EU Project No: 608078 (CP-FP)

IMPRESS

IMproving Preparedness and Response of HEalth Services in major criseS

Dissemination level:	CO
Type of Document:	O
Contractual date of delivery:	31/08/2015
Actual Date of Delivery:	16/09/2015
Deliverable Number:	D 1.7
Deliverable Name:	MoU and Confidentiality Agreement for the use and exchange of patient and other sensitive data between the partners
Deliverable Leader:	EUC (Louisa Shakou/ l.shakou@external.euc.ac.cy)
Work package(s):	WP1
Status & version:	Final, Version 1.0
Number of pages	14
WP contributing to the deliverable	1
WP / Task responsible	WP 1/ Task 1.4
Coordinator (name / contact)	INTRA (Aggelos Liapis / Aggelos.LIAPIS@intrasoft-intl.com)
Other Contributors	PHE, IICT-BAS, IVI, KEMEA, ECOMED, CNR
EC Project Officer	Mr. Marc Carton
Keywords:	Memorandum of Understanding, personal data, privacy, data processing, confidentiality agreement
Abstract (few lines):	This Memorandum of Understanding (MoU) sets out the responsibilities and commitments of the consortium to ensure that the collection, processing and storage of medical data and any other sensitive data is conducted in an ethical and legal manner.

Document History			
Ver.	Date	Contributor(s)	Description
0.1	08/07/2015	EUC	1st draft
0.2	28/07/2015	EUC, Ethical Review Committee	2nd draft
0.3	29/07/2015	EUC	Draft to include confidentiality agreement/clause
0.4	09/09/2015	EUC, PHE	Revisions based on comments and feedback from PHE- insertion of Annex 2 IMPRESS anonymisation standard
0.5	15/09/2015	IVI	Corrections
1.0	16/09/2015	EUC	Final version

TABLE OF CONTENTS

MEMORANDUM OF UNDERSTANDING AND CONFIDENTIALITY AGREEMENT FOR THE USE AND EXCHANGE OF PATIENT AND OTHER SENSITIVE DATA

between

INTRASOFT INTERNATIONAL SA (BELGIUM)
DEPARTMENT OF HEALTH
CONSIGLIO NAZIONALE DELLE RICERCHE
ADITESS ADVANCED INTEGRATED TECHNOLOGY SOLUTIONS &SERVICES LTD
SATWAYS- PROIONTA KAI YPIRESIES TILEMATIKIS DIKTYAKON KAI TILEPIKINONIAKON EFARMOGON ETAIRIA PERIORISMENIS EFTHINIS EPE
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES
CENTER FOR SECURITY STUDIES
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.
ECOMED bvba
AS CYPRUS COLLEGE LIMITED
INTRASOFT INTERNATIONAL SA (LUXEMBOURG)

1. PARTIES

The parties to this Memorandum of Understanding (MOU) are INTRASOFT International SA (Belgium); The Department of Health; Consiglio Nazionale Delle Ricerche; ADITESS Advanced Integrated Technology Solutions & Services LTD; SATWAYS-Proionta kai Ypiresies Tilematikis Diktyakon kai Tilepikinoniakon Efarmogon Etairia Periorismenis Efthinis EPE; Institute of Information and Communication Technologies; Center For Security Studies; FRAUNHOFER-Gesellschaft zur Förderung der angewandten Forschung e.V.; ECOMED bvba; AS Cyprus College Limited; and INTRASOFT International SA (Luxembourg) (*hereby known as the 'parties'*).

2. BACKGROUND

Project IMPRESS aims to advance the preparedness of emergency medical services (ambulance dispatch centres, hospitals, volunteer communities etc.) in various ways such as: through all-hazards planning; increasing surge capacity; tracking the availability of beds and other resources electronically; and the development of systems that are interoperable with other response teams. To achieve this, it will develop a Decision Support System (DSS) tool that will improve the efficiency of decision making in emergency health operations. The overarching objective is for the IMPRESS DSS tool to effectively manage medical resources and prepare and coordinate response activities using data from multiple heterogeneous sources. The proposed solution will facilitate communication between Health Services (and Emergency Responders) at all levels of the response and crisis cycle. Thus, the IMPRESS tool will collect and use patient data as well as other data relating to organisations involved in crisis management, raising issues of data collection, the ethical processing of this data and data protection. The IMPRESS consortium (*the 'parties'*) have agreed to sign a memorandum of understanding which affirms their intent to adhere to lawful and ethical standards for the use and exchange of patient and other sensitive data.

3. AUTHORITIES

This agreement is authorised in accordance to Article 8 of The European Convention on Human Rights; Articles 7 and 8 of The EU Charter of Fundamental Rights; Council of Europe Convention 108;

Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997) of the Council of Europe, Committee of Ministers; the EU Data Protection Directive 95/46/EC; The World Medical Association's Helsinki Declaration; and other future legal provisions that may arise pursuant to data protection and privacy.

4. PURPOSE

The purpose of this Memorandum of Understanding and Confidentiality Agreement is to manage and control the access, transfer, subsequent processing and storage of personal data concerning health (as defined in the Council of Europe Convention 108) between the parties. Data may be shared between the parties in order to fulfil their obligations as part of the activities of the IMPRESS project.

This agreement ensures that data are shared in a way which satisfies both the legal and statutory obligations of the parties.

5. DEFINITIONS

i. **Personal Data** means any information relating to an identified or identifiable individual.

ii. **Personal Data Concerning Health** includes in particular all data pertaining to the health status of a data subject; information about the registration of the individual for the provision of health services; information about payments or eligibility for healthcare with respect to the individual; a number, symbol or particular assigned to an individual to uniquely identify the individual for health purposes; any information about the individual collected in the course of the provision of health services to the individual; information derived from the testing or examination of a body part or bodily substance, including biological samples; identification of a person as provider of healthcare to the individual; or any information on e.g. a disease, disability, disease risk, medical history, clinical treatment, or the actual physiological or biomedical state of the data subject independent of its source, such as e.g. from a physician or other health professional, a hospital, a medical device, or an in vitro diagnostic test. Article 8 of the Data Protection Directive (95/46/EC) qualifies health data as a special category of data to which a higher level of data protection applies.

iii. **Anonymised Information** is information which does not identify an individual directly, and which cannot reasonably be used to establish identity. Anonymisation is designed to irreversibly sever the connection between the information collected and the individual, so that the information no longer reveals anything about that individual. It requires the removal of name, address and any other detail or combination of details that might result in identification. There can be no re-identification of anonymised information. Anonymised information is different from de-identified information in that in the latter you can re-identify an individual from the de-identified information using a number of different methods.

iv. **Privacy,** for the purposes of this memorandum of understanding, refer to informational privacy and involves the right of an individual to expect that personal information collected about them will be processed securely and will not be distributed in any form without their written consent, unless there is an exception provided by law.

v. **Data subject** means an individual who is the subject of personal data.

vi. **Data controller** means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

vii. **Data processor** means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

viii. **Processing** means performing any operation or set of operations on data, including:

- obtaining, recording or keeping data,
- collecting, organising, storing, altering or adapting the data,
- retrieving, consulting or using the data,
- disclosing the information or data by transmitting, disseminating or otherwise making it available,
- aligning, combining, blocking, erasing or destroying the data,
- anonymising, de-identifying and pseudo-anonymising the data[1].

6. THE PARTIES AGREE TO THE FOLLOWING

6.1 That in each stage of the IMPRESS project the rights and freedoms of the data subject and mainly his/her dignity and privacy will be respected and protected according to the law and the ethical guidelines set out in the 1st Interim Ethics Report (D 1.10).

6.2 That data will be obtained (collected) fairly. To ensure fair collection no person/data subject will participate without his/her legally effective explicit and informed consent or the consent of the data subject's guardian/judicial supporter or his/her legally authorised representative. Consent will be requested by the parties in a manner that will allow a prospective data subject or their representative to fully understand the implications of their participation and which will provide them with sufficient information so that they can consider fully whether or not to participate; minimising therefore the possibility of coercion or undue influence. The parties ensure that the information that will be given to any data subject or their representative shall be in a language understandable to the data subject or their representative.

6.3 Data controllers and data processors may only process personal data purely for the explicit, legitimate, clearly specified and documented purpose(s) of the IMPRESS project as laid down in the Description of Work of the project. Data may not be processed for purposes which are not compatible with the project's purposes and/or further (re)used for any other purpose(s).

6.4 Only personal data that are adequate, relevant and not excessive to the purposes of the project (i.e. only the minimum amount of data needed to achieve the purpose(s) of IMPRESS) shall be collected and processed by the parties.

[1] As per Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

6.5 That data will be anonymised using the anonymisation protocol set out in Annex 2 in order to protect privacy and the right to data protection. This anonymisation is carried out under the responsibility of the data controller just after data collection and before the further processing of data by data processors; who thus will only have access to anonymised data.

6.6 Only anonymised data will be exchanged by and between the parties.

6.7 The parties must ensure that during data collection, processing and exchange the data remain accurate and reliable.

6.8 If personal data is no longer necessary the parties will erase/destroy them unless and to the extent that retention is necessary for the documentation of the IMPRESS research activities.

6.9 Researchers employed by the parties acting as data processors will have access only to data that they are specifically mandated and/or authorised to use. Access to any database holding personal data is restricted to data processors who are specifically mandated /authorised to have access and process personal data for the purposes of the project. Data may be transferred to data processors only after the approval of the data controller.

6.10 No party is allowed to transfer, disclose or to make available data to third parties outside the IMPRESS Consortium without the express approval of the IMPRESS Consortium and without a signed Confidentiality Agreement.

6.11 No party is allowed to transfer, disclose or to make available data to third parties outside the IMPRESS Consortium without the express approval of the data subject.

6.12 Data subjects may exercise their right to access their data collected and stored for the purposes of the project as well as the right to object to the further processing and/or to request rectification or erasure of their data. Where a data subject exercises these rights the data controller will notify the data processors who have to act accordingly.

7. IT IS MUTUALLY AGREED AND UNDERSTOOD BY AND AMONG THE PARTIES THAT

7.1 Each Party is responsible for ensuring the integrity of data transferred to it and maintained in its systems; for maintaining safeguards to prevent any unauthorised disclosure of the data; and for ensuring that access to data is only provided to employees that are part of the IMPRESS project. Disclosure of the data must be consistent with applicable laws and policies including the EU Data Protection Directive 95/46/EC and any future amendments; Article 8 of The European Convention on Human Rights; Articles 7 and 8 of The EU Charter of Fundamental Rights; Council of Europe Convention 108; and Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997) of the Council of Europe, Committee of Ministers.

7.2 They are bound by a confidentiality obligation.

8. SECURITY

8.1 All parties agree to ensure the security of the data they store, process, and transmit, during the IMPRESS project. The Data Controller and the Data Processors (researchers and the organisations in which they are situated) are responsible for data security and will adopt and implement all the appropriate technical and organisational measures to protect personal medical and other data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

8.2 If access to data or the exchange of data involves their transmission over a network, the data controller and the data processors will take all the appropriate measures to transmit the data via a secured network and/or by a secured procedure in order to prevent unauthorised access and interference to the network or to the data. Data security will be preserved through anonymisation, encryption, and regulation of the medium of transfer.

8.3 Each party will be responsible for data security within its own organisation, according to the national law, respective codes of conduct and professional standards as well as the guidelines approved within the consortium for data treatment and data security (D 1.10).

9. NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT FOR EXTERNAL THIRD PARTIES

Each party undertakes to enter into a non-disclosure and confidentiality agreement with any external third party with which it will exchange and use personal and sensitive data, in the form or substantially in the form as set out in Annex 1.

10. DATE EFFECTIVE

This MoU shall be effective from the date of signature of the last Party to sign by the Parties and is intended to be in force until terminated by either Party. Any amendment or modification is effective upon mutual written consent of the Parties.

11. SIGNATURES

NAME, SURNAME, Position
INTRASOFT INTERNATIONAL SA (BELGIUM)

NAME, SURNAME, Position
DEPARTMENT OF HEALTH

NAME, SURNAME, Position
CONSIGLIO NAZIONALE DELLE RICERCHE

NAME, SURNAME, Position
ADITESS ADVANCED INTEGRATED TECHNOLOGY SOLUTIONS &SERVICES LTD

NAME, SURNAME, Position
SATWAYS EPE

NAME, SURNAME, Position
INSTITUTE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

NAME, SURNAME, Position
CENTER FOR SECURITY STUDIES

NAME, SURNMANE, Position
FRAUNHOFER-GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V.

NAME, SURNAME, Position
ECOMED bvba

NAME, SURNAME, Position
AS CYPRUS COLLEGE LIMITED

NAME, SURNAME, Position
INTRASOFT INTERNATIONAL SA (LUXEMBOURG)

Date: XXXX 2015

ANNEX 1

CONFIDENTIALITY AGREEMENT FOR THE USE AND EXCHANGE OF PATIENT AND OTHER SENSITIVE DATA

Date: XXXX

Between

[IMPRESS party(ies)- *insert as appropriate*]

And

[3rd external party- *insert as appropriate*]

Individually referred to as a Party or collectively as the Parties.

12. THE PARTIES AGREE AS FOLLOWS

1.1 For the purpose of this agreement Confidential Information shall mean any and all information, which is supplied or disclosed, directly or indirectly, in writing or in any other means, by each Party to the other as well as to third parties including, but not limited to any data, documents, prototypes, know-how, foreground, background and which at the time of its disclosure or supply is identified as confidential.

1.2 Each party to this Agreement is referred to as 'the Recipient' when it receives or uses the Confidential Information/Data disclosed by the other party.

1.3 Each Party intends to disclose Confidential Information to the other Party for purposes agreed between the parties to this agreement. Any data (personal or organisational) will only be used for purposes agreed and information will be retained for a period agreed between the parties and destroyed by an agreed method.

Agreed purposes are: [*To be completed]*

Agreed retention period: [*To be completed]*

Agreed destruction method: [*To be completed]*

1.4 The Recipient shall:

i. undertake to keep the Confidential Information confidential and not to disclose it nor to permit the disclosure of it to any third party, except in accordance with clause 1.6 of this agreement, and not to make it available to the public or accessible in any way, except with the prior written consent of the Party disclosing it;

ii. undertake to use the Confidential Information solely for the Purpose of this agreement and not to make any other use, without the prior written consent of the Party disclosing it.

1.5 The Recipient shall limit and control any copies and reproductions of the Confidential Information. The Recipient shall return all records or copies of the Confidential Information at the request of the other Party and at the latest on termination of this agreement. This shall not apply to Confidential Information or copies thereof which must be stored by the Recipient according to mandatory law, provided that such Confidentiality Information or copies thereof shall be subject to an indefinite confidentiality obligation.

1.6 The Recipient undertakes to disclose the Confidential Information only to its employees who:

i. reasonably need to receive the Confidential Information for the Purpose of the present agreement; and
ii. have been informed by the Recipient of the confidential nature of the Confidential Information and of the terms of the present agreement; and
iii. have been advised of and agree to be bound by equivalent obligations to those in the present agreement.

13. MISCELLANEOUS

2.1 This Agreement shall be effective from the date of signature of the last Party to sign and shall remain in effect until terminated by either party.

2.2 All the clauses of this Agreement are intended to be legally binding.

2.3 A Party may at any time terminate this Non-Disclosure Agreement and Confidentiality Agreement. Such termination shall be done in writing to all other Parties.

2.4 This Non-Disclosure Agreement and Confidentiality Agreement shall be governed by and construed in accordance with the laws of [insert the country].

IN WITNESS WHEREOF, the Parties hereto have caused this Non-Disclosure and Confidentiality Agreement to be executed as of the date stated above.

FOR [insert name of potential participant]

[insert name of representative]

[insert title]

Done at [place] on [date]

[Add the identification of all the potential participants]

ANNEX 2

1.1 IMPRESS ANONYMISATION PROTOCOL

There is no prescriptive standard in EU legislation on anonymisation standards[2]. This Annex sets out a protocol for the IMPRESS consortium on the anonymisation of personal data.

In order to ensure an adequate level of data anonymisation within the activities of IMPRESS the following criteria [2,3] must be used to inform decisions on the anonymisation technique (s) which will be used:

- Is it still possible to single out or re-identify an individual?
- Is it still possible to link records relating to an individual?
- Can information be inferred concerning an individual?

This Annex does not recommend a particular anonymisation technique(s); each technique has its strengths and weaknesses[4]. The choice of an anonymisation technique lies with the data controller, based on the criteria above and the particular context for which data will be shared amongst the parties of this MoU. The best solution should be decided on a case-by-case basis, which may include using a combination of different anonymisation techniques. Commonly used anonymisation techniques include:

Randomisation[2] — Family of techniques that alters the accuracy of the data in order to remove the strong link between the data and the individual. If the data are sufficiently uncertain then they can no longer be attributed to a specific individual. Includes:

1. Noise Addition
2. Permutation
3. Differential Privacy

Generalisation[2] — This approach consists of generalising, or diluting, the attributes of data subjects by modifying the respective scale or order of magnitude (i.e. a region rather than a city, a month rather than a week). Includes:

1. Aggregation and K-anonymity
2. Cross-tabulation of data
3. L-diversity/T-closeness

Data Reduction[3] — Data reduction methods are used to increase the number of individuals in the sample that share the same characteristics. Data reduction techniques are devised to minimise the presence and number of unique identifiable records of

[2] Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm

[3] ICO (2012), *Anonymisation: managing data protection risk code of practice*, Information Commissioner's Office

[4] See Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party for a discussion on the merits and weaknesses of several anonymisation techniques as well the ICO's Anonymisation: managing data protection risk code of practice Annex 3

	individuals. Includes: 1. Removing variables 2. Removing records 3. Global recoding 4. Top and bottom coding 5. Local suppression
Data perturbation[3]	Includes: 1. Micro-aggregation 2. Data swapping 3. Post-Randomisation Method 4. Resampling

Once data has been anonymised, before it is shared or exchanged with the parties of this MoU, the data controller must test the data to ensure the robustness of anonymisation. The Article 29 Data Protection Working Party recommends that tests for robustness should take into account the following risks to anonymisation:

- **Singling out** , which corresponds to the possibility to isolate some or all records which identify an individual in the dataset;
- **Linkability**, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability;
- **Inference**, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

The process of testing for the robustness of the anonymisation of the data must be documented.

1.2 NOTE ON ANONYMISATION AND PSEUDO-ANONYMIZATION

According to the EU Data Protection Directive 95/46/EC, data either identify an individual or they do not. When data are identifying, there are significant constraints on how they can be used. In fact, the processing of identifying personal data is prohibited by the EU Data Protection Directive 95/46/EC. Derogation from this prohibition is only justified in certain circumstances and even then, as little as possible identifying information must be used. Identifying data may be used in one of the following circumstances:

- With the explicit consent of the data subject;
- For the purposes of direct patient care;
- Where there is statutory authority for a particular use (e.g. the prevention, investigation, detection and prosecution of criminal offences); or

- In exceptional circumstances, where it is justified in the public interest (e.g. national security and defence).

Where no lawful justification exists e.g. in the case of research, non-identifying data must be used, which is where the need for anonymisation arises. Commonly, when data are not identifying there are few, if any, constraints on their use.

However, individuals can be identified in a number of different ways which affects the route to anonymisation. Individuals can be identified directly, where someone is explicitly identifiable from a single data source, such as a list including full names, or indirectly, from the data collected and 'other information' which is owned, or is likely to be obtained by the data controller. For example, an individual can be identified from the combination of two or more data sources or from the combination of the data collected with other information available to certain organisations, to certain members of the public or that is available to everyone because it has been published on the internet. To further complicate matters, the risk of identification may increase over time as information and communication technology develops and research tools, data linkage techniques and computational power evolve e.g. the use of powerful data analysis techniques are now widespread when they were once rare.

In broad terms there are two categories of non-identifying data:

Anonymised data	Data which does not identify an individual directly, and which cannot reasonably be used to establish identity. Anonymisation results from processing personal data in order to irreversibly sever the connection between the information collected and the individual, so that the information no longer reveals anything about that individual. Anonymisation prevents all parties from singling out an individual in a dataset, from linking two records within a dataset or between two separate datasets and from inferring any information in such datasets. There can be no re-identification of anonymised data. Anonymised data is different from pseudo-anonymised/de-identified data in that in the latter you can re-identify an individual from the pseudo-anonymised/de-identified i using a number of different methods.
Pseudonymised data[5] (also known as De-identified or coded data)	Pseudo-anonymised data is data where personal identifying characteristics are removed from the data and assigned a unique identifier or a code of randomly assigned numbers and/or letters often generated by a system (known as a pseudo-anonymized identifier). There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field. Data can be re-identified by decrypting the code using a key. As long as the code key exists, it could still be possible to identify a patient, and guardians of the key would have to comply with the EU Data Protection Directive 95/46/EC. To further increase data security the pseudo-anonymised data may be stored separately to the identifiable data and in some cases a second coding system may be added.

[5] POST (2005),*Data Protection and Medical Research*, POSTnote 235 http://www.parliament.uk/documents/post/postpn235.pdf

Pseudonymised data is **not equivalent** to anonymised data. According to the Article 29 Data Protection Working Party pseudonymised data cannot be equated to anonymised information[6]. Pseudonymity is likely to allow an individual data subject to be singled out and linkable across different data sets. Pseudonymised data therefore falls within the scope of the legal regime of data protection.

1.2.1 SPATIAL DATA

Spatial data includes information such as postcodes, GPS data or map references. The EU Data Protection Directive 95/46/EC does not have any hard and fast rules on how such data should be handled. In some cases spatial data may constitute personal data, e.g. where information about a place or property is, essentially, also information about the individual associated with it. In other cases it will not constitute personal data. To determine whether spatial data is also personal data the context of the data and other variables, and how they can be combined to make inferences is crucial. For example, the more complete a postcode (such as the number of households covered by a postcode) or the more precise a piece of geographical information, the more possible it becomes to analyse it or combine it with other information, resulting in personal data being disclosed.

[6] Opinion 05/2014 on Anonymisation Techniques of the Article 29 Data Protection Working Party http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm