PARTNER
Grant Agreement Number 215840

WP22/WP23 – Deliverable 2 - 06/2010

Ethical and Legal Requirements for HISP Services

Faustin Laurentiu Roman (WP22)

Supervisors:
Prof. Manjit Dosanjh (CERN),
Prof. Jose Bernabeu (IFIC)

Daniel Abler (WP23)

Supervisors:
Prof. Manjit Dosanjh (CERN),
Prof. Ken Peach (PTCRi, University of Oxford),
Prof. Jim Davies (Computing Laboratory, University of Oxford)

Date 09.07.2010
PARTNER Work Package 22 and 23, Deliverable 2

Services of the Hadrontherapy Information Sharing Platform. Legal and Ethical implications.

Faustin Laurentiu Roman (WP22), Daniel Abler (WP23)

Faustin.Roman@cern.ch
Daniel.Abler@cern.ch

June 2010
This is a common report of the PARTNER Work Package 22 and 23 Deliverable 2 within the Marie Curie Initial Training Fellowship of the European Community’s Seventh Framework Programme under contract number PITN-GA-2008-215840-PARTNER.
# Contents

1 Introduction ................................................. 1  
1.1 e-Health ................................................. 1  
1.2 Hadrontherapy Information Sharing Platform ............... 1  
1.3 Storyline ................................................. 3  
1.4 Report Scope and Structure .................................. 4  

2 Ethics ....................................................... 6  
2.1 Introduction ................................................. 6  
2.1.1 Medical Ethics ........................................... 6  
2.1.2 Research Ethics ............................................ 7  
2.2 Privacy and Confidentiality ................................... 8  
2.2.1 Privacy .................................................. 8  
2.2.2 Confidentiality ............................................ 8  
2.2.3 Breaches of Privacy and Confidentiality .................. 9  
2.3 Free and Informed Consent ................................... 10  
2.3.1 Broad consent for Biobank Research ..................... 11  

3 Law .......................................................... 13  
3.1 European Legislation ........................................ 13  
3.1.1 Directive 95/46/EC on European data protection ......... 13  
3.1.2 Directive 2007/47/EC on medical devices .................. 15  
3.1.3 Directive 2002/58/EC on e-Privacy ......................... 15  
3.1.4 Recommendation on cross-border interoperability of electronic health record systems .......................... 16  
3.2 Country-specific Legal Considerations ......................... 17  

4 HISP Environment ............................................ 19  
4.1 Scenarios .................................................. 19  
4.1.1 Patient Referral .......................................... 19  
4.1.2 Research .................................................. 20  
4.2 HISP Services ............................................... 21
## Contents

4.2.1 Communication ................................................. 22
4.2.2 Logging ....................................................... 22
4.2.3 Agreement .................................................... 22
4.2.4 Authentication and Authorisation .......................... 23
4.2.5 Data Import .................................................. 23
4.2.6 Metadata ..................................................... 23
4.2.7 Data Access ................................................. 24
4.2.8 Data Analysis * ............................................. 25

4.3 Conclusions ...................................................... 25
   4.3.1 Patient Referral ........................................ 25
   4.3.2 Research .................................................. 26

Bibliography .................................................. 28
Abstract

This report covers the second Deliverable of PARTNER WP 22 and WP 23. We discuss the legal and ethical considerations with regard to collaborative applications in Particle Therapy, namely patient referral and medical research. Following the storyline of a cancer patient we developed two scenarios where we give an overview of the services and functionalities of the Hadrontherapy Information Sharing Platform (HISP). We introduce ethical and legal aspects applied to medicine and research and we conclude on the implications and constraints for the HISP services.

Faustin Laurentiu Roman

Supervisors:
Prof. Manjit Dosanjh manjit.dosanjh@cern.ch CERN
Prof. Jose Bernabeu bernabeu@ific.uv.es IFIC

Co-Supervisors:
Dr. Jose Salt Cairols salt@ific.uv.es IFIC
Dr. Gabriel Amoros amoros@ific.uv.es IFIC

Daniel Abler

Supervisors
Prof. Manjit Dosanjh manjit.dosanjh@cern.ch CERN
Prof. Ken Peach k.peach1@physics.ox.ac.uk University of Oxford, PTCRi
Prof. Jim Davies jim.davies@comlab.ox.ac.uk University of Oxford, Computing Laboratory

This is a common report of the PARTNER Work Package 22 and 23 Deliverable 2 within the Marie Curie Initial Training Fellowship of the European Community’s...
Contents

Seventh Framework Programme under contract number PITN-GA-2008-215840-PARTNER.
1 Introduction

1.1 e-Health

Interoperability of systems and secure information sharing across institutional boundaries nationally and even internationally is an important topic in e-Health, and considerable efforts have been made in several projects to face these challenges [1]. Extending a domestic system across borders means that separate IT systems with different technologies must be interfaced. Any problems arising from this are, however, usually limited to designing a proper technical and financially affordable solution. However, challenges other than technical ones have to be considered as well:

- Organisational issues, including users’ training and uptake
- Regulatory issues, including accreditation and certification
- Legal issues, including personal data protection, reimbursement, liability.

The advantages of a pan-European electronic data sharing system for the Particle Therapy community are:

- Faster access to patient history and less duplication of medical acts
- Improved diagnostic and treatment information
- Better quality of life for the patient: less waiting times, travelling and hospital bed days
- Access to geographically distributed research data

1.2 Hadrontherapy Information Sharing Platform

Work packages (WP) 22 and 23 within the PARTNER FP7 project aim to build a prototype of such an e-Health infrastructure for the hadrontherapy community: the Hadrontherapy Information Sharing Platform (HISP).
1 Introduction

Figure 1.1: Conceptual layout of the PARTNER Hadrontherapy Information Sharing Platform (HISP) as presented at the Physics for Health in Europe workshop in February 2010. [4]

The HISP conceptual architecture (Fig. 1.1) consists of a common access point to heterogeneous data sources using secure grid services. A rare tumour database (RTDB), provided by PARTNER WP 24, will access HISP to provide a view on rare tumours. HISP will give researchers and clinicians a tool for medical data sharing, clinical analyses and epidemiological studies while RTDB will support modelling of cancer treatment outcome and indications for hadrontherapy.

The relevance of information sharing to hadrontherapy and technical challenges have been discussed in the PARTNER Deliverable 1 of WP 22 [2] and WP 23 [3].

The following section illustrates how the advantages of a collaborative tool like HISP could manifest in the daily routine of the patient, the medical doctor and the researcher by telling the story of a cancer patient¹.

¹The storyline is based on realistic scenarios (with the help of Dr. Bleddyn Jones and Dr. Raj Jena), however, adapted to illustrate the added value of a collaborative tool like HISP.
1 Introduction

Figure 1.2: Example of chondrosarcoma:
(left) A large bright lesion on MRI in the lumbar epidural space of a four year old patient who presented with pain and refusal to walk. The white arrow points to the edge of the mass.
(right) Shows a spinal MRI the same patient two years later, having completed surgery, radiation therapy and chemotherapy.
Pictures taken from: http://sarcomahelp.org/learning_center/mesenchymal_chondrosarcoma.html

1.3 Storyline

Mr. X sees his general practitioner (GP) because of backpain around the spine. The GP diagnoses early spinal compression, suspects a cancer close to the spine responsible for the pain and sends Mr. X to the local city hospital. A CT scan reveals that Mr. X has a tumour of the vertebral bone with some displacement of the spinal cord. A multidisciplinary team (MDT) decides that Mr. X should first undergo surgery which aims to excise as much of the tumour as possible in order to decompress the spine and to establish a diagnosis. A pathological examination confirms that the tumour is a low grade Chondrosarcoma (figure 1.2).

Since Chondrosarcoma requires multiple treatment modalities, Mr. X would like to weight the various options. Mr. X’s information is inserted into the PARTNER Hadrontherapy Information Sharing Platform (HISP), an information system connecting cancer centres. HISP matches patient data to an existing database on treatments and suggests that Mr. X has chances to benefit from Particle Therapy (PT).

Two options are therefore offered by the Oncologist to Mr. X, either post-operative radiotherapy by X-rays in the UK or PT abroad. Mr. X decides for the PT treatment.
This decision needs to be approved by a national MDT for PT referrals: the patient record of Mr. X therefore needs to be made available to the members of the referral panel.

The referral panel analyses the case using HISP and a decision is taken: Mr. X can now be referred to a PT centre.

Similarly, a request is issued to the PT centre abroad to review Mr. X’s case. Based on the clinical details and imaging information available in HISP, the PT centre also accepts Mr. X and enrolls him in their running clinical trial on Chondrosarcoma.

Both reviewing processes only took a few days because HISP made the patient data instantly available to the different parties and supported the negotiation between the centres.

After the treatment the patient returns to the UK and in order to monitor the treatment outcome, Mr. X undergoes follow-up examinations. Mr. X’s case history is reviewed collaboratively by the local doctor, experts in the city hospital and the PT centre using HISP.

At the same time, Dr. W, a radiation biologist wants to corroborate her work on the $\alpha/\beta$ ratio for low grade Chondrosarcoma cells. She has performed initial experiments using clonogenic survival assays to determine the radiation sensitivity of this cell line to 250kV X-rays. Her findings suggest a possible role for hypofractionated therapy with protons or higher LET species, as e.g. carbon ions. Although several centres are running clinical trials with Chondrosarcoma patients, like Mr. X, none of these centres has accumulated sufficient data for Dr. W’s hypothesis to be tested since Chondrosarcoma is a rare cancer. Dr. W would need to collect information about Chondrosarcoma patients over the last years from a number of European PT centres.

Dr. W finds relevant data available in the rare tumor database, a service of HISP, submits a research proposal and asks for data access for her study. Dr. W’s proposal is accepted, she runs the proposed analysis and finds her assumption confirmed. A new cancer management strategy emerges from this study, from which patients like Mr. X will profit in the future.

### 1.4 Report Scope and Structure

Mr. X personal data being processed for clinical and research purposes raises ethical and legal concerns.

The scope of this report is to discuss the legal and ethical considerations with regard to collaborative applications in Particle Therapy, namely patient referral and medical research.

This report covers the second PARTNER deliverable for WP 22 and WP 23:

“Inventory of all applications (common elements) to be used collaboratively and stating explicitly the underlying European regulations, together with the other student and in consultation with centres of the PARTNER consortium.”
1 Introduction

Since only one of the emerging PT centres in the EU, HIT, has started treating patients\(^2\), the applications were derived from brainstorming discussions among the PARTNER WP 22, 23 and 24 research groups\(^3\).

The storyline in section 1.3 gives a rough overview of the functionality of the Hadrontherapy Information Sharing Platform (HISP). For implementing these functionalities, not only technical challenges have to be overcome, also the ethical and legal requirements need to be taken into consideration.

Chapter 2 briefly introduces ethics applied to medicine and research and explains important concepts like privacy, confidentiality and consent. Chapter 3 summarises relevant European Directives and their national implementation.

Based on the storyline, chapter 4 develops two detailed scenarios for patient referral and research. From these scenarios a set of services is derived, section 4.2. Section 4.3 concludes on the legal and ethical constraints for HISP.

\(^2\)http://cerncourier.com/cws/article/cern/40999
\(^3\)Thanks to: Manjit Dosanjh, Ken Peach, Bleddyn Jones, Ramona Mayer, Jim Davies, Gabriel Amorós, Jose Salt Cairols, Norman Kirkby, Karen Kirkby, Raj Jena, Steve Harris, Patricia Méndez Lorenzo, Massimo Lamanna, Jamie Shiers, and Vassiliki Kanellopoulos
2 Ethics

2.1 Introduction

Ethics, or moral philosophy, involves systematising, defending, and recommending concepts of right and wrong behaviour. Ethical theories can be divided into three general subject areas: meta-ethics, normative ethics, and applied ethics [5]. Meta-ethics concerns the nature of moral statements, normative ethics concerns what people should believe to be right or wrong and applied ethics examines specific controversial issues in private and public life from a moral standpoint. Two branches of applied ethics need to be considered in the context of the PARTNER platform: medical ethics (section 2.1.1) and research ethics (2.1.2). The following section will give a brief introduction into these topics and to explain concepts like privacy and confidentiality (section 2.2) and their relevance to the PARTNER platform.

Medical and research ethics are based on fundamental ethical values. These values do not describe how to handle a particular situation, rather they provide a framework for dealing with conflicts. Especially relevant are the values of autonomy, dignity and respect for persons.

Autonomy recognises the capacity of individuals to make decisions about themselves. Dignity gives (human) beings an innate right to respect and ethical treatment. Respect for persons is the acceptance of an individual without judging him/her, e.g. his/her values, behaviours or lifestyle.

2.1.1 Medical Ethics

Western medical ethics can be traced back to guidelines on the duty of physicians in antiquity, such as the Hippocratic Oath. The oath gives guidelines on the conduct and duties of doctors in the relation to their patients. While medical ethics discusses many aspects of patient care, in relation to the PARTNER platform we are only concerned with the aspect of keeping the confidentiality of the patient-doctor relation and thus ensuring the patient’s privacy.

In terms of the Hippocratic Oath [6]:

... And about whatever I may see or hear in treatment, or even without treatment, in the life of human beings - things that should not ever be blurted out outside - I will remain silent, holding
such things to be unutterable [sacred, not to be divulged] ...

A trust relationship is created when individuals voluntarily seek advice or treatment from the doctor and have the expectation that their communication will be treated confidentially\(^1\). This expectation does not need to be explicitly expressed, it is implied by the circumstances.

The oath, however, does not define what “should not ever be blurted out outside”. The physician is left with the decision to decide what has to be kept secret and what not. The directive therefore has been understood to mean that only if, in the physician’s professional opinion, disclosure of patient’s confidential information is of best interest for this patient, the physician is allowed to disclose patient information without violating the oath \(^7\). This is the case when a healthcare team discusses a patient’s case in a MDT meeting or if patient’s information is reviewed by a panel prior to referral. In both cases, the disclosure of information serves the patient’s benefit in the sense that the patient may expect the most appropriate treatment as an outcome of the discussion and reviews.

2.1.2 Research Ethics

Research ethics applies fundamental ethical principles, like autonomy, dignity and respect for persons (see section 2.1) to the conduct of research. Research ethics is especially developed in the context of medical research and in social sciences where the interest of individuals has to be taken into account when conducting a study.

While medical treatment should aim at directly contributing to the health of the patient, research in general aims to generate new information, knowledge and understanding by means of systematic investigation of a subject \(^8\).

Assuming that scientific research benefits all humans, research participants might have a common interest in research activities being pursued. Participation in research may involve costs and risks to the research participants and other individuals. In addition to this, the beneficial outcome of a piece of research is often uncertain. The instrumentation of research subjects in research becomes morally objectionable only when there is a form of exploitation of the individual, i.e. when the autonomy of the individual is not respected or when their well-being is negatively affected \(^9\).

The above principles not only apply to clinical research but also to research involving data and biological materials collected from patients. The principle of autonomy demands the subject to be informed about the experiment and about the usage of

\(^1\) Although the origin of modern medical ethics of respect for the confidentiality of medical information may be traced to this passage, it needs to be mentioned that our idea of confidential medical care did not exist in ancient Greece: Physicians examined and treated patients in public or houses while being watched by relatives and strangers; male guardians or owners were entitled to medical information about women, children and slaves and could even dictate medical choices.

The original meaning of the passage probably refers to the safeguarding of a particular set of information: not the patient’s name and treatment should be kept secret but rather the patient’s history and circumstances of living which could be used to dishonour the patient in public life.\(^6\)
information gained in the experiment. According to international standards, informed consent is therefore required for collecting, storing, and using human biological material such as tissue, blood, or DNA and data processed from tissue.

Ethical decision-making is generally complex, so that an individual researcher may not be able to decide about the ethical issues involved in a research project. A group of scientific and ethical experts is usually better placed to make a good decision about the ethical legitimacy of an action and to take the society’s plurality of ethical views into account. Research Ethics Committees (REC) have been established to review research involving human participants. Within the EU, such a review is obligatory for clinical trials by the Directive 2001/20/EC [10].

The following sections explore the notion of privacy and confidentiality towards patients and illustrate their meaning in the context of informed consent.

### 2.2 Privacy and Confidentiality

Ethical duties (referring to privacy and confidentiality) are frequently formalised in laws (section 3.1), however, they may go beyond legal requirements.

#### 2.2.1 Privacy

Privacy, in a contemporary interpretation, concerns the protection of personal information. Not only should others be prevented from gaining access to personal information but also each person should maintain control over their own information, even if this information is stored elsewhere.

There had been attempts to formalise the ethical concept of privacy into a legal concept. Documents like the Universal Declaration of Human Rights and the European Convention on Human Rights, and legal documents like the European Data Protection act (see section 3.1) identify aspects of life in which privacy is typically applied but these documents do not fully define its scope.

Breaching privacy results in threats to the individual’s ability to make their own choices and gives the possibility of being taken advantage of by others.

#### 2.2.2 Confidentiality

Respecting confidentiality, can be considered as a contract, either explicit or implicit, to keep the promise not to disclose information of a person which this person considers secret. Often in professional relations, private information is assumed to be treated confidentially. The researcher therefore would need to state the use of that information explicitly before receiving it in order not to be bound to the duty of confidentiality. Confidentiality is purely linked to information and only certain relationships or agreements demand confidentiality, whereas the duty to respect others’ privacy is more general. A breach of confidentiality would be a violation of the informational aspect of privacy.
Confidentiality protects the interest of a person to stay in control of their personal information.

While respect for privacy constrains researchers in the ways in which they acquire information, confidentiality refers to the way already existing information is treated.

Confidentiality is not an absolute duty. One ethical reason for maintaining confidentiality is to respect the autonomy of the person, but it may be overridden by other considerations, for example the legal obligation to disclose information when there is a risk of serious harm to others.

If information is to an institution rather than an individual, confidentiality would not be broken by disseminating the information within this institution. However, this has to be made clear to the information suppliers, e.g. patients, in order not to reveal information which they expect only to be revealed to the healthcare team. If no details about the use of information are stated explicitly, the agreement on which the information was provided (and therefore the recipient’s moral obligations in handling it) would be defined by the expectations of the information supplier.

2.2.3 Breaches of Privacy and Confidentiality

Some research situations may (ethically) require to breach confidentiality and to pass on relevant information to third parties. This can occur in the following situations:

1. The law requires it.
2. Breaching confidentiality is permissible by law but not required.

While the first case usually occurs when there is tension between confidentiality and public safety, the second case tends to apply to situations which involve weighing up of potential harms and interests, for example a strong public interest.

Two strategies allow to preserve confidentiality in those cases:

1. The third party seeks consent of the subject.
2. The information is anonymised.

A basic mean of ensuring that privacy-breaking methods of data collection or confidentiality-breaking methods of data dissemination are ethically acceptable is to obtain consent of the individuals involved (strategy 1). The connection between individual and information is maintained. However, passing the information to the third person is not regarded as a breach of confidentiality since the subject has agreed with this and the subject keeps the control of its information. Obtaining consent is not always possible, because e.g. the person is not competent, because the study reveals information not only about the subject but also about others (as is the case in genetic studies), or simply because the contact details may not be available or the number of participants in a study is too large. If obtaining consent is not possible, it is important to know how strong the obligation is to protect privacy. This depends on the kind of invasion into
the person’s privacy and if measures can be put in place which ensure minimising the consequences of breaches of privacy.

Preserving the anonymity of research subjects (strategy 2), is an important way of dealing with breaches of privacy. However, this dissemination technique also has limitations. Anonymisation does not account for people’s interest in controlling information about themselves, and in the case of health or genetic information, also about close family members. The initial anonymisation process should be done by a person who is entitled to access the data, otherwise a (small) breach of confidentiality will have occurred. After anonymisation, individuals may still be identifiable from the remaining data, for example in very localised studies or when dealing with rare conditions.

Anonymisation of data makes it harder to cross-check results for errors or scientific fraud. Untraceable data raises other ethical problems, e.g. members of the study group cannot profit from research outcomes.

The compromise solution often is to use coded data. In this case, the identifying information is removed from the dataset and a key allows to link the identifying information back to the dataset. The identifying information has to be securely stored and the circumstances under which it may be accessed have to be considered in advance by the researchers.

Many countries have legal requirements relating to confidentiality and the revealing of personal information. The data protection act as part of the EU Charter of Fundamental Rights [11] lays out guidelines for the processing of any information relating to identifiable living individuals and the restriction of its use to specific purposes. The implementation in national laws varies from country to country, see section 3.2.

2.3 Free and Informed Consent

Free and informed consent is “any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed”. [12]

For the consent to be valid (also known as free and informed consent) it must be based on adequate and accurate information and be given voluntarily by a competent person who must be able to understand the implications of their consent.

The recruiting process into a study therefore must provide adequate quantity and quality of information which discloses all relevant information to the potential participant in an understandable way without overloading him or her with scientific/technical details.

The patient needs to be free to decide about his participation in research. Coercion hopefully will rarely be applied, but inducements (monetary, or other rewards) may be used to manipulate a person’s decision. These have to be avoided in order to assure a voluntary participation.
Competence implies that the person giving consent has the mental capability to understand the information he received. Although persons seem mentally competent, the situation (and their psychological or physical condition) in which they have to take the decision (e.g. terminal illness) may have made them vulnerable\(^2\) and therefore incapable of protecting their own interest. Vulnerable persons are at higher risk to be harmed or exploited than other persons would be in a similar situation since they are less able to protect themselves.

Consent from any human participant is necessary for conducting research in an ethical way. The need for informed consent for research follows from more fundamental ethical principals, among these the respect for autonomy, dignity and persons. These “respect principles” imply that interfering with a person, be it for medical treatment, research or other purposes without his/her consent would be wrong.

Documents of different status (professional associations, treaties with or without direct legal force) agree on the importance of consent especially in biomedical research ethics, e.g. in article five of “Convention for the Protection of Human Rights and Dignity with regard to the Application of Biology and Medicine” of the council of Europe:

> “An intervention in the health field may only be carried out after the person concerned has given free and informed consent to it. This person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. The person concerned may freely withdraw consent at any time.”\(^{[14]}\)

### 2.3.1 Broad consent for Biobank Research

Biobanks are repositories for various human biological material, e.g. DNA, tissues, tumour samples and blood. Also, they can contain clinical data of the donors in order to maximise the potential for useful patient-related research. Since the usual model of consent is related to a specific research project, it requires consent to be sought when the samples are passed on to a different group of researchers. Considering the number of donors who might be involved in a biobank, their usefulness would be seriously limited if this model were applied here. Therefore a broad consent model is applied to biobanks.

Broad consent requires the participants to agree for their data to be used in different research projects, carried out by different researchers and in different contexts. Broad consent (unlike open consent which is understood as consent to the unrestricted use of data) is therefore based on information about the kinds of research that will be conducted.

When individuals give broad consent to the use of their samples or data in future research, they are giving permission for someone else to decide how to use that sample or data on their behalf. Typically a ERC decides about the usage of the accumulated data for independent research projects. Disclosing the governance arrangements (of a Biobank) is an important part of the broad consent.

\(^{2}\)The Council for International Organisations of Medical Sciences defines “vulnerable persons” as “those who are relatively (or absolutely) incapable of protecting their own interests”.\(^{[13]}\)
It can be argued that this form of consent lacks specific information about the particular use of the samples and therefore cannot be autonomous. However, in practice the model of broad consent is justified by pointing out the potential benefits the research can offer.

(Anonymous) [15] see broad consent as ethically valid and recommended it for biobank research, “provided that personal information related to the research is handled safely, that donors of biological samples are granted the right to withdraw consent, and that every new study is approved by the ethics-review board”.

A number of ethical concerns have been brought forward against the broad consent used in biobanks (e.g. (Anonymous) [16]):

- **Withdrawal** from particular research projects is **hardly possible** for the donor because the data is used in many different research projects. Also, persons who have given broad consent must know that they are enrolled in a study. It may not be possible to keep people up-to-date about ongoing research projects carried out by their biobank.

- In order to adequately (safely) handle confident information, the value of this information must be known. However in many cases it is not clear if a particular information is going to be harmful or not or if it may make anonymised/coded information identifiable.

- **Anonymisation** of the samples would reduce the harm of security breaches, however the donors would then **lose the control over their data** completely and would not be able to protect their own interests regarding the usage of their data. **Coding** the data may be a compromise which also keeps the possibility of providing feedback of findings. However, **breaches of security** would then still **affect privacy and confidentiality**.

- Some ERCs may not be competent for biobank research since they are too eager to promote research.
3 Law

European citizens should be able to move freely through all Member States, which requires services that extend beyond national borders while ensuring that legal and ethical rights are preserved. This chapter presents the legal framework governing the cross-border electronic medical data exchange in Europe. The entire system, its participants, components and processes are governed by a similar set of laws and regulations.

Legislation ranges from general regulations on the handling of personal data, e.g. European Data Protection Directive to regulations regarding specific services, e.g. Directive concerning medical devices, and finally to national and local implementations of laws.

First we give an introduction to the EU laws applicable to our domain which represent the basic environment and the base of more specialised national laws. Next we describe some particularities of national laws.

3.1 European Legislation

3.1.1 Directive 95/46/EC on European data protection

The European Data Protection Directive 95/46/EC concerns the protection of individuals with regard to the processing of personal data and on the free movement of such data [12]. The base of this Directive is that Member States are required to ensure the rights and freedoms of natural persons with regard to the processing of personal data, and in particular their right to privacy, in order to ensure the free flow of personal data in the European Community.

This Directive contains the definitions, rules and roles involved in personal data sharing across borders within and outside European Economic Area (EEA). While the Directive was designed for EU countries, now its coverage has been extended to a number of third countries², e.g. Switzerland, Canada, US.

---

¹Data Protection in Europe: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm
²Agreement on data sharing with third countries
Directive 95/46/EC defines **personal data** as any information relating to an identified or identifiable natural person which is called a **data subject**. In addition, **sensitive data** means data revealing race or ethnic origin, political opinions, religious or philosophical belief, trade-union membership, health or sexual life.

This Directive does not apply to **anonymous data** as stated in Recital 26: “the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable”. A definition of **pseudoanonymised data** is not mentioned in the Directive.

**Data processing** is defined as any **set of operations performed upon personal data**, whether or not by automatic means, e.g. collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. Data has to be **fairly and lawfully processed and kept no longer than necessary**. The processing has to be **adequate, relevant and not excessive, accurate, secure** regarding the purposes of collection or of further processing. Also data is to be transferred only to countries with adequate protection. The **rules of fair processing** are that so far as practicable, and subject to exemptions, data subjects should be provided with certain information at the time of collection or as soon as practicable thereafter, so that they understand why and how their data are being processed.

Thus, **processing of personal data, especially sensitive data**[^1], is prohibited by **default** except for the following situations:

- **clinical usage by health professional** with obligation of secrecy
- **having the data subject's consent**: any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.
- **acting on the basis of a contract involving the data subject**
- **protecting the vital interest of the data subject** or another person when the data subject is physically or legally incapable of giving consent
- **data manifestly made public or where there are legal claims**

In processing data several **roles** are defined:

- Data subject mentioned before.
- **The controller** determines the purposes and means of the processing of personal data following laws or regulations. Data controllers also must implement appropriate technical measures for data protection ensuring a level of security conform with the risk associated with data processing methods and nature.
- **The processor** processes personal data on behalf of the controller and

[^1]: Sensitive data is treated more strict than personal data thus processing is more complicated
a **third party** is the entity other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data.

- **The recipient** is to whom data are disclosed, whether a third party or not.

The data subject has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

A follow-up on the Data Protection Directive appears to be needed as many EU reports states[^1], e.g. 17. Two obvious aspects that need to be addressed are anonymised and pseudo-anonymised data, these aspects being of importance for the research domain in which the PARTNER Platform will function.

As Directive 95/46/EC concerns **only personal data** the applicability scope of this law for PARTNER Platform is described in section 4.3 in connection to the patient referral system, and considering the procedures associated with the anonymisation process for the research scenario.

### 3.1.2 Directive 2007/47/EC on medical devices

Directive 2007/47/EC amends several Directives relating to general and active implantable medical devices[^18]. The following concepts are defined in the context of this Directive:

A **medical device** is defined as any instrument, apparatus, appliance, **software**, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:

- **diagnosis, prevention**, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
- **investigation**, replacement or modification of the anatomy or of a physiological process,
- control of conception

The PARTNER Platform may fall in the definitions of Directive 07/47/EC and the implications are discussed in section 4.3.

### 3.1.3 Directive 2002/58/EC on e-Privacy

Directive 2002/58/EC on Privacy and Electronic Communications concerning the processing of personal data and the protection of privacy in the electronic communications

sector [19]complements Directive 95/46/EC by dealing with aspects such as confidentiality of information and treatment of traffic data.

The first general obligation in the Directive is to provide security of services including the duty to inform the subscribers whenever there is a particular risk, such as a virus or a security breach.

This Directive will come into play concerning communication across borders in the PARTNER Platform as discussed in section 4.3.

### 3.1.4 Recommendation on cross-border interoperability of electronic health record systems


The Recommendation is intended to support the premise that connecting people, systems and services is vital for the provision of good healthcare in Europe. Its eventual purpose is to contribute to the achievement of overall European eHealth interoperability by the end of the year 2015.

The key objective of this recommendation is to allow patient choice to access his/her important information stored in electronic health record systems anywhere any time. For example it should be possible to make patient summaries available to avoid delays in diagnosis for victims with certain risk factors, e.g. allergies.

The guidelines address these objectives:

- Establish aspects of electronic health records that should be exchangeable between systems, such as patient summaries, emergency data sets, and medication records facilitating ePrescription.

- Enable health data to be shared among different healthcare systems, based on a limited range of applications currently in use in different Member States.

- Build appropriate networked systems and services covering all areas of healthcare, while fulfilling appropriate legal, operational and educational requirements.

The scenarios presented in the EC Rec. 2008/594/EC are designed primarily for emergency and extreme situations, like in treating victims of car accidents. The recommendations for these situations are suitable also for the PARTNER Platform regarding patient referral.
3.2 Country-specific Legal Considerations

In this section we describe examples of particular implementations of national laws following the EU Directives mentioned in the previous section. In particular the notions of anonymised data and pseudoanonymised data are exemplified for different countries.

For example, the German legislation follows European Directive 95/46/EC and extends it making it more strict and appropriate to national requirements. Following the initial Directive proposal, “rendering anonymous” means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labour be attributed to an identified or identifiable individual.

The rules for processing of personal data for research, relevant also for PARTNER Platform, are the following:

1. Personal data collected or recorded for purposes of scientific research may be processed or used only for purposes of scientific research.

2. Personal data shall be rendered anonymous as soon as the research purpose allows. Until then, the features enabling the attribution of information concerning personal or material circumstances to an identified or identifiable person shall be kept separately. They may be combined with the information only to the extent required by the research purpose.

3. Bodies conducting scientific research may publish personal data only if
   a) the data subject has consented,
   b) this is essential to present research findings concerning events of contemporary history.

In the UK there are two laws governing personal data, the Data Protection Act 1998 (DPA 1998) and the ‘Caldicott’ recommendations from 1997. DPA 1998 apply to all person-identifiable information, whether manually-held or on computer, stating that processing should be ‘fair’, meaning that it must be carried out without deception. The Caldicott recommendations apply specifically to patient-identifiable information, and emphasise the need for controls over the availability of such information, and access to it. There are considerable similarities and overlaps between the requirements of the Data Protection Act and Caldicott. Interesting for PARTNER Platform is the processing of personal data for cancer registration: in 2002 the UK Association of Cancer Registries obtained an exception form the DPA 1998. Specifically, Regulation 2 makes provision relating to “the processing of confidential patient information in connection with the construction and maintenance of databases by bodies (known as "cancer registries")

---

5 A full review of the national implementation of the European Data Protection Directive can be found here: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm
which undertake the surveillance of health and disease of patients referred for the
diagnosis or treatment of neoplasia." 6

Switzerland is not a member of the European Union (EU) or of the European
Economic Area but it has partially implemented the EU Directive on the protection
of personal data in 2006. However, Swiss law imposes fewer restrictions upon data
processing than the Directive in several respects. The law applies to the processing of
personal data by private persons and federal government agencies. Unlike the data
protection legislation of many other countries, the DPA protects both personal data
pertaining to natural persons and legal entities 7.

Most Swiss cantons have enacted their own data protection laws regulating the
processing of personal data by cantonal and municipal bodies, e.g. the project “e-toile”8,
aiming to build a healthcare information network for the Canton of Geneve, described
the system, participants and the operations in a project law 9.

---

6http://82.110.76.19/confidentiality/background.asp
7From: http://en.wikipedia.org/wiki/Information_privacy#Switzerland
8See (in French): http://www.geneve.ch/sante/avantprojet/etoile.html
4 HISP Environment

The storyline in section 1.3 implies two distinct scenarios: a clinical scenario in which a patient is referred from a local cancer centre to a hadron therapy centre, and a research scenario in which clinical data is used to draw scientific conclusions. Both scenarios are detailed in section 4.1. Common elements and services were derived from these scenarios. Section 4.2 contains an explanation of these services and their functionalities. Lastly, we conclude on the legal and ethical requirements of proposed services in the light of the scenarios.

4.1 Scenarios

4.1.1 Patient Referral

To check if Mr. X would be suitable for PT and to refer him to a PT centre, Mr. X’s medical doctor (MD) logs in to the PARTNER Hadrontherapy Information Sharing Platform (HISP) using the authorisation service. Since this is the first use of this service the MD is presented with the conditions for joining and using HISP and signs an electronic contract delivered by the agreement service which grants him access to HISP.

Using his credentials the MD uploads the medical history of Mr. X using HISP web import service. The information is checked for consistency and then the case is registered in the HISP database. Also, data entities are annotated with definitions from the Metadata Registry (MDR) service to describe the meaning of each data entry in the own MD language and standard.

As an extra service, HISP matches patient data to an existing database on cancer treatments, which reveals that Mr. X is likely to benefit from PT.

After Mr. X’s decision, his MD has to send the data to the multidisciplinary team (MDT) in the national referral panel to review Mr. X’s case. The MD authorises the MDT to see the medical case using the HISP authorisation service. At this stage also the patient could give his electronic consent on these operations. The time delay between request and decision of the panel should be as short as possible.

The MDT agrees to the conditions given by the agreement service, is granted access to Mr. X’s data and visualises his case report, using the HISP data access service. After
the referral is approved by the national panel, Mr. X’s information has to be reviewed by the PT centre abroad, which follows the same procedure as the MDT to access the patient files. This procedure may include a negotiation process for data transfer terms in compliance with different national laws, mediated again by the agreement service.

If the PT centre uses other standards than the referring centre a mapping and transformation service in HISP provides means for data translation. The PT centre can use the built-in data visualisation service of HISP or export data to their own systems.

Based on the clinical details and imaging information available in HISP, the PT centre accepts Mr. X and treats him. Treatment data is uploaded in HISP and also the follow-up data is kept updated in the system where all the parties interested will be able to access it.

### 4.1.2 Research

HISP supports PT patient referrals and therefore keeps track of the patient personal information, diagnosis, treatment, follow-up and additional data. Each data source, typically the referring hospital or a PT centre, have annotated their datasets with additional information, defining the meaning of each data item. These definitions are registered, stored and curated in so-called metadata registries (MDRs) and are advertised in HISP.

Dr. W’s research project requires to combine and evaluate data related to cancer treatment from several hospitals and research institutions across Europe.

She learns about HISP and registers for an user account in the platform. When she logs in for the first time, she needs to agree to the general terms of usage of HISP which define the rights and obligations for users like Dr. W. For example, Dr. W is allowed to browse the data definitions which the different data sources in the federation use to describe their data.

Although Dr. W is not yet able to access any data, using the data definitions and statistical information (like the number of data items recorded for a specific type of data), she identifies datasets relevant to the study she wants to perform.

Dr. W submits her research proposal to HISP asking for access to the selected datasets, specifying the scope and possible outcome of her study. A few days later she finds a message in the inbox of her HISP workspace, notifying her that more information about the purpose of her research is needed by the committee reviewing the research proposal. She submits the requested information and receives another message the following day.

The committee has fully analysed her proposal with the additional information and concluded that Dr. W is conducting relevant and scientifically sound research.

In order to respect the confidentiality towards the data donors, Dr. W is allowed to either download a reduced data set in anonymised form or to perform the analysis directly on HISP making use of all the available information.

Dr. W knows that her research will be more significant if she can use the patients’ year of birth in her analysis rather than the age of the patients. The anonymised dataset however would only contain the patients’ age in order to make the re-identification of
data sets less likely. Dr. W therefore prefers to run her analysis on HISP rather than on her private PC and informs HISP about her decision.

A contract is generated describing the access rights of Dr. W and the conditions of data access and processing. After signing this electronic agreement, Dr. W has a limited time window in which she can submit analyses for the selected datasets. Before doing this she needs to review the data definitions of the sources which she has selected.

It turns out that two of the sources use different prognostic factors to describe the expected disease evolution. Although both prognostic factors are related finding a translation between both definitions is not trivial and involves a significant amount of specialist knowledge.

Dr. W is lucky because Dr. V, a previous user of HISP, has already defined an appropriate mapping to transform one prognostic factor into the other. Relying on user ratings and recommendations, Dr W reuses this mapping to solve the interoperability problem between the two data sources.

Apart from the two different units being used in another set of definitions, the remaining data definitions are fully compatible although slightly different names are used. Dr W just needs to assert which data definitions correspond to each other and the platform will then convert the actual data into her preferred representation.

Now, Dr. W starts designing her analysis programme. She uses the integrated workflow tool with predefined functions and parts of her own code to minimise the programming effort.

She submits the analysis and HISP automatically retrieves the data items from the datasets requested, transforms them according to the selected mappings and runs the simulations required.

After a while, Dr. W receives a notification that the analysis terminated successfully and she visualises the results. Her findings are not only of academic interest but could have an influence on future European policy making. Dr. W follows the HISP policy and publishes her findings on the HISP public portal, a citation acknowledging the data sources is automatically added. The research history gives other researchers the opportunity to re-run Dr. W's analysis using the same data and the same interpretation of the data values, so that they can draw their own conclusions.

### 4.2 HISP Services

Following the scenario description above we identified an initial set of services and their functions for the PARTNER Platform. These services are suitable for a Service Oriented Architecture and the implementation and deployment will be the focus of the next WP22 and WP23 deliverable. The core services are depicted in figure 4.1: the user interface, e.g. a portal or generic programming interface; the authentication and authorisation service, and the base communication level that ensures service interoperability. The rest of the services, e.g. metadata or analysis, rely on the core services and are invoked depending on user needs.
4.2.1 Communication

This service will allow the creation of a network fabric which the rest of the services will rely on. The functions of this service are to provide:

- **secure networks** from the data owner to the data consumers
- **encryption** of the data while it traverses open networks
- **service discovery** providing an index of services, e.g. a local MDR instance

4.2.2 Logging

This service will keep a **history** of all the operations, e.g. log-in, data access, and it will be used for audit and provenance functions. **Auditing** the services is in most clinical cases a legal requirement. The **provenance** function could provide quality assurance in the clinical setting while in the research case can be used for having reproducibility of results, workflow re-usage and means to acknowledge data sources.

4.2.3 Agreement

Many aspects of data handling will require **negotiation** between the data controller and a third party, e.g. another practitioner or a researcher. Many cases of data handling are not explicitly covered by law. For this reason, often specific **contracts** need to be established between the parties exchanging data.

Also the scientific usage of data is commonly subject to a prior **review of the proposed research**\(^1\) by a committee to make sure that the research is scientifically

---

\(^1\) denotes a function which is unique to the research scenario.
sound and ethically permissible. In this case the agreement service facilitates the negotiation process between researcher and committee.

The service will keep records of the agreements in the following situations:

- data sharing for clinical and research purposes
- terms for viewing metadata definitions
- patient consent
- 3rd party audit contract

### 4.2.4 Authentication and Authorisation

Authentication and Authorisation (A&A) services identifies users and controls the rights of users for viewing metadata items, editing metadata, creating mappings and accessing or processing data. These service will control also the access to and from third-party services via a service delegation function. The control on A&A depends on the access roles, ranging from sysadmins to data controllers and researchers.

### 4.2.5 Data Import

For referral purposes, data needs to be imported into the platform. Also, institutes may have an interest in making their data available to a wider researcher community. The data import service provides the following functionalities:

- **Upload**: data can be imported as bulk/raw files and plug-ins for interpreting it will have to be developed, data owners could also use forms constructed using the MDR definitions.

- **Consistency Check**: data will be be checked for obvious errors but also, if the upload follows an agreed terminology and ontology, more deep reasoning can be foreseen.

- **Registration**: data has to be registered to be available in the system. The registration function should also match the new data set to a person if this person already has an entry in HISP.

### 4.2.6 Metadata

The metadata service provides methods to describe the meaning of data in the platform, to author and to curate these data definitions and to allow reuse of data elements beyond institutional boundaries. Since metadata gives only information about the kind of data recorded by a particular institution, not the data itself, the metadata service in most cases is not concerned with legal and ethical restrictions regarding privacy and confidentiality. However, the disclosure of certain rare types or combinations of (meta)data elements may render data subjects identifiable.
• **Registration** of common data elements (CDEs)
  Users can register common data elements in the MDR if they have the corresponding privileges for their registration authority. The CDEs will be kept in a repository so that other users can re-use these definitions to describe their data items.

• **Curation** of CDEs

• **Data Annotation**
  Different institutions may employ different definitions to describe their measurements. When importing data into another system, the meaning of this data in the context in which it was taken is important. Data annotation links a definition to data items. These links can be established after data import, or linking rules can be set before data import.

• **Browsing** of registered CDEs
  CDEs only describe the kind of data kept in a repository. Viewing these definitions should require only low access rights so that users can discover data sources holding a specific type of data and can re-use existing definitions to describe their own data items.

• **Mappings** between different registered CDEs
  Mapping specifies rules between different definitions. These rules will transform between different representations of data. Like the CDE definitions, the mapping rules should be in a repository to be accessible for re-use.

**4.2.7 Data Access**

Once data items have been selected, and their use been approved through the agreement service, the data has to be retrieved for further processing, visualisation or export.

• **Query**: HISP will translate the client request into the underlying database language

• Data **Transformation**: using the annotations and mappings between the definitions, data will be transformed into the selected format

• **Visualisation**: this function will provide HISP with built-in capabilities to view different data types, e.g. DICOM, JPEG, microarray samples...

• **Workspace**: users will retain their settings, workflow and custom definitions

• **Export**: allows to export data in various formats, e.g. a CSV file or a JPEG plot

• **Anonymisation** *: this function will allow researchers data access conform with their rights and privileges for specific requests, e.g maintaining patient privacy.
4.2.8 Data Analysis *

The service offers the researchers an integrated tool to design, execute and analyse their research, e.g. simulation algorithms.

4.3 Conclusions

ICT systems will revolutionise information sharing between health professionals and patient-doctor relations but they need standardisation, interoperability, a common legal framework and support from all the parties involved. The PARTNER Platform focuses on the technical aspects of syntactic and semantic interoperability between systems. Nevertheless, the prototype development should take the ethical and legal requirements for such an information sharing system into consideration and follow them as closely as possible. Using the information from chapters 2 and 3, this section concludes on how the two HISP scenarios are affected by ethical and legal constraints.

4.3.1 Patient Referral

In this scenario patient information is transferred to health care institutions in different EU countries for the purpose of establishing a precise diagnosis and providing the best available treatment. As long as the parties follow similar ethical code of conducts and legal frameworks in handling patient data, sharing data between two practitioners is possible.

However, the way in which information is exchanged between healthcare institutions raises issues with patient’s privacy and confidentiality. Patient consent would need to be sought, explaining how the patient’s data will be protected when leaving the hospital. Since most patients will not be competent to do a risk assessment about technologies for secure data sharing, this evaluation would need to be done beforehand by a third party on whose decision a patient can trust and rely. Before being used for real patient referrals, using personal data, HISP might need to undergo medical device certification (see 3.1.2).

Processing personal data across borders carries the risk of having different laws governing this process. The scope of the Directive on data protection [12] is broad and thus the national implementation varies and amendments may be required for specific data transfers between countries. The common requirements of personal data processing [22] are to:

- leave medical data at the source
- aggregate data as needed and only during the limited period of use
- empower the patient to decide on the type of information and people allowed to access it
The communication between parties should be protected, as discussed in section 3.1.3, encrypted and the solutions range from industry standards, like Transport Layer Security protocol\(^2\), or special networks like the EESSI\(^3\) that allow pan-European electronic personal data exchange between Member States [1].

The heterogeneity of EU Directives implementations in the Members States can only be solved in the legal field. For the PARTNER Platform, as much for any other system, the easiest solution for data exchange is to have a contract between the health care system participants following strictly the EU recommendations.

### 4.3.2 Research

In order to use patient data for research, the research has to qualify as scientifically sound and ethical. Depending on the research needs data can be provided in different levels of anonymity: personal, anonymised or pseudoanonymised.

For many types of research, anonymised data is sufficient. Anonymisation of a person’s data is in conflict with the right for autonomy because the person can no longer decide about the usage of the data once it has been made public. However, anonymisation significantly lowers the security requirements for a system.

In some cases, research may require personal data or it may not be possible to anonymise data, as e.g. is the case with tissue samples or genetic data. In these cases, the data can only be used if the patient gives his/her consent. Optimally this consent would be specific to one research project and therefore for one specific use of data. However, the purpose of a repository like HISP is to use existing data in various research contexts over time. The majority of these experiments cannot be foreseen at the time of data collection when the consent is sought. An alternative to the conventional form of a specific consent is the so-called broad consent for future research. In this case, a patient consents for his data being used for research in general or for a certain type of research and he transfers his right to decide about his data to an ethics committee.

Guidelines for ethical conduct, like AMA or GMC, state that the duty for confidentiality persists beyond the death of a patient. The patient’s wishes need to be respected and the purpose of disclosure and possible distress to the patient’s family, partner or close friends need to be considered. However the potential for disclosing information to cause distress or to damage the public’s trust is considered to diminish over time.\(^{[23]}\)

In general, a committee needs to make sure that the level of disclosure of patient details is appropriate to the research needs and conform with the patient consent. By storing data in pseudonymised form (recommended e.g. by the German implementation of the European Directive 95/46/EC\(^21\)), the access rights can then be adapted to the needs of a specific research project.

The legal responsibility of the platform hereby is reduced to:

- enforcing the data access rights foreseen by the ethical review committee,

---


\(^3\) [http://ec.europa.eu/trasr/](http://ec.europa.eu/trasr/)
• keeping the contracts between HISP and the medical centers

• providing secure communications between parties

• logging the activities of a user to be able to verify if the actual usage of data is conform with the foreseen usage laid out in the proposal,

• ensuring that unauthorised users cannot access personal data.

The approach of maintaining links between identifiable and non-identifiable data has the additional advantage that research results could be communicated to the patient, if the patient gave his consent on this, and ensure reproducibility of scientific results.
Bibliography

electronic authentication, Tech. rep., ENISA (February 2010).

[2] F. Roman, Health grids: overview and added-value (partner work package 22,
deliverable 1; prototype grid hadron therapy testbed;), Tech. rep., CERN
(November 2009).
URL https://espace.cern.ch/partnersite/workspace/faust/
Shared%20Documents/FaustinRoman.WP22.D1.pdf

[3] D. Abler, Data integration for the partner hadron therapy information sharing
platform (partner work package 23, deliverable 1; prototype grid hadron therapy
testbed;), Tech. rep., CERN (March 2010).

therapy, Poster at 'Physics for Health in Europe' workshop, 2-4 Feb. 2010, CERN,
Geneva (February 2010).
URL https://espace.cern.ch/partnersite/workspace/abler/
Shared%20Documents/ConferencePoster/PARTNER_Grid_ 
PosterAndAbstract_PhysicsForHealthCERN2010.pdf

URL http://www.iep.utm.edu/ethics/

[6] S. H. Miles, The Hippocratic Oath and the Ethics of Medicine, Oxford University

relationship., Canadian family physician Médecin de famille canadien 35 (1989)
921–926.

URL http://dx.doi.org/10.1007/s11017-007-9036-y


doi:DOI:10.1016/S1470-2045(06)70618-0.
URL http://www.sciencedirect.com/science/article/B6W85-4JC688T-14/2/27a924e91d49724c019a0f2dab95fee6

arXiv: http://jme.bmj.com/content/35/2/125.full.pdf,


