European Security in Health Data Exchange

Deliverable D1.8

Ethical protocols and approval

Editor(s):	Brian Pickering (IT Innovation)
Responsible Partner:	IT Innovation
Status-Version:	Final
Date:	30/06/2017
Distribution level (CO, PU):	PU

Project Number:	GA 727301
Project Title:	SHIELD

Title of Deliverable:	Ethical protocols and approval
Due Date of Delivery to the EC:	2017/06/30

Workpackage responsible for the Deliverable:	WP1
Editor(s):	Brian Pickering, IT Innovation
Contributor(s):	Xabier Larrucea (Tecnalia); Tony Schaffel (Lancs NHS)
Reviewer(s):	Alberto Berreteaga (Tecnalia)
Approved by:	Xabier Larrucea (Tecnalia)
Recommended/mandatory readers:	All WP's

Abstract:	Specification of the ethical research protocols to be used in SHiELD, including specific protocols for validation testing
Keyword List:	Ethics; Ethical Approval; Data Protection; Research Protocol; Trial Management
Disclaimer	This document reflects only the author's views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein

Document Description

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	Modified by
v0.1	18/05/2017	Table of contents for Partner Approval	Brian Pickering (IT Innovation)
V0.2	01/06/2017	Integrated partner input (Lancashire NHS, Tecnalia)	Xabier Larrucea (Tecnalia), Tony Schaffel (NW HNS), Brian Pickering (IT Innovation)
V0.3	22/06/2017	Integrated input from FCSR	Eleonora Lavalle (FCSR), Brian Pickering (IT Innovation)
V0.4	23/06/2016	Revision by Tecnalia	Alberto Berreteaga (Tecnalia)
V1.0	29/06/2017	Final version	Brian Pickering (IT Innovation)

Table of Contents

List of Figures

List of Tables

Terms and abbreviations

AB	Advisory Board
CA	Consortium Agreement
DPA	Data Protection Agency; also known as the Supervisory Authority
EHR	Electronic Health Record
EtC	Ethics Committee
GDPR	General Data Protection Regulation
MS	Member State of the European Union
WP	Work Package
WPL	Work Package Leader

Executive Summary

The objective of the present report is to introduce the ethical management and planning for the proposed SHiELD trials. To demonstrate not only the functional completeness of the SHiELD offerings but also their acceptability to potential adopters, a number of trial scenarios within the healthcare domain are planned. These scenarios are targeted at typical situations where a patient may be aware from their home location and require appropriate treatment at a different location typically within a different EU Member State. With the patient's care requirements paramount, such scenarios would typically require access to sensitive ("special category") personal data for that patient.

In consideration of the ethical execution of these tests, this deliverable focuses on a number of areas:

- Chapters 1 and 2 summarise the ethical principles and project governance structure to be applied during the trials;
- Chapter 3 then provides a high-level description of the trials, including a default research protocol (Section 3.1) which is intended as a proforma to be developed and customised in WP6; and describes the three specific scenarios which will be used to exercise the SHiELD offerings (Sections 3.2, 3.3 and 3.4);
- Based on the outline in Chapter 3, Chapter 4 and 5 review any specific concerns and challenges from an ethical perspective which need to be considered in the planning and execution of the trials, as well as by the technical partners in how they develop the supporting components;
- Finally, Chapter 6 provides the current status of ethical approval for the default research protocol outlined in Chapter 3.

This report therefore explores all ethical aspects of the proposed trials in SHiELD. As such, it should be read in conjunction with D1.5 Data management plan, D3.1 Report on legal requirements and D8.1 GEN Requirement no1 (proformas). It will also provide a basis against which to develop customised and specific trials in WP6.

1 Introduction

As set out in Article 34 of the Grant Agreement, there are two guiding principles for ethical research:

(a) ethical principles (including the highest standards of research integrity — as set out, for instance, in the European Code of Conduct for Research Integrity — and including, in particular, avoiding fabrication, falsification, plagiarism or other research misconduct) and
(b) applicable international, EU and national law.

In response to these provisions, the validation cases in SHiELD project follow the basic principles outlined in the European Code of Conduct for Research Integrity itself [1], as well as related research guidelines [2, 3]; whilst at the same time respecting the provisions of the General Data Protection Regulation (GDPR) with regard to the applicable EU law [4]. Indeed, the whole project is based around the fundamental right of all EU citizens to the protection of personal data[1].

There is, however, another principle. In addition to an inalienable right to protection of personal data, every individual has the right to care and an expectation of appropriate medical treatment. This may lead to conflict: if the individual is unable to provide consent, then do their 'vital interests', i.e., the decision of another medically component individual to intervene, take precedence? The purpose of the SHiELD project is to explore ways in which this possible conflict can be managed to ensure the best possible outcomes for the individual who may need treatment away from their home country.

With this in mind, this deliverable sets out the general approach to the ethical management and execution of the validation activities of the project.

1.1 Ethical management structure

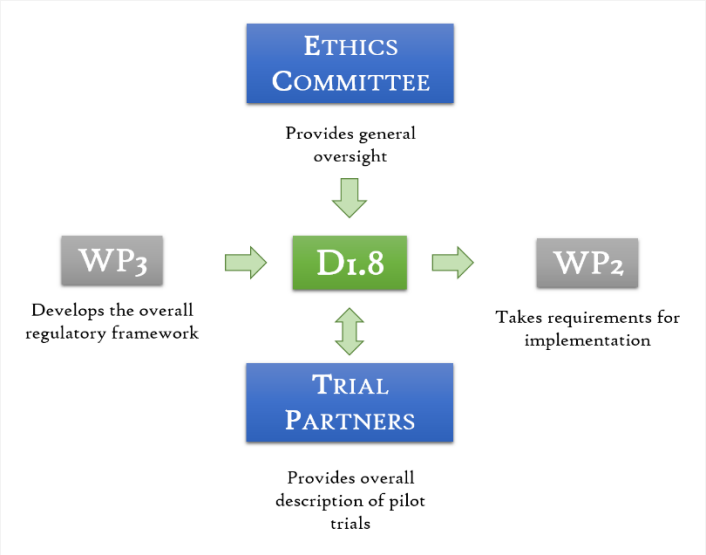

Figure 1: How this deliverable fits in with the SHiELD project

[1] Article 8 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012P/TXT&from=EN

This report provides the initial set of guidelines and reference point for the management of the external trials. As such it is dependent on various parties (shown in blue in Figure 1 above) and relates to other work packages (shown in grey). The research protocols are therefore constrained by the regulatory framework reported via **WP3**; and subject to oversight during trial execution by an Ethics Committee. As well as validating the solution proposed by SHiELD, as the research protocols are executed there may be additional or refined technical requirements which need to be fed back to the technical partners via **WP2**.

In addition, this report takes input from the **trial partners** themselves to describe and understand the objectives of each of the trials directly and via **D1.5** the Data Management Plan to develop appropriate research protocols to ensure appropriate ethical management of the trials. In return, the trial partners will use D1.8 as a reference to ensure that any modification to the research protocols are understood and can be accommodated within the existing approvals.

The **Ethics Committee (EtC)** is one of the management structures in the project[2] and will maintain ongoing oversight of the trials, with regular status updates and a virtual meeting currently planned for M10, M22 and M34 of the project. In addition, the EtC provides an interface externally with the Faculty Ethics Committee of the Faculty of Physical Science and Engineering at the University of Southampton. This Committee will be approached to provide research ethics approval for the initial research protocols outlined in this document. As described in the Grant Agreement[2] the EtC includes members of the project and technical management of the project along with the work package leaders from each of the work packages. In consequence, the project management teams will be aware of an issues raised immediately so that appropriate action can be taken without delay.

1.2 SHiELD Trial Data

There are three sorts of data involved specifically in the proposed SHiELD trials. These include:

I. **Patient health records** (EHR): these summarise an individual's state of health, along with appropriate personal (identifying) information. For the purposes of the SHiELD project, these data are **simulated**, and therefore will not identify any living individual. In consequence, they require no specific treatment. However, to ensure that tests are viable, they must be good exemplars of such real life data. This is the responsibility of the respective trial partners. Although there is no legal requirement to manage or process these data with any special care, in practical terms and for the purposes of the trials themselves, they will be treated as if they were real patient data.

II. **Trial participant details**: personal information (contact details etc.) about those recruited to take part in the trials. These data will be managed by the respective trial partners in accordance with their standard procedures. They will **not be shared** with other project partners. There is no plan to release the data anywhere else during or after the project.

III. **Trial outcome data**: depending on the specific experimental design for a given trial, these data will typically be qualitative such as specific feedback and responses by participants. Although no personal details will be collected, all qualitative data will be pseudonymised to ensure that no participant might be identified from their input.

The latter two categories, especially the third, are the most relevant for the SHiELD trials planned.

[2] GA 727301 – pp50ff

1.3 Background

The General Data Protection Regulation (GDPR) [4] was published in April, 2016, and is set to become law across EU Members States (MS) in May, 2018. Notwithstanding any minor country-specific deviations and the ongoing negotiations under Article 50 between the EU and the United Kingdom, the GDPR represents the most important legal reference in terms of the protection of personal data. As presented in **D3.1 Report on legal requirements**, the GDPR will provide the basis for the ethical research protocols in SHiELD. In the spirit of the GDPR, the following basic principles will be used:

1. Given that the GDPR sets out that only a single Data Protection Authority (DPA) need to be notified for cross-jurisdiction activities involving more than one Member State ([4], Article 56; see also Recital 53), **DPA Registration** for the research activities of the trials is already in place with the University of Southampton and the UK DPA. There are two caveats here:
    a. Individual partners in Italy and Spain (Vizcaya) may be required to register locally for such activities;
    b. In the event of EU/UK negotiations completing during the project lifetime, additional DPA registration will be sought either in Italy or Spain.
2. In spirit of extended responsibilities to the data processor (see the next section for a definition of the term; and [4] Article 28), the nominal responsibilities of **Data controller** and **Data processor** will apply to all project partners involved in the trials: i.e., the Data controller and processor will share the responsibility for the appropriate management and treatment of personal data in the trials (see also Figure 2).

One objective of the SHiELD project is to support a legal basis of processing by the relevant authorities as:

3. "Processing is necessary in order to protect the vital interests of the data subject or of another natural purpose" ([4] Article 6(1)(d))

In the next section, we consider the relevance of the legal definitions in the GDPR ([4] Article 4) as they relate to SHiELD.

1.4 Definitions

The following table provides definitions for relevant terms from the GDPR along with an explanation of why they are relevant to the SHiELD trials (see Table 1). As the third column in the table shows, applying the legal constructs of the GDPR to SHiELD is very context dependent.

Term	Legal Definition	Relevance to SHiELD
CONSENT	"'[C]onsent' of the data subject means any freely given, specific, information and unambiguous indication of the data subject's wishes by which he or she, by a statement or aby a clear affirmative	Consent is the most obvious legal basis for the processing of personal data. In the majority of research cases, this should be informed consent. This in turn needs to be based on appropriate information about a given trial being made available, for instance, telling the participant what will happen in a given

Term	Legal Definition	Relevance to SHiELD
	action, signifies agreement to the processing of personal data relating to him or her". (Article 4, (11))[3]	trial, what data will be collected and how those data will be managed. For SHiELD, consent will be needed principally to show participant agreement to take part in the study. This should therefore be on the basis of detailed participant information provided to the potential participant to let them know what they will be expected to do. Any consent forms[4] would themselves constitute personal data and so must be stored appropriately.
DATA CONTROLLER	"[The] 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (Article 4, (7))	As summarised in Figure 2, the data controller is individual or organisation who decides what data are to be collected and what processing will be done with those data. For the purposes of the project as a whole, the Project Steering Committee[2] acts as overall data controller since it is responsible for the overall direction of the project. However, for the individual trials, given that they know what needs to be done to satisfy their end users and the obligations they have towards those users, individual trial partners will also act as data controllers for their respective trials.
DATA PROCESSOR	"[The] 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (Article 4, (8))	As with the data controller, different partners and constructs in the project assume responsibility for the role of data processor (see Figure 2). The default data processor is the Technical committee[2] responsible for providing the general mechanisms

[3] Unless otherwise stated, definitions are taken from the GDPR [1]

[4] A suggested template is given in Section 7.2.1

Term	Legal Definition	Relevance to SHiELD
		within the product design and implementation to enable partners to process data (even simulated data) securely. In support of these responsibilities, individual work packages (specifically the WPLs of WP2, WP4 and WP5) are responsible for providing the individual components to enable the Technical committee to meet their obligations in this respect.
DATA SUBJECT[5]	"Data subject means an individual who is the subject of personal data"[5]; further "an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly" ([4], Article 4, (1))	Since the SHiELD trials in WP6 use simulated but representative data only, the only data subjects are the participants[5] who take part in studies; i.e., not patients themselves to whom the simulated EHR may refer.
LEAD SUPERVISORY AUTHORITY[6]	"[A]n independent public authority which is established by a Member State" (Article 4, (21)) to oversee data protection	As outlined above (section 1.2), the Lead Supervisory Authority (or DPA) is the UK DPA for the external trials. So long as the trials involve *research* only[7], the DPA Registration of the University of Southampton may be used.
PERSONAL DATA	"any information relating to an identified or identifiable natural person" (Article 4, (1))	There are two possible sources of personal data in the WP6 trials. First, contact and demographic information about participants in the validation trials. Such data is held and managed under existing procedures by the partners responsible and is **not**

[5] "Participant" is used to identify an individual who **takes part in** a given research trial. They may not necessarily provide personal data within the context of the research study itself. See, for example, [5]

[6] The term Data Protection Authority (DPA) is used throughout this deliverable.

[7] Research is understood in the Frascati sense [7]

Term	Legal Definition	Relevance to SHiELD
		shared with other members of the consortium. In addition, and adhering strictly to the legal definition, it is possible that qualitative feedback provided as part of the research protocols *could* lead to the identification of an individual. To mitigate against this, any such data will be *pseudonymised* (see below).
PSEUDONYMISATION	"[T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without additional information" (Article 4, (5)) ANONYMISATION [6, Paragraph (26)]	There is no need to pseudonymise the EHR data since they are simulated and therefore do not refer to any living, identifiable individual. Any reporting around the participants (e.g., general demographic information) will be fully anonymised such that no individual can be identified. Any qualitative data represents a particular problem. Although it is relatively easy to pseudonymise[8] transcripts from interviews or focus groups, for instance, there can be more subtle indicators of style and language competence that could lead to identification. This will be dealt with as and if the need arises[9].
SENSITIVE PERSONAL DATA	Or special categories of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, […] data concerning health or data concerning a natural person's sex life or sexual orientation" (Article	Since the data to be used in the trials are based on patient health data, they would be classed as *sensitive* or special category personal data. However, since such data in the trials are simulated, then there is no need to protect or otherwise ensure security of the data. Having said that, in practical terms, the simulated EHR data will be treated as

[8] Typically proper names are simply replaced along with any specific information such as job title.

[9] One approach is to normalise the text as much as possible and then return to participant(s) for their approval prior to release. Care must be taken not only to avoid any risk of personal identification, but also to reduce the research potential of the raw data if shared with the research community. See also D1.5: Data Management plan.

Term	Legal Definition	Relevance to SHiELD
	9, (1)).	sensitive personal data in order to validate the effectiveness of the solution.
THIRD PARTY	"[A] natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who under the direct authority of the controller or processor, are authorised to process personal data" (Article 4,(10))	There are currently no plans within SHiELD to engage with any third party for the purposes of the project itself. However, in accordance with D1.5 Data Management plan, it is possible that publication of research data may lead to the processing of some of the research data by others. If required, this will form the basis of any conditions imposed on data sharing via external repositories[10].

Table 1: Definitions from the GDPR as they apply to the SHiELD validation cases

As can be seen in the table (Table 1), along with the Data management plan in D1.5: Data management plan and D3.1: Report on legal requirements, the project is seeking to apply legal requirements to the practical and ethical processing of data across the validation use cases.

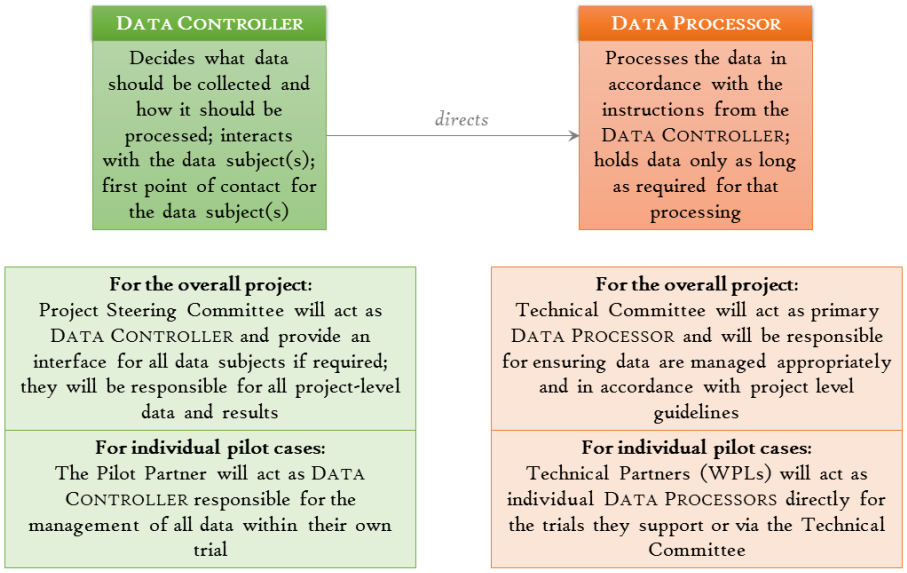

Figure 2: Summary of data management responsibilities for the project

With this in mind, Figure 2 makes clear the specific application of the terms Data controller and Data processor to SHiELD and how the associated responsibilities are understood as they apply to the work being carried out in validating the SHiELD offering. As the figure shows, the management structures outlined in the project provide the basis Data controller and Data

[10] See D1.5, section 3.2 "Data openly accessible"

processor responsibilities. For Data controller, the Project Steering Committee determines how personal data should be used and managed across the project. Correspondingly, the Technical Committee then assume the default Data processor role since it is their responsibility to act on and support the project goals identified by the Project Steering Committee.

However, as stated briefly in Table 1, there is a further pragmatic layer to ensure complete control and accountability for data, both personal data and research data. In regard to the individual pilot trials outlined below (see Chapter 3), the trial partners themselves assume responsibility as Data controller for their respective trials. In this may, they maintain complete control over their own trials. Conversely, the individual WPLs act as Data processors. Although they do not directly respond to the processing requests of the trial partners, they are responsible to the Technical manager of the project to generate the appropriate component parts which provide the total SHiELD offering.

2 Ethical principles

The European Code of Conduct for Research Integrity [1] outlines a set of research principles as follows (*op.cit.*, p.4):

PRINCIPLE	DEFINITION	RELEVANCE TO SHIELD
Reliability	Research design should be appropriate and results replicable	The research protocols set out in this deliverable will provide detailed information to allow those interested to be able to replicate procedures used to test the validity and applicability of the validation findings
Honesty	Research must be undertaken and presented with complete honesty and integrity	The project quality assurance processes are in place to ensure that research findings are shared and presented appropriately
Respect	Research must respect individuals, society and the environment	The validation trials will be carried out with the approval of a university faculty ethics committee providing initial review and validation of the research protocol during planning. Subsequently the project Ethics Committee will monitor the execution of the tests
Accountability	Research should be carried out to be shared with and to benefit all	The project will share results as outlined in D1.5 Data management report. Project partners will also engage directly with their stakeholders to make them aware of what has been done in the project and how those outcomes are relevance for them.

Table 2: Relevance of Ethical Principles to SHiELD

The purpose of this document therefore is to provide an initial default research protocol which may be checked against these research principles. The default protocol is also used to seek initial, external Ethics approval.

3 Pilot trials

In the following sections, we describe the initial default research protocol along with the three specific scenarios to be covered in the three trials in Italy, Spain and the UK. The default research protocol provides a basis for partners to consider any specifics which would require a different protocol. This is important because it will help isolate specific aspects for individual trials which may require additional ethical approval.

3.1 Default Research Protocol

3.1.1 Data subjects

Data subjects will be colleagues known to trial partners, role-playing various activities.

3.1.2 Participants

The participants in this will be test subjects with no link to 'real' patients/citizens.

3.1.3 Trial procedure

There will be three specific scenarios:

1. "Break glass" scenario (Section 3.2) whereby a potential patient is in need of care but unable to provide consent. The patient is in a situation of life-threatening risk and access to clinical data can determine a safer and more efficient management;
2. Surgical follow-up (Section 3.3) where it is important for clinicians to consult a potential patient's EHR to identify factors which may (or may not) be relevant to ensure appropriate treatment; and
3. Remote monitoring (Section 3.4) whereby access is required to monitoring data from a potential data source. This case would be applicable mostly in patients with chronic diseases suffering an exacerbation in the condition.

Each of these tests the basic motivation for the project: the ethical and legal handling of sensitive personal data across jurisdictions. This is not simply a question of consent, of course, but also of protecting the vital interests of potential patients. The overall aim therefore is to ensure the best level of care for any given patient is managed appropriately.

Across these three scenarios, participants will role-play the individual scenarios and provide two types of input:

I. By monitoring the way participants use the SHiELD platform, trial partners will gather performance data to share with technical partners on whether or not the platform works; and
II. Qualitative feedback from participants (patients, health care professionals and stakeholders) to be shared with consortium partners relating to whether or not the proposed solution is appropriate for these scenarios.

Final schedules and planning for the trials will be confirmed by trial partners in WP6.

3.1.4 Data to be collected

In connection with the trials, three types of data are collected and shared as summarised here:

TRIAL DATA / RESULT	CONSENT REQUIREMENT	COMMENTS
PERSONAL DATA (participant contact details)	Requires consent	Held solely by the individual trial partner and not shared with other partners. Summary (anonymised) demographic information may be provided in the relevant deliverables.
TECHNICAL EVALUATION	Does not require consent. This is not personal data.	Shared with the consortium, especially the technical partners. These data will be used solely to evaluate the technical quality of the platform. They may be published in relevant deliverables.
QUALITATIVE FEEDBACK	Does not require consent. This is not personal data, unless this involves audio recording	Shared with the consortium, and published in summary form in relevant deliverables and potential publications. Audio data may pose a specific challenge. See Chapter 4 below.

Table 3: trial Information and its Ethical Treatment

As can be seen here, *personal data* is restricted both in type (it includes only contact details) and how it is shared in the project. Other data are simply related to the evaluation of the technical features of the proposed solution, and of the suitability of the solution to the specific domain (cross-jurisdiction sensitive personal data management).

3.1.5 Legal basis for processing

Only the collection and retention of *personal data* require specific and explicit consent, that is a legal basis for processing. Nonetheless, there is a need in the trials to get participant consent to take part in the role-play and evaluation activities themselves. This is a research ethics requirement.

3.1.5.1 Data management

Different types of data require different types of curation and management. These are summarised in the following list:

- *Participant information*: these data, i.e., the contact data for those taking part, will be held securely at the respective partner sites only.

- *Simulated EHR*: For cross-border medical care, the data involved will be based on the medical information included in the *minimum patient summary dataset* described in epSOS project[11] and some wearable and health related mobile data. During pilot

[11] http://www.epsos.eu/

validation, a **synthetic data set** will be created. This dataset will be based on commonly encountered patterns of illness which may then be associated with fictitious patients.

The minimum patient summary[12] is defined from a clinical perspective and bearing in mind the medical viewpoint of the final users (medical doctors and patients). This will be included in **Electronic Health Records** (EHR) that will constitute the complete set of patient data to be exchanged across borders. The patient EHR, by definition, includes all the health information necessary to provide an overview of the patient's medical history. It comprises different kinds of data, both structured and unstructured.

Examples of the possible data collected during patient's life include:

- **Structured Data**
  - Medial discharge form after hospitalization
  - ED (emergency department) data set
  - Medical Images
  - Treatment forms
  - Constant collection forms.

- **Unstructured Data**

  - Medical doctor diagnoses
  - Medications
  - Allergies
  - Radiology images
  - Lab and test results
  - Medical histories & Progress notes
  - Reports of complementary tests (radiology, pathological anatomy, endoscopy, etc.)
  - Discharge letter
  - Monitoring of evolutions in external consultations.

The unstructured data are usually, but not exclusively, uploaded in PDF format. As simulated data, there is no requirement for secure handling. However, in as much as these are useful data to test specific health challenges, then these simulated data could be shared across the research community.

- *Qualitative feedback*: except where audio and transcriptions are used (see Chapter 4 below), the qualitative data will be summarised and shared across the consortium, but also with the broader research community as part of the broader dissemination activities of the project.

As outlined in Section 3.1.4 above, each of these data types will be separately handled.

[12] http://ec.europa.eu/health/sites/health/files/ehealth/docs/guidelines_patient_summary_en.pdf

3.2 "Break Glass" Scenario

The first of the three scenarios to be covered in the trials involves the situation where a patient is not in a position to give consent, yet needs to be treated. This has implications as outlined here.

3.2.1 Scenario Description

A tourist is travelling abroad and is taken ill, with a life-threatening risk, which involves them falling unconscious. Local medical professions need to access the home medical records of the tourist for effective and secure diagnosis and treatment.

3.2.2 Ethical considerations

This scenario throws up the issue where legal requirements data protection as illustrated in the GDPR [4]) must be carefully interpreted. Since consent of any kind from the data subject is not possible, then the vital interests of that individual must be invoked to access the appropriate sensitive personal data. Alternatively, if the equivalent of a (medical) power of attorney exists, then the other party may be approached for consent.

3.2.3 Legal requirements

If consent is not available as the legal basis for process, the vital rights of the patient must be invoked. Any technology involved here – i.e., the SHiELD solution – must provide an audit trial to demonstrate this.

3.3 Surgical Follow-up

In the second scenario, additional personal data is required. However, it may not be possible to provide a complete list of what is required in advance of the sensitive personal data access request, since the local medical team may not know in advance what is and is not relevant for their treatment of the patient.

3.3.1 Scenario Description

A patient who has undergone a recent surgical procedure wishes to travel abroad. On departure, they take information with them which they hope will help if needed. When away, complications develop. Local medical professionals need access not only to the patient medical record, but also specific detail of the procedure that was carried out.

3.3.2 Ethical considerations

Consent is possible here, since the patient is aware of the motivation for providing access. However, informed / explicit consent is more problematic since the medical team may not know in advance what they are looking for or even why they are looking for it in the personal data of the data subject.

3.3.3 Legal requirements

Consent can only form part of the legal basis for processing here. This may be invoked along with the vital interests of the data subject. To ensure compliance, the SHiELD solution will need to provide appropriate reporting and audit capabilities such that a record is maintained of any records accessed.

3.4 Remote monitoring of an ongoing, chronic condition

The final scenario involves the case where monitoring data collected as part of routine medical care as opposed to more permanent, traditional EHRs. These data may be useful in support of an appropriate diagnosis and appropriate treatment for a patient presenting locally who is suffering an exacerbation of a chronic condition.

3.4.1 Scenario Description

A patient with a chronic condition, involving regular monitoring, is travelling. They fall ill, including an exacerbation of their condition, and seek medical help. Local medical professionals not only want access to the patient's medical records but also the data from any monitoring device being used in support of the patient's medical condition.

3.4.2 Ethical considerations

The data controller and/or processor may not allow access to the data to a third party. Overriding any such conditions may have to be done for the vital interests of the patient.

3.4.3 Legal requirements

Overriding the terms imposed by any monitoring device supplier may require complex negotiation between multiple parties. SHiELD may need to maintain a record of the current status of such discussions to allow local medical professionals to keep abreast of what is happening.

4 Ethical issues

As outlined in the previous chapter, the main ethical issue involves the balance between standard procedures for access and processing of (sensitive) personal data where explicit and informed consent are sought and the vital interests of the patient needed local treatment when travelling to another member state. The SHiELD offering can provide certain technical features around data access monitoring, provenance and access attempts / requests. But part of the qualitative feedback to be requested from participants in the trials, participants will be asked to comment on:

a) How they perceive this balance;
b) How best to ensure that appropriate measures are taken to protect the patient.

Such feedback will add to the debate surrounding the ethical treatment of sensitive personal data within a healthcare environment.

5 Requirements

In respect of explicit and informed consent, participants are expected to be given a consent form and detailed information sheets explaining what data will be accessed, why and how they will be used. Such consent and information sheets should:

- be written in a language and in terms the data subject can fully understand
- describe the aims, methods and implications of the research, the nature of the participation and any benefits, risks or discomfort that might ensue

- explicitly state that participation is voluntary and that anyone has the right to refuse to participate and to withdraw their participation, samples or data at any time —without any consequences

In addition, and if relevant, such forms would also:

- State how biological samples and data will be collected, protected during the project and either destroyed or reused subsequently
- State what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings)

The consent and participant information sheets suggested in respect of the default research protocol above are appended in the D8.1 GEN Requirement no1 (Thical application proformas).

In addition, and in passing in third subsection of each of the sections in Chapter 3 above, specific technical requirements in very broad-stroke descriptive terms are listed.

6 Ethical approvals

Ethical approval is required for the trials in cases where personal data are collected (i.e., participants' contact details), as well as from a research ethics perspective, where individuals are recruited to take part in the role-play scenarios. For the contact details (personal data), since these are restricted solely to the local trial partner organisation and not shared with the rest of the consortium, no approval is needed beyond compliance with data protection laws in the respective jurisdictions. However, for research ethics and participants taking part in the role play of each if the scenarios mentioned above, ethical approval is required.

6.1 General ethical approval

For the default research protocol described above (Section 3.1), ethical approval has been sought through the Faculty of Physical Science and Engineering at the University of Southampton. The documents submitted along with the approval from the Faculty Ethics Committee are reproduced in D8.1 GEN Requirement no1 (Ethical application proformas). This approval will cover role-play trials across partner member states for the duration of the SHiELD project so long as they adhere to the default research protocol. Further, the University of Southampton is registered with the UK DPA for the processing of *research data*, that is the evaluation and qualitative data resulting from the trials. This general ethical approval therefore provides a basis and mechanism to run initial exploratory work as part of the planning and execution of the use case trials in WP6.

6.2 Additional trial specific approvals

Any deviation from or extension to the default research protocol that individual trial partners may wish to do, *either* as a result of running the default protocol *or* because they wish to cover other aspects of cross-jurisdiction medical data sharing, will require additional approval. This will be discussed with the SHiELD EtC on an on-demand basis as and if required during the project.

In addition, where different local requirements are in place (for example in the Basque Region), or where there is any departure from the default research protocol suggested, then local approval will have to be sought in addition to this general approval. This will be

developed further in WP6. However, the initial approval here may prove useful as an example for the creation of more specific applications which may be required locally.

7 Conclusions

This report has introduced the trials planned to demonstrate the technical completeness and acceptability of the SHiELD offerings. The main focus has been on the specifically *ethical* issues associated with running trials in the healthcare domain. As such, the ethical principles and framework has been described which provides the foundation for developing the trial protocols and assessing their ethical appropriateness. The deliverable also outlines specific issues and challenges associated with a default research protocol that might be applicable along with the specific scenarios to be used to test the appropriateness of the SHiELD solution. The issues and challenges identified provide useful input to the trials themselves in WP6, but also provide a base for the technical partners to consider what they are developing.

Against that background, an initial ethical application has been submitted for research ethics approval on the basis of the default research protocol outlined. Such approval provides two benefits:

1. It acts as a baseline and example which might be used to seek more specific approval for individual trials, customised to local requirements;
2. It provides an umbrella approval from a research ethics perspective to cover an initial exploratory work.

This deliverable is therefore an important part of the overall planning for SHiELD. Together with the data management plan (D1.5) and the initial legal requirements (D3.1), this provides the project management team with a comprehensive framework for appropriate governance of the work planned during the project.

8 References

1. ALLEA, “The European Code of Conduct for Research Integrity,” *Book The European Code of Conduct for Research Integrity*, Series The European Code of Conduct for Research Integrity, Revised Edition ed., Editor ed.^eds., Allea.org, 2017, pp.
2. APA, *Ethical Principles of Psychologists and Code of Conduct*, American Psychological Association, 2010.
3. BPS, *Code of Human Research Ethics*, The British Psychological Society, 2014.
4. European Commission, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016,” 2016.
5. Information Commissioner's Office, “Key Definitions of the Data Protection Act,” n.d.
6. European Commission, “DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” 1995.