number of people) that can be made available	Human data inputs	Impact on the freedom, health and, in some cases, survival prospects of individuals	Low	Negligible	Efforts made to avoid and/or reduce collateral damage that may result from decisions about resource allocation (e.g., denial of surgery and/or treatment for critically or terminally ill patients).

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
	within the prediction interval.					The possibility of collateral damage is highly limited. The SCGT is used only during the simulation of the possible outcome of the emergency situation. Furthermore, the simulation itself is just a one of the Decision Support functionalities provided by the PULSE platform.
SCGT	Lack of integrity and quality of the processes underlying the tool.	Basis of tool processes not clear.	Decisions based on prohibited grounds	Medium	Intermittent	Align with the ethical framework and existing surge management and triage processes.
SCGT	Failure of the surge capacity tool to respond to client request	Internet connection is required for the client to gain access to the model web services and the correct retrieval of the results. In the absence of Internet connectivity, the	Failure of the system	Medium	Intermittent	The SCGT is invoked during the simulation process. In absence of Internet connectivity, the simulation process will be performed even without the invocation of the SCGT (but with less accurate results).

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
		client reports that the results are not available.				
SCGT	Infringement of intellectual property rights	Use of third party libraries and/or frameworks	Violation of intellectual property rights	Low	Negligible	A list of third party libraries/frameworks has been acknowledged and those used are: PHP License 3.01, Apache 2.0, Oracle Binary Code License Agreement, GNU Lesser General Public License. GNU General Public License (GNU GPL or GPL) are widely used free software licenses, which guarantee users freedoms to run, study, share (copy), and modify the software.
Training tools	Collection and recording of data (without the users being aware)	Automatic gathering of interactive examination results from trainees	Judgement about user competency	Low	Negligible	Trainees will be made aware of automated monitoring via the LMS/LRS system and the uses of such data. Obtain informed consent of users. PULSE will only monitor trends in order to mitigate the collection of unnecessary

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
						personal information.
Training tools	Ignorance of game feedback	Inadequate and/or failure of communication with trainees	Unethical and unprofessional actions by trainees, resulting in compromises in patient safety	Low	Intermittent	<p>In order to start an MPORG training session, one user must have a login account with the main Pulse server in order to fetch a game scenario. This user then assumes a leader role and it is their responsibility to communicate the details effectively and explain the feedback, whether face to face, or via the provided chat window. A user manual is also made available for all users if additional information is required.</p> <p>Within the technical remit of the apps, the details are provided in as much detail as possible. However, responsibility also falls on the users themselves to read and make use of this information.</p>
Training tools	Failure to address differing cultural competencies of users	Differing cultural competencies have not been taken into account (training	Influences on game behaviour might not be understood, which may impact on	Low	Intermittent.	Although unlikely, if there are innate biases discovered these would need to be assessed for impact as they arise. App development was kept minimal

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
		tools use other tools as basis)	people's ability to provide consent, and so on.			and functional with no concessions to any cultural influences. However, they are developed in English and from an implicitly European perspective, so there may be an innate bias that has not been discovered to date.
Training tools	Training tools not adaptable to different healthcare settings	The MPORG is only for the stadium-crush like scenario. There will be training materials available for the SARS trial.	Lack of flexibility, reusability	Low	Negligible	The tools are adaptable for different types of location based emergency scenarios. Scenario details, locations, types of events, etc., could all be adjusted for a variety of training settings.
Training tools	Static nature of the training tools	Lack of adaptability of the MPORG to different healthcare and cultural settings	Irrelevance and future redundancies of the training tools	Low	Negligible	Feedback on the quality of end users opinions of the training activities will be performed through the use of a Learning Questionnaire (LQ). As noted in the previous two items, the MPORG engine is kept direct & functional, allowing for flexibility in content and scenarios. Adapting that content to differing settings is straightforward. Adapting the engine itself to go

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
						beyond location-based emergencies is a conceptual change that is beyond the scope of the project.
Training tools	Infringement of intellectual property rights	Use of third party libraries and/or frameworks	Violation of intellectual property rights	Low	Negligible	A list of third party libraries and/or frameworks has been acknowledged. Those used are under GNU General Public License (GNU GPL or GPL) - widely used free software license, which guarantees end users (individuals, organisations, companies) the freedom to run, study, share (copy), and modify the software.
PCET	Capture of irrelevant historical information	Functionalities to store historical information and retrieve that information through the elaboration of ad hoc correlations, analytics and statistics	Ineffectiveness of the PCET tool	Low	Negligible	PCET is able to capture and manage several historical data describing the evolution of current and past emergencies, such as: <ul style="list-style-type: none"> • the decisions taken during the crisis; • the resources employed in terms of (i) people who intervened to help (e.g. doctors and nurses) and (ii) allocated medical assets (e.g., hospitals, ambulances, surgical masks,

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
						sterile gauzes); <ul style="list-style-type: none"> • persons who have been injured, infected or recovered, and persons who died during the crisis; • information on whether conditions; • information on traffic conditions; • weak signals related to possible epidemic issues; • communications from WHO.
PCET	Infringement of intellectual property rights	Use of third party libraries and/or frameworks	Violation of intellectual property rights	Low	Negligible	A list of third party libraries/frameworks has been acknowledge; their licenses e.g. Apache 2.0, Dual License: - CDDL 1.1 and - GNU GPL 2, Copyright 2002 JSON.org are all open source and royalty free.
ENSIR	User errors	Human user inputs and/or involvement	Erroneous results	Medium	Intermittent	Confirmation is requested from the user before the start of the ENSIR simulation
ENSIR	Unnecessary processing of data	Processing of data beyond the necessary scope.	Detrimental effect on privacy	Low	Negligible	The ENSIR tool doesn't process privacy and personal data but just a set of information related to the territory and the population (e.g. population density, transportations)

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
ENSIR	Inaccuracies, inefficiencies	Complexity of the tools underlying interaction and limited parameters of the tool	Risk to health and safety of people	Low	Negligible	Parameter tuning and implementation refinements (based on the processes of integration and validation and/or trials in WP6-WP7) will provide a further opportunity for tuning the model/tool parameters. Furthermore, the lessons learnt from the procedures from the WP5 deliverables and of the application of the PULSE platform in realistic conditions for the considered scenario will provide opportunities for refinement of the model/tool.
ENSIR	Infringement of intellectual property rights	Use of third party libraries and/or frameworks	Violation of intellectual property rights	Low	Negligible	A list of third party libraries/frameworks has been acknowledged and these are as follows: PHP License 3.01; Apache 2.0; Oracle Binary Code License Agreement; GNU LESSER GENERAL PUBLIC LICENSE
Mobile App	Collection and storage of large quantities of and unnecessary data	No restriction or policies on collection and storage of data	Violation of data protection principles, resulting in privacy	Low	Negligible	Minimising the collection of data required to make the app run Only minimal user information is

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
	from the device		infringements			<p>required for the public app. PULSE is only concerned with data public users are reporting and if the source has been reliable in the past</p> <p>Any PID is given voluntarily, sandboxed on the device, encrypted in transmission, and stored on the server with similar privacy & security policies in place</p>
Mobile App	The app may want to access, process and gain more value from personal data	No specification of purpose(s) for which data will further processed	<p>Non-compliance with legal obligations</p> <p>Damage to reputation</p> <p>Security breach</p>	Low	Negligible	<p>App privacy, and data protection (including valid consent) policies in place, followed and audited</p> <p>Specification and documentation of the purposes for which data will be collected</p> <p>Anonymisation and de-identification for data that might be re-purposed</p>
Mobile App	Unlimited retention of data	Gaps in policies on data retention	<p>Non-compliance with legal obligations</p> <p>Damage to reputation</p>	Low	Negligible	On the mobile device, data is only stored temporarily (cached) until it has been successfully saved on the server. Once saved, the record is deleted from the device.

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
			Security breach			There is no long-term storage of recorded data on the device.
Mobile App	Unauthorised access	Gap in access policies	Data security compromises Data breaches Data loss	Low	Negligible	App users must be registered in the system to gain access. They will log in using the OAuth system on the server, which will authorise that user to have full access to the app. Each of the user's reports to the server will be signed as having come from that user. Without valid log-in credentials, the user will not be able to load the main screens on the app, and will not be able to connect to the server to save data. If a user somehow gains unauthorised access, each record from that user would still be signed with a unique identifier from that user session, allowing for easy identification & removal of corrupt/unauthorised data, enabling the incident to be reversed once discovered.
Mobile App	Onsite data capture and/or recording inaccuracies and redundancies	Lack of rules and/or time to check the reliability of the	Harmful, erroneous decision- making	Low	Negligible	Data from the public web forms is known to be from an untrusted, public source and as such will be assessed based on

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
		information	Negative impact on assistance provided			<p>the content after review</p> <p>For the mobile app, all records are tagged with user ID, timestamp & geo-location details, in order that: duplicate records can be easily spotted & removed; any user supplying spurious or inaccurate data can be removed or blocked.</p> <p>With the use of QR Code bracelets or similar, a unique identifier is given to the casualty and scanned into the system as part of their unique record</p>
Mobile App	Mobile app data interception, iPhone or Android jailbreaks, user impersonation	<p>Data breaches</p> <p>Unsafe data storage</p> <p>Unsafe data transmission</p>	<p>Loss of control over personal data</p> <p>Sensitive data leakage</p> <p>Damage to credibility and reputation of PULSE</p>	Low	Negligible	<p>Data security measures in app design and development</p> <p>Adequate safeguards embedded E.g. sandboxing features of app, use of HTTPS</p> <p>User needs access to their device and to have a login account on the PULSE server to save data.</p> <p>If a device is lost or stolen, an unauthorised user may be able</p>

Tool	Threat	Vulnerability	Risk	Likelihood of risk (high, medium, low)	Potential impact (catastrophic, serious, intermittent, negligible)	Proposed mitigation measure(s)
						to launch the app but cannot interact with the PULSE server Only temporary holding of data and encryption means that even if the device is jail-broken and the unauthorised user can gain full access, there would be no readable records stored in the device
Mobile App	Tracking and potentially unauthorised use of geo-location data	Lack of defined policies on tracking and use of geo-location data	Non-compliance with data protection legislation, leading to unauthorised tracking and surveillance	Low	Negligible	Use of geo-location data only as necessary and authorised by law. PULSE app will only track the device, not the user, and so no personally identifiable data (PID) is strictly required from the public user Permission to use geo-location is explicitly asked of the user. Location details are saved with casualty records (as expected) and to report the current location of the user and/or device while active during the emergency, to aid in the planning.

ANNEX 11: EXTERNAL RISK ASSESSMENT OF PULSE TOOLS – DATA

RISK	LIKELIHOOD			Risk	POTENTIAL IMPACT				Depends on structure, implementation
	HIGH	MEDIUM	LOW		CATASTROPHIC	SERIOUS	INTERMITTENT	NEGLIGIBLE	
Information confidentiality and system security risks	4	3		Information confidentiality and system security risks	1	3	2	1	
Human suffering, amplification of crisis effects/ Risk to health and safety of people		1	6	Human suffering, amplification of crisis effects/ Risk to health and safety of people	1	1	1	3	
Adverse impact on decision makers abilities to, when needed, find the “most-efficient” way to handle emergencies.		2	3	Adverse impact on decision makers abilities to, when needed, find the “most-efficient” way to handle emergencies.	1	1	1	2	1
Risk of mis-assessing the crisis/emergency	1	1	3	Risk of mis-assessing the crisis/emergency	1	2	1	1	1
Ineffective coordination and management of the health emergency events	1	1	4	Ineffective coordination and management of the health emergency events	1	3	1	1	
Ineffective delivery of healthcare for individuals and communities		2	4	Ineffective delivery of healthcare for individuals and communities	1	3	1	1	1
Risk to privacy and personal data	2	3	1	Risk to privacy and personal data		3	2	1	1
Violation of intellectual property rights	1		5	Violation of intellectual property rights			2	4	
Adverse impact on relationship between patients (as a group) and organisations involved (such as clinical teams, hospitals)		1	6	Adverse impact on relationship between patients (as a group) and organisations involved (such as clinical teams, hospitals)		4	1	2	
Surveillance via profiling and geotagging	3	3	1	Surveillance via profiling and geotagging		3	4		
Psychological and other unforeseen harms		2	5	Psychological and other unforeseen harms		1	5	1	
Discrimination in relation to treatment of patients			7	Discrimination in relation to treatment of patients	1	1	2	3	
Irrelevance and future redundancies of the PULSE training tools		4	2	Irrelevance and future redundancies of the PULSE training tools		2	2	2	
Unethical and unprofessional actions by trainees		2	4	Unethical and unprofessional actions by trainees		2	2	2	
Harm to vulnerable groups/individuals (due to e.g. inability to provide informed consent)		4	3	Harm to vulnerable groups/individuals (due to e.g. inability to provide informed consent)		2	2	3	

ANNEX 12: DATA PROTECTION GUIDANCE CHECKLIST

This checklist, adapted for use by projects such as PULSE is based on Annex three of the *ICO Guidance Linking the PIA to the data protection principles*.¹¹⁹

- Have you identified the purpose of the project?
- How will individuals be told about the use of their personal data?
- Do you need to amend privacy notices?
- Have you established which conditions for processing apply?
- If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
- If your organisation is subject to human rights legislation, you also need to consider:
 - Will your actions interfere with the rights enshrined in the EU Charter of Fundamental Rights (e.g. Article 3 – Right to the integrity of the person which includes both physical and mental integrity; Article 7 – Respect for private and family life; and Article 8 – Protection of Personal Data), the *European Convention on Human Rights* especially Article 8 (Right to Respect for Private and Family Life) and national human rights legislation (as applicable)?
- Have you identified the social need and aims of the project? Are your actions a proportionate response to the social need?
- Does your project plan cover all the purposes for processing personal data?
- Have potential new purposes been identified as the scope of the project expands?
- Is the information you are using of adequate quality for its specified purposes?
- Which personal data could you not use without compromising the needs of the project?
- If you are procuring new software, does it allow you to amend data when necessary? How are you ensuring that personal data obtained from individuals or other organisations is accurate?
- What retention periods are suitable for the personal data you will be processing?
- Are you procuring software which will allow you to delete information in line with your retention periods?
- Will the systems you are putting in place allow you to respond to subject access requests more easily?
- If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
- Do any new systems provide protection against the security risks you have identified?
- What training and instructions are necessary to ensure that staff know how to operate a new system securely?
- Will the project require you to transfer data outside of the EEA? If you will be making transfers, how will you ensure that the data is adequately protected?

¹¹⁹ <https://ico.org.uk/media/1042836/pia-code-of-practice-editable-annexes.docx>

ANNEX 13: EELPS QUESTIONNAIRE

Name (optional):	
You are (please mark with a cross):	Actor (active participant):
	Observer:
	Member of the PULSE Consortium:
Your type of organisation (please mark with a cross): HC: Health Care EM: Emergency Management PH: Public Health	HC & EM Worldwide:
	HC & EM European:
	HC & EM National (Ministry):
	HC & EM National (other):
	PH & EM Regional:
	PH & EM Local:
	Specialised Hospitals:
	General Hospitals:
	University:
	Other (please specify):

	EELPS Aspects	Strongly disagree	Disagree	Neither disagree nor agree	Agree	Strongly agree
1	Ethical					
1a	Will PULSE change societal ethical values in a negative way?					
1b	Is PULSE open and transparent in terms of how it handles health-related information?					
1c	Is PULSE open and transparent in terms of system functionality?					
1d	Will PULSE help channel medical resources appropriately in a public health emergency?					
2	Economic					
2a	Will PULSE contribute to, or influence economic stability in any way?					
2b	Will PULSE create market advantages for its suppliers, developers and operators?					
3	Legal					
3a	Does PULSE comply with existing regulations and the rule of law?					
3b	Is the measure compatible with human rights principles and the core values such human dignity,					

	freedom, equality and solidarity?					
3c	Do you think the PULSE system creates any data protection risks? ¹²⁰					
4	Political					
4a	Does PULSE fit into related international and EU health strategies?					
4b	Does PULSE fit into related national health strategies?					
4c	Does PULSE have the potential to create political risks?					
5	Societal					
5a	Does PULSE have the potential to increase control over people and/or society?					
5b	Will PULSE bring direct benefits to people and/or society?					

Summary assessment, recommendations, remarks:

¹²⁰ Added after discussions in Rome, to the Cork trial EELPS assessment.

GLOSSARY

Terms	Definitions	Notes
Critical infrastructure (CI)	An asset or system which is essential for the maintenance of vital societal functions	
Ethical Assessment Impact	An EIA is a process during which an organisation – or project consortium, as in the case of PULSE – together with stakeholders (and, in particular, end-users) considers the ethical issues or impacts posed by a new project, technology, service, programme, legislation, or other initiative, to identify risks and solutions.	
Ethical issues	Ethical issues refer to the issues concerning some aspect that raise ethical questions	
Ethics	Ethics is the systematic reflection on right and wrong conduct according to norms and values to which we think we should adhere	
EMS	Emergency Medical Service	
ICT	Information and Communication Technology	
Legislation	A law or a body of laws enacted	e.g. The Charter of Fundamental Rights
Personal data	‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular	Article 4(1), General Data Protection Regulation.

Terms	Definitions	Notes
	by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person	
Phase	A subset of a Scenario. It may be, for instance, identified, in terms of time (e.g., before the incident) and/or location (e.g. hospital) and/or type of population involved (e.g. people in "uncertain" status in a SARS-like epidemic) and/or purpose (prepare, recover)	Each PULSE Scenario is split into two Phases: Preparedness and Response.
Platform	See PULSE Platform	
Policy	Document that provides high-level guidelines, in terms of actors and responsibilities	The "Decision No. 1082/2013/EU of European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health" is an example of policy
Preparedness phase	Activities that prepare and train responders and ensure that the required mix of resources are ready to respond in case of adverse events	
Procedure	A document describing a series of actions that, in the end, produce an output; a procedure normally specifies the flow diagram (logic and time sequence of the actions), the actors (who does the action) and the software tools used to carry out the action	Classification rule for separating people "assaulting" a hospital

Terms	Definitions	Notes
PULSE	Platform for European Medical Support during major emergencies	
PULSE End-user	Any actor that is expected to interact with the PULSE Platform. Interaction with the Tools may consist of: providing input, launching simulations, elaborations, receiving input	
PULSE Platform	PULSE System + PULSE SOP	
PULSE Project	The Project that will specify, design, implement and validate the PULSE platform.	
Response phase	Activities that are triggered by the adverse event, with the purpose to diminish/contain its effects	
Requirements	Justified characteristic needs, formulated by users and experts. For IT systems, usually one distinguishes between technical and operational (possibly strategic) requirements	
SARS	Severe Acute Respiratory Syndrome	
Stakeholder	A person or group that has a stake or interest in something	
System	Collection of interrelated components	
Tool	Any helping software instrument, including input/output interfaces with users or other Tools or Systems (mostly software). A Tool may use Modules. A software Tool may also be identified with the set of functionalities	

REFERENCES

1. Borri, Alessandro, Andrea De Gaetano, Francesco Malmignati, *PULSE Deliverable D4.7 - Event evaluation for biological event*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_7_Event_Evaluation_for_Biological_Events.pdf
2. Borri, Alessandro, Andrea De Gaetano, Sabina Magalini, Francesco Malmignati, *PULSE Deliverable D4.4 - Surge Capacity Tool*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_4_Surge_Capacity_Tool.pdf
3. Brey, P., "Ethical Aspects of Information Security and Privacy", in M. Petković and W. Jonker (eds.), *Security, Privacy, and Trust in Modern Data Management*, Springer Berlin, Heidelberg, 2007, pp. 21-36.
4. Carty, Shane, Karl Chadwick, Paul Kiernan, *PULSE Deliverable D4.5- Training Tools*, 20 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_5_Training_Tools.pdf
5. Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, Rome, 4.XI.1950. http://www.echr.coe.int/Documents/Convention_ENG.pdf
6. European Commission Migration and Home Affairs, Critical Infrastructure. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
7. European Commission, "Annex 4:", Strategy for Generic Preparedness Planning Technical guidance on generic preparedness planning for public health emergencies, Update April 2011 http://ec.europa.eu/health/preparedness_response/docs/gpp_technical_guidance_document_april2011_en.pdf
8. European Commission, *Ethics for researchers Facilitating Research Excellence in FP7*, Publications Office of the European Union, Luxembourg, 2013. http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf
9. European Commission, "EU Civil Protection Legislation ECHO Factsheet", 2014. http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_legislation_en.pdf
10. European Commission, "EU Civil Protection Mechanism". <http://ec.europa.eu/echo/en/what/civil-protection/mechanism>
11. European Commission, *European Programme for Critical Infrastructure Protection*, 2007. <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:l33260>
12. European Parliament and the Council of the European Union, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281*, 23 Nov 1995, pp. 0031 – 0050.
13. European Parliament and the Council, Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, *Official Journal L 88*, 4 April 2011, pp. 45-65.

14. European Parliament and the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *Official Journal L* 119, 4 May 2016, pp. 1–88.
15. European Parliament, the Council and the Commission, Charter of Fundamental Rights of the European Union (2000/C 364/01), *Official Journal of the European Communities C* 364/1, 18 Dec 2000.
16. European Road Safety Observatory, “Which hospital? The importance of field triage”, 19 March 2015.
http://ec.europa.eu/transport/road_safety/specialist/knowledge/postimpact/pre_hospital_medical_care/which_hospital_the_importance_of_field_triage_en.htm
17. Hämmerli, Bernhard, *Protecting critical infrastructure in the EU*, CEPS Task Force report, 2010. <http://www.ceps.eu/publications/protecting-critical-infrastructure-eu>
18. HM Government, *Data Protection and Sharing – Guidance for Emergency Planners and Responders Non-statutory guidance to complement Emergency Preparedness and Emergency Response & Recovery*, February 2007.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60970/dataprotection.pdf
19. Hodge Jr., J. G., “The evolution of law in biopreparedness”, *Biosecurity and Bioterrorism*, 10(1), 2012, pp. 38-48.
20. Hutter, Reinhard, Hans Kühl, Pasquale Mari, Cian OBrian, Viorel Pectu, Mihai Palfi, *PULSE D5.1: Procedures and Status Quo Report*, 30 Nov 2015.
http://www.pulse-fp7.com/pdfs/D5_1_Procedures_and_Status_Quo_Report.pdf
21. Hutter, Reinhard, Hans Kühl, Pasquale Mari, Francesco Malmignati, Cian OBrian, Paul Kiernan, *D5.2 PULSE SOP*, 30 Nov 2015.
http://www.pulse-fp7.com/pdfs/D5_2_PULSE_SOP.pdf
22. Hutter, Reinhard, Pasquale Mari, Sabina Magalini, Paolo Pucci, Francesco Malmignati, Peter Daly, *PULSE Deliverable D2.2-Use case specification*, 31 Jan 2015.
http://www.pulse-fp7.com/pdfs/D2_2_Use_Case_Specification.pdf
23. Information and Privacy Commissioner of Ontario, *Planning for Success: Privacy Impact Assessment Guide*, May 2015.
<https://www.ipc.on.ca/wp-content/uploads/2015/05/Planning-for-Success-PIA-Guide.pdf>
24. Information Commissioner's Office, *Conducting privacy impact assessments code of practice*, February 2014.
<https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>
25. International Association for Information Systems for Crisis Response and Management (ISCRAM). <http://www.iscram.org/>
26. International Association of Emergency Managers, “Emergency Management: Definition, Vision, Mission, Principles”.
<http://www.iaem.com/documents/Principles-of-Emergency-Management-Flyer.pdf>

- 27.ISO/IEC, ISO/IEC 27000:2012 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. http://www.iso.org/iso/catalogue_detail?csnumber=56891
- 28.ISO/IEC, ISO/IEC DIS 29134 Information technology -- Security techniques -- Privacy impact assessment – Guidelines. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62289
- 29.ISO/IEC, ISO/IEC 29100:2011, Information technology -- Security techniques -- Privacy framework, 2011. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123.
- 30.Jacobson, P. D., J. Wasserman, A. Botosaneanu, A. Silverstein, & H. W. Wu, "The role of law in public health preparedness: Opportunities and challenges", *Journal of Health Politics, Policy and Law*, 37(2), 2012, pp. 297-328
- 31.Kaska, Kadri and Lorena Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2015.
- 32.Lo, Bernard, *Resolving ethical dilemmas: A Guide for Clinicians*, Wolters Kluwer, Philadelphia, 2013.
- 33.Malmignati, Francesco, Antonio Di Novi, Karl Chadwick, Paul Kiernan, *PULSE Deliverable D4.1 - Decision support validation tool*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_1_Decision_Support_and_Validation_Tool.pdf
- 34.Malmignati, Francesco, Massimiliano Taglieri, *PULSE Deliverable D4.2-IAT Tool*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_2_IAT_Tool.pdf
- 35.Mari, Pasquale, Viorel Petcu, Adelina Georgescu, Paul Kiernan, Reinhard Hutter, Clare Shelley-Egan, Lorenzo Marchesi, *PULSE Deliverable D2.1-Requirements specifications*, 30 Sept 2014. http://www.pulse-fp7.com/pdfs/D2_1_Requirements_Specification.pdf
- 36.Mari, Pasquale, Francesco Lauria, Reinhard Hutter, Hans Köhl, (CESS), Cian O'Brien (HSE), Peter Daly (HSE), Viorel Petcu (OST), Francesco Malmignati, Massimiliano Taglieri, Rowena Rodrigues, *PULSE Deliverable D7.1-Trials Definition*, 31 May 2016.
- 37.Mignanti, Silvano, Francesco Malmignati, *PULSE Deliverable D4.3 - Logistic tool*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_3_Logistics_Tool.pdf
- 38.O'Connor, J., P. Jarris, R. Vogt, & H. Horton, "Public health preparedness laws and policies: Where do we go after pandemic 2009 H1N1 influenza?" *The Journal of Law, Medicine & Ethics*, 39, 2011, pp. 51-55.
- 39.Sasser, S., M. Varghese, A. Kellermann, J.D. Lormand, "Pre-hospital trauma care guidelines", Geneva, World Health Organization, Geneva, 2005.
- 40.Shelley-Egan, Clare, David Wright and Kush Wadhwa, *PULSE Deliverable 8.1. Plan for Ethical Impact Assessment*, 31 October 2014. http://www.pulse-fp7.com/pdfs/D8_1_Review_of_Ethical_Issues_Affecting_PULSE.pdf
- 41.Taglieri, Massimiliano, Francesco Malmignati, *PULSE Deliverable D4.6-Post Crisis Evaluation Tool*, 30 Nov 2015. http://www.pulse-fp7.com/pdfs/D4_6_Post_Crisis_Evaluation_Tool.pdf

42. The European Group on Ethics in Science and New Technologies (EGE). <https://ec.europa.eu/research/ege/index.cfm>
43. The European Group on Ethics in Science and New Technologies (EGE), *Opinion no. 28 of the European Group on Ethics in Science and New Technologies, Ethics of Security and Surveillance Technologies*, Brussels, 20 May 2014. <http://bookshop.europa.eu/en/ethics-of-security-and-surveillance-technologies-pbNJAJ14028/>
44. The European Group on Ethics in Science and New Technologies (EGE), 2012. *Opinion n°26 - 22/02/2012 Ethics of information and communication technologies*. <http://bookshop.europa.eu/en/ethics-of-information-and-communication-technologies-pbNJAJ12026/>
45. The European Group on Ethics in Science and New Technologies (EGE), *Opinion n°13 Ethical Issues of Healthcare in the Information Society*, 30 July 1999. http://ec.europa.eu/archives/bepa/european-group-ethics/docs/avis13_en.pdf
46. The European Parliament and the Council of the European Union, Decision no 1982/2006/EC of the European Parliament and of the Council of 18 December 2006 concerning the Seventh Framework Programme of the European Community for research, technological development and demonstration activities (2007-2013). <http://cordis.europa.eu/documents/documentlibrary/90798681EN6.pdf>
47. Von Solms, Rossouw and Johan van Niekerk, "From information security to cyber security", *Computers and Security*, Vol. 38, 2013, pp. 97 – 102.
48. Whitman, Michael E., and Herbert J. Mattord, *Principles of Information Security*, 2012 Course Technology, Cengage Learning, 2012.
49. World Health Organisation, European Observatory on Health Systems and Policies Observatory, e-Bulletin. <http://www.euro.who.int/en/about-us/partners/observatory/observatory-e-bulletin>
50. World Health Organization, *Emergency Medical Services Systems in the European Union: Report of an assessment project co-ordinated by the World Health Organization*, DG SANCO, WHO, 2008. <https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/WHO.pdf>
51. Wright, D., "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, Vol. 13, 2011, pp. 199-126.
52. Wright, David, "Ethical Impact Assessment", in J. Britt Holbrook and Carl Mitcham (eds.), *Ethics, Science, Technology and Engineering: A Global Resource, 2nd edition*, Macmillan Reference, Farmington Hills, MI, USA, 2015, pp. 163-167.