PICASO

A Personalised Integrated Care Platform

(Grant Agreement No. 689209)

D3.5 Privacy Compliance Laws Associated with Surveillance

Date: 22-12-2017

Version 1.0

Published by the PICASO Consortium

Dissemination Level: Public

Co-funded by the European Union’s Horizon 2020 Framework Programme for Research and Innovation under Grant Agreement No 689209

Document control page

Document file: D3.5 Privacy Compliance Laws Associated with Surveillance.docx
Document version: 1.0
Document owner: VUB

Work package: WP3 – Integrated Care Models, Multi-morbidities, and Privacy
Task: T3.4 – Legal Challenges Associated with Surveillance
Deliverable type: [R]

Document status: ☒ approved by the document owner for internal review
☒ approved for submission to the EC

Document history:

Version	Author(s)	Date	Summary of changes made
0.1	VUB, Paul Quinn	14-02-2017	Basic structure
0.2.	VUB, Paul De Hert, Paul Quinn	21-03-2017	More detail on data protection
0.3	Paul Quinn	28-05-2017	More detail on medical device framework
0.4	VUB, Paul Quinn, Paul De Hert Darek Kloza	05-12-2917	Changes made following departure of IBM from PICASO consortium.
1.0			Final version submitted to the European Commission

Internal review history:

Reviewed by	Date	Summary of comments
Trine F. Sørensen (IN-JET)	19-12-2017	Minor corrections and comments. Formatting should be corrected.

Legal Notice

The information in this document is subject to change without notice.

The Members of the PICASO Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the PICASO Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Possible inaccuracies of information are under the responsibility of the project. This report reflects solely the views of its authors. The European Commission is not liable for any use that may be made of the information contained therein.

Index:

1 Executive Summary

1.1 Document Purpose

The purpose of this document is to advise the consortium on legal issues that relate to surveillance issues in the context of the activities that are proposed and foreseen within the PICASO project. Accordingly, the focus of this deliverable is on legal issues that are likely to relate to the use of patient data in a manner that is foreseen by the PICASO project. This relates to the use of patient data and the use of monitoring techniques devised to collect such data. This document does not attempt to provide legal advice on actual medical practice as this would be beyond the scope of the project (which is itself not attempting to implement new forms of medical treatment but only collect and interpret data in a novel manner).

The reader should note that in addition to issues related to surveillance, data privacy and data protection this project will also consider potential issues that might arise as a result of Medical Device Regulation. This issue has been raised by partners several times during consortium meetings. As a result, it was felt that a consideration of such issues within this deliverable would be opportune.

It is necessary to conceptualise PICASO in two forms. The first and most pressing is well planned and described trial in two different legal jurisdictions (this will be referred to throughout this paper as 'PICASO as an exploitable system'). The second is a platform architecture that has been successfully deployed after the PICASO project has been finished (this will be referred to throughout this paper as 'PICASO as an exploitable product').

1.2 The Link Between Privacy and Data Protection

Privacy and data protection are issues that are clearly linked.[1] As this deliverable discusses, privacy is mostly understood to be a wider concept than data protection, with the latter representing one legal approach amongst many that may be considered capable of protecting privacy.[2] Whilst many theorists have put forward their respective definitions of privacy it has proven impossible to reach consensus regarding a single definition. Common elements can be discerned, including most importantly the preservation of a sense of autonomy and the ability to choose for one's self her preferred path in life. Such autonomy in the medical context can relate to several aspects. This can include the right of individuals to select the form of medical care they feel best suits them. As a result, many ideas are related to PICASO from an ethical perspective concerning patient participation in monitoring. These were considered in deliverable D3.3 The PICASO ethical guidelines and will not be discussed further in this deliverable.

Informational self determination is also an important manner to safeguard individual privacy. As this deliverable discusses there are various legal approaches in Europe that are concerned with the preservation of privacy through protecting informational self-determination. These include on a European level the European Charter of Fundamental Rights and more importantly the European Convention on Human Rights[3]. One of the most important sources of law for a project such PICASO however is the European Framework on Data Protection. Data protection laws in Europe have come to replace traditional legal approaches to medical confidentiality as the primary source of law used to protect patients in Europe. This framework applies to the processing of all personal data within Europe, included in a medical context. Importantly the EU data protection framework is currently in a state of flux, with a new regulation – the General Data Protection Regulation (the GDPR) replacing the current directive (95/46/EC). This document considers the application of both, including the potential application of new requirements in the GDPR. This was necessary because the new regulation comes into force in May 2018 – i.e. during the life time of the PICASO project.

1.3 The Main Elements of Data Protection

As this deliverable discusses the data protection framework in general obliges data controllers (in 'PICASO as a research project' the data controllers will be the Hospital Partners in Germany and Italy Respectively in three main ways. These are:

- To process data online with recognised data processing principles.
- To have a correct legal basis for the processing of personal data.

[1] *P De Hert and S Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacety of the Individual and Transparency of the Power," in Privacy and the Criminal Law, ed. E Claes, A Duff, and S Gutwirth (Antwerp - Oxford: Intersentia, 2006).*

[2] *S Gutwirth, Privacy and the Information Age (New York: Rowman and Littlefield, 2002).*

[3] The latter, unlike the former applies to all questions of law. The European Charter only applies in questions relating to the implementation of EU law.

- To respect the rights of data subjects.

1.4 Respecting Data Processing Principles

In terms of data processing principles, the GDPR contains an expanded list (in comparison with Directive 95/46/EC). It will be important that each of these is respected within the course of the PICASO project. This will involve considering carefully their potential implications within the context of the PICASO project itself. Where data processors are involved it will be necessary for the data controller to conclude a contract with such processors in order to ensure that these principles are respected.[4] These principles include inter alia:

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Data protection by design;
- Accuracy;
- Privacy by design;
- Storage limitation;
- Integrity and confidentiality; and
- Accountability.

1.5 The Need for a Legal Basis for Processing

The possession of a correct legal base is required for the processing of personal data. Without it personal data may not be processed even if such processing was otherwise in compliance with the data protection principles described above. In the context of 'PICASO as a research project' and potentially 'PICASO as an exploitable product' the correct legal base will be 'explicit consent'[5] Whilst within the confines of the PICASO project the consent forms foreseen by the respective hospital institutions will conform to this requirement (provided they contain the correct information), the situation concerning any exploitable product developed thereafter is more complex. This is because it is envisaged that any PICASO-like product would make use of granular consent provided through electronic means, i.e. through tablets, computers or phone apps. Whilst granular consent is encouraged by the GDPR there is a fine balance to be had between the level of granularity and the informational obligations incumbent upon the data controller when asking potential data subjects for consent. As the authors of this report identify consistently presenting individuals with too much information (for purposes of legal compliance) may make a mockery of granular consent and reduce its exercise to a mere tick box exercise. Ultimately it will be for future data controllers to discern how this balance must be found, taking into account the context in which they are faced.

1.6 Rights of the Data Subject

In addition, data controllers must respect key data subject rights and ensure that data subjects are able to make use of them. Once again as this document identifies it will be necessary to take into account specific aspects of the PICASO project when interpreting how they should be facilitated. The key rights are:

- A right to be informed about basic information (consenting the processing and associated legal rights);
- A right to revoke consent;
- A right of access;
- A right of rectification;
- A right of data portability; and
- A right to have third parties notified of their obligations viz-á-viz the data subject.

1.7 The Importance of the Medical Device Framework.

The Medical Device Framework (MDF) represents one of the most important EU legal initiatives in the area of healthcare. Also undergoing revision, the MDF will, in the course of the coming years, be the subject of a new regulation aimed at harmonizing regulation of medical devices across Europe. It will be important for the

[4] *For more see section 5*

[5] Described in article 9(2) of the GDPR and article 8 of Directive 95/46/EC respectively.

PICASO project to consider the application of this framework. Although devices used for research purposes within the context of the PICASO project need not go through the MDF certification process, this will not be the case for any exploitable product thereafter. In the context of healthcare medical professionals and institutions will be under an obligation to ensure that they use correctly certified devices (i.e. that possess the *CE* Mark). This means that any devices that were to be later developed within the PICASO project would have to go through the certification process if they were to be used in actual medical practice (e.g. any monitoring devices developed or integrated into the 'patient dashboard'). This entails *inter alia*:

- Discerning whether a device meets the conditions for a medical device i.e. in terms of ''intended purpose' and being for 'monitoring' or 'diagnostic' purposes;
- Discerning which class the developed device belongs to;
- Complying with the essential requirements for that class; and
- Complying with the administrative requirements that exist for that class (these are more onerous for certain classes).

2 Introduction

As described in the PICASO DoA the main aim of the deliverable is to advise the PICASO consortium on legal issues related to privacy and data protection. This deliverable will also discuss important issues pertaining to the regulation of medical devices for which it had become evident, through discussions with partners, that such issues should be considered given their obvious relevance.

2.1 PICASO as a Project – Outline

The PICASO project aims to build a service oriented, ICT based integration platform that will support collaborative sharing of care plans across sectors based on dynamic and personalized orchestration of care services.[6] It will further provide a method for sharing patient information across all relevant formal and informal care providers using a unique, trust federated solution to the problem of data privacy in cloud based health systems. In simple terms the aim of the project is demonstrate how various health professionals and carers to view information about a patient (where they all have a direct relationship with that patient), even when they may be based at different institutions.

PICASO develops a service oriented, ICT based integration platform that will support collaborative sharing of care plans across sectors based on dynamic and personalised orchestration of care services. It will further provide a method for sharing patient information across all relevant formal and informal care providers using trust federated solution to the problem of data privacy in cloud based health systems.[7]

The PICASO project will conduct two separate but complementary use case driven trials for proof-of-concept demonstrators of integrated care. The trials will be conducted in Germany (Trial 1) and Italy (Trial 2) and involve actual patients (described briefly below). The main purpose of the trials is 1) to demonstrate the concept of the PICASO platform and its components, and 2) to validate the impact on the effectiveness of the care systems and the acceptance of the wider group of stakeholders, patients, relatives and the society at large. Trial 1 “Rheumatoid Arthritis (RA) with Cardiovascular Disease (CVD)” will be carried out by the Policlinic of Rheumatology and Hiller Research Unit Rheumatology at the Heinrich-Heine-University (HHUD) / University Hospital of Düsseldorf (UDUS). Trial 2 “Parkinson’s disease (PD) with Cardiovascular Disease” will be conducted by UTV (The University Hospital of Tor Vergata in Rome) in conjunction with the institute of treatment and research Santa Lucia in Rome.

2.2 The need to consider the legal compatibility of PICASO 'Pre' and 'Post' Project

As much of the discussions below indicate it is necessary to conceptualise PICASO in two forms. The first and most pressing one are the well planned and described trials in two different legal jurisdictions (this will be referred to throughout this paper as 'PICASO as an exploitable system’). The second is a platform architecture that has been successfully deployed after the PICASO project has been finished (this will be referred to throughout this paper as 'PICASO as an exploitable product’). This deliverable will consider the legal issues that will be raised by both potential manifestations and discuss what will be necessary in order to ensure compliance. This is because differing legal requirements will apply to 'PICASO as research product' than will do to any system architecture that is deployed subsequently in 'PICASO as an exploitable product'. Given that the point of PICASO as a project is to demonstrate the potential viability of a novel type of information sharing infrastructure, it is also therefore arguably 'necessary' to demonstrate its viability in terms of legal compatibility. This will be achieved by considering the application of the various legal requirements in this project to both the trials as proposed above and the likely hypothetical form that a post PICASO project would take. This will occur on a case by case basis as each legal requirement or principle is considered. In doing so this deliverable aims to contribute to the nature of this project as primarily being to demonstrate the viability of the novel PICASO architecture. In doing so this project will also be complying *inter alia* with the requirements of Article 35 of the General Data Protection Regulation (discussed further in section 5.16) which requires an impact assessment of the potential risks in terms of data protection rights.

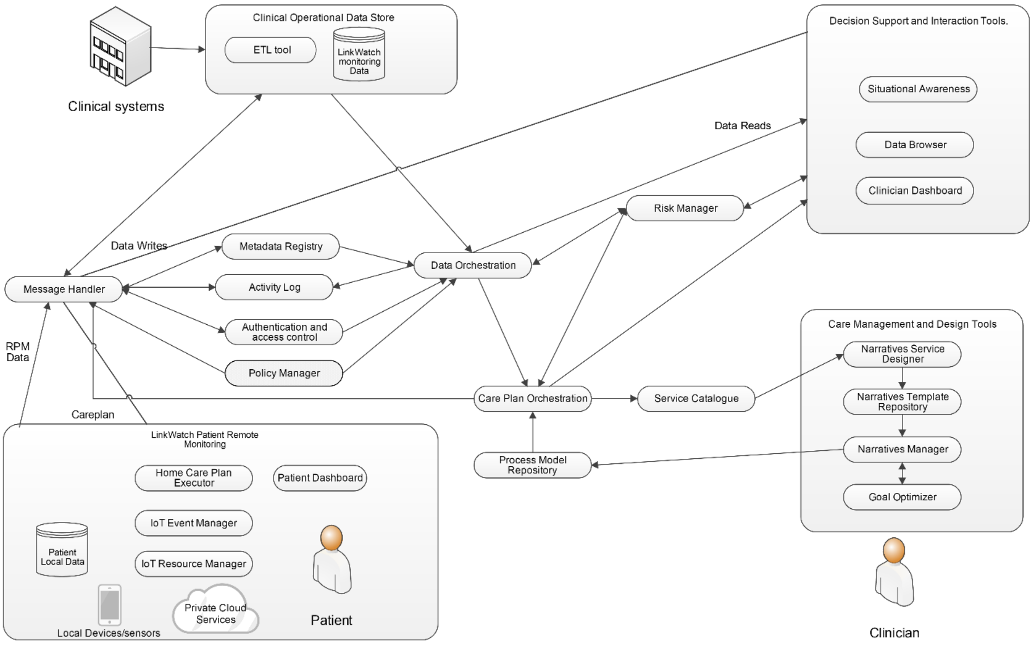
[6] This subsection is taken Directly from PICASO deliverable ' D2.1 Scenarios and Use Cases for Integrated Care'

[7] PICASO Deliverable 2.3 Architecture Specification

2.3 Potential Goal of PICASO Project – 'PICASO as an Exploitable Product'.

(i) General Goal Project Goals

The goal of the PICASO is to demonstrate that the federation of patient data is possible in a way that respects ethical and legal concerns surrounding privacy. Although the project itself will not be creating such a finalised and ready-to use-system, the aim is to demonstrate that it is indeed feasible. The diagram bellow shows one possible way to view the architecture of the project.[8]



(ii) Key Elements

This view of the architecture demonstrates some key features of a potential PICASO system that may be used. Some of the most important elements that are important from a legal perspective are listed below.

(i) **Patient data is not stored centrally in a cloud** - Although the aim of the PICASO project aims to share details of patient records between physicians and carers this is achieved without the creation of any central repository of such data. Accordingly, there is no cloud repository containing individual personal data. Data is rather passed between different sources with the role of the centralised 'data orchestration function' mainly being rather to direct physicians and care giver to the location of the data they desire (i.e. being stored in the system of the care giver concerned). Once such data is requested it is 'pushed' to the user that requested in a way that it is temporarily viewable and cannot be stored on the terminal of the individual. This has important implications for who can be considered the data controller/data processor (see section 5.5) in addition to the type of content that is necessary.[9]

(ii) **A number of physicians or carers may have access to a patient's data**. The point of the PICASO project is to demonstrate a system in which various physicians and carers will be able to view relevant medical details of individuals, even if they are stored on the information systems of other physicians in other institutions. The PICASO system will through its orchestration unit direct an interested party (assuming he or she has permission) to the location where relevant data is stored. Data will be 'pushed' to the requesting party but they will not be able to store it locally.

(iii) **Individual patients will have control over which physicians can see their data and what they can see.** They will be able to alter the access permissions that relate to their data. In this way a patient will be able to exercise their explicit consent in a granular manner over who is able to process their

[8] Taken from PICASO deliverable D2.3 Architecture Specification
[9] *See chapter IV of the GDPR*

medical data and for what purposes. As section 5.17will discuss this is important when considering the legal grounds for the processing of medical data in the project.[10]

(iv) **This can include data that comes from mobile monitoring devices**. Included within the data available to physicians and to carers may also be data made available from various monitoring devices. These devices may for example include various monitoring devices related to chronic diseases that individuals may have. As sections 5 and 6 will discuss this will also be important in terms of both data protection requirements and requirements related to the Medical Device Framework. It will also be necessary to gain consent for the use of any medical data generated in a correct manner (see section 5.17).

2.4 'PICASO as a research Project'.

The aim of the PICASO project is to demonstrate the possibility of such an infrastructure (as described above) on a small scale in the context of two controlled trials. Thus, whilst the description above represents the type of PICASO system it is hoped would be possible for 'PICASO as an exploitable product', within the project itself it will be demonstrated on a smaller scale at two different sites (in Germany and Italy). These trials will involve the communication of data between specialists of two different categories in other to demonstrate the principles discussed above. In both instances all data will be transfer between the local hospital site and other care providers through the use of a local cloud service provider. This provider will be based in the same jurisdiction as the trial is taking place. All processing will be in compliance with local data protection law and ethical requirements. This involved getting clearance from local ethics committees and producing consent forms for trial participants in line with both the demands of the local ethic committees and the demands made by the PICASO ethical board.[11]

Trial 1: Rheumatoid Arthritis with Cardiovascular Disease[12]

Trial 1 will involve patients with Rheumatoid Arthritis as primary morbidity and a cardiovascular disease as co-morbidity. The patients need to be managed in terms of medication, exercise and health status with the main aim of retaining a permanent good remission status. Rheumatoid Arthritis (RA) is an inflammatory rheumatic disease with a prevalence of 1% of the normal population. RA is an auto-immune systemic disease. Immunosuppressive medication (including steroids, disease modifying anti-rheumatic drugs, and biologicals) is used to prevent inflammation and damage. However, the medication leaves the patient open to all kinds of infections. The medication may thus be reduced before operations and when the patient suffers from infections. For example, with an infection in the upper airways, the GP prescribes antibiotics and may reduce the RA medication. But then he may forget to increase the RA medication after the infection has been treated. Further, if the patient seeks treatment for other conditions elsewhere, the risk increases because he may not mention that he has RA. Medication may also include pain medication.

The inflammation may cause co-morbidities, but if the inflammation can be contained the risk of co-morbidities may be reduced. The medication for patients with co-morbidities can be very complex. Early treatment is substantial.

The purpose of the treatment is to obtain the highest possible and sustained state of remission, meaning that the patient is functioning

Trial 2 Parkinson's Disease with Cardiovascular Disease

Trial 2 lay-out will involve patients with Parkinson's disease as primary morbidity and cardiovascular disease (CVD) as co-morbidity. The patients need to be managed in terms of medication, exercise and health status with the main aim of retaining a permanent good remission status.

Parkinson's disease (PD) is a neurodegenerative disorder with an incidence that rises steeply with age. The main histo-pathological feature of this disease is a neurodegenerative process that affects the neurons of the substantia nigra that primarily affect motor symptomatology. If one considers that the diagnosis of PD is usually performed in adult subjects (with the highest peak of incidence being detected in

[10] *Article 9 GDPR describes that explicit consent is necessary if consent is to be the legal base for the processing of health data.*

[11] For a more in-depth description of these demands see: PICASO deliverable D3.3

[12] For more in-depth information on the two PICASO trial see: PICASO deliverable D2.1 Scenarios and Use Cases for Integrated Care

patients over 65 years old), Cardiovascular Disease (CVD), diabetes and kidney failure are among the most frequent co-morbidities in subjects affected by PD. Data show that 80% of PD patients older than 65 have CVD, and 20% as direct cause of PD.

The following list of data are examples of the type of data that are likely to figure in the PICASO trials (and accordingly represent sensitive personal data - see section 5.17).

- Blood test results
- Exercise plan.
- Existing images
- Health/medical history & general information
- List of medications used
- Medication withdrawal (necessary for the scan)
- Medicine plan
- Prescription for PD medication
- Referral letter to Cardiologist
- Referral letter to Nuclear Medicine Physician
- Referral to Neuropsychologist
- Report/referral letter from GP
- Scanning images
- Scanning instructions (type of scanning and what to look for)
- Scanning report/results
- Symptoms description
- Treatment plan

3 The Concept of Privacy and its Relevance to the PICASO Project[13]

3.1 Privacy as an 'Illusive Concept'.

Privacy is a term that is omnipresent in our informational society. Individuals seek it, business and governments claim to respect it. It would be difficult to find an individual that did not value his or her privacy in one way or another. Despite this, if you were to ask the man in the street, those who are in a position of trust with regards to information, or even legal theorists you would be unlikely to receive a succinct and similar definition as to what exactly privacy is. Indeed what privacy means will be different to different individuals and groups in different contexts at different times[14]. The former justice French Minister Robert Badinter went so far as to say that “respect for the secret of privacy was such that it went beyond definition”[15]. Despite this, it is often difficult to find opponents when calls are made to improve privacy.

The elusive nature of an agreed definition of privacy has created problems for legal scholars who normally strive to create definitions that can be used to create legal rules. The contextually of privacy and its intrinsic illusiveness have greatly complicated this task. A plethora of pseudonyms that are used interchangeably with privacy including ‘private life’, ‘private sphere’, intimacy’ and ‘secrecy’ have only complicated this further. This has led some scholars to give up attempting to find a global definition and to rely on a more contextual approach where privacy is defined according to the context it is discussed within[16] (in the context of medicine, the concept of professional confidentiality is perhaps the best example). This means that for legal purposes a global ‘catch all’ definition of privacy is useless and perhaps undesirable as rigid and inflexible definitions often make for bad laws. If this is true and privacy is in fact indefinable then why do people seek so often to have their privacy protected and what function does the concept serve?

Whilst some have accepted that privacy is indefinable in a single legal definition, it has been argued however that the broad principle of privacy itself is central and indispensable to a democratic state.[17] A core principle of privacy is the freedom to mould, express and use one’s own personality. This includes the philosophical, social and cultural choices that are central to one’s identity[18]. Such privacy gives everyone the freedom to establish an individual path in life and the potential to resist infringement on this freedom of choice. As Alain Touraine stated democracy is inextricably linked to pluralism and diversity. The freedom to determine one’s own opinion and identity are required to create such pluralism and diversity, as is the freedom to form relationships and associations unhindered. It is through such freedoms that plurality emerges and society can draw upon the viewpoints and experience of many different individuals and groups. Privacy is in reality the legal name given to many of the freedoms and protections that allow such a society to be formed[19]. Without such freedoms society would lose its pluralist character that is essential to a democracy. Within the medical context (and therefore relevant to PICASO) such concepts of privacy dictate the need for patients to be able to choose the type of healthcare they receive and what occurs with any data that is generated therefrom.[20]

3.2 Examples of Varying Theoretical Conceptions of Privacy

There are continuous efforts for conceptualisation and classification of privacy with discussions of what privacy ought to be about, therefore various views exist regarding the scope of its concept. This section will highlight the most influential typologies to illustrate the difficulties of its perception. As the reader will see these ideas show how the concept of privacy is difficult to pin down. It further more shows how most concepts of privacy

[13] Some contents of this section are taken from an deliverable authored by the VUB in the MAthisis Project Managing Affective-learning THrough Intelligent atoms and Smart InteractionS. Deliverable D2.6 – 'Framework for impact assessment of MaTHiSiS against LEPOSA requirements (The LEPOSA report)' Authored by Eugenio Mantovani and István Böröcz

[14] Wright, D., Gutwirth, S., Friedewald, M., Vildjiounate, E., & Punie, Y. (2008). Safeguards in a World of Ambient Intelligence. Springer. P144

[15] Gutwirth, S. (2002). Privacy and the Information Age. Rowman & Littlefield Publishers P34

[16] Examples of such contextual contexts are ‘home privacy’, ‘informational privacy’ and ‘relational privacy’. See Gutwirth, S. (2002). Privacy and the Information Age. Rowman & Littlefield Publishers P34

[17] “The central tenant of democracy is not the fact that the government is elected but it is the fact that rules are put in place from preventing that government from doing what it wishes. “ See: Gutwirth, S. (2002). Privacy and the Information Age. Rowman & Littlefield Publishers P42

[18] Rouvroy, A., & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self Development: Researching the Importance of Privacy for Democarcy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & Nouwt, Reinventing Data Protection.

[19] Gutwirth, S. (2002). Privacy and the Information Age. Rowman & Littlefield Publishers P44

[20] Within the domain of medical ethics the concept of autonomy is often interpreted giving rise to such requirements

are likely to be applicable towards the practice of medicine in general and more specifically a project like PICASO.[21]

- *William Prosser* - identified four kinds of privacy:
    - Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs;
    - Public disclosure of embarrassing private facts about the plaintiff;
    - Publicity which places the plaintiff in a false light in public eye;
    - Appropriation for the defendant's advantage, of the plaintiff's name or likeness.

- *Alan Westin* - opined that "Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". He defined the relation of the individual to social participation as follows: "privacy is the voluntary and temporary withdrawal of a person from the general society through physical or physiological means, either in a state of **solitude** or small-group **intimacy** or, when among larger groups, in a condition of **anonymity** or **reserve**".

- *Roger Clarke* - developed an updated system in 1992. According to him "privacy is the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations." He separated four categories with an addition in 2013:
    - privacy of the person,
    - privacy of personal behaviour,
    - privacy of personal communications,
    - privacy of personal data,
    - privacy of personal experience.

- *Rössler* - analysed three dimensions of privacy: decisional privacy which establishes a space for manoeuvre in social action that is necessary for individual autonomy; informational privacy, i.e. who knows what about a person and how they know it (control over information relating to that person); local privacy, i.e. privacy of the household, of one's flat or room and thus privacy of personal objects. In modern societies it denotes a realm of life and a way of life that is bound up with this realm and is intrinsically indebted to the existence of private spaces, however varied the concrete form this may take. In a project such as PICASO which involves monitoring patients in the privacy of their homes such a concept is of obvious relevance.

- *Solove* proposed a taxonomy of privacy, i.e. a framework for understanding privacy in a pluralistic and contextual manner. The taxonomy is grounded in the different kinds of activities that impinge upon privacy, each of which is relevant to a project like PICASO. The taxonomy is as follows:
    1. Information collection
        a. Surveillance
        b. Interrogation
    2. Information processing
        a. Aggregation
        b. Identification
        c. Insecurity
        d. Secondary use
        e. Exclusion
    3. Information dissemination
        a. Breach of confidentiality
        b. Disclosure
        c. Exposure
        d. Increased accessibility
        e. Blackmail
        f. Appropriation
        g. Distortion
    4. Invasion

[21] Some contents of this section are taken from an deliverable authored by the VUB in the MAthisis Project Managing Affective-learning THrough Intelligent atoms and Smart InteractionS. Deliverable D2.6 – 'Framework for impact assessment of MaTHiSiS against LEPOSA requirements (The LEPOSA report)' Authored by Eugenio Mantovani and István Böröcz

    a. Intrusion
    b. Decisional interference.

- *Finn, Wright, and Friedewald* - developed a typology against the backdrop of EU legislation, designed to address modern technology-related threats to privacy in the twenty-first century. They defined seven types of privacy:
    - privacy of the person;
    - privacy of behaviour and action;
    - privacy of communication;
    - privacy of data and image;
    - privacy of thoughts and feelings;
    - privacy of location and space;

3.3 Distinguishing the terms 'privacy' and 'data protection' as legal approaches

Privacy and data protection are not equivalents, there is a substantive difference between these two phenomena. According to certain interpretations, privacy is broader than data protection; the latter is just a tool to protect the former. Protection of privacy is furthermore not only found within the domain of the law. Protection of privacy is for example an important aim of many ethical approaches which play a crucial role the governance of the use of personal health information. This was reflected by PICASO deliverable D3.3 The PICASO ethical guidelines which discussed the ethical approach which the PICASO project would take. This document will not repeat such analysis and will focus on solely legal issues.

Both fundamental rights – to privacy and to data protection exist in law. One useful way to conceptualise the difference between the two concepts is using the notions of opacity and transparency. Privacy rules often set prohibitive limits that shied the individual against the public authorities and other powers warranting a certain level of opacity of the citizen, whilst data protection channels legitimate use of power, imposing a certain level of transparency and accountability. Data protection tools on the other hand often lay down binding rules concerning how personal data may be used and the limits of such use, providing individuals with confidence that their data will be used in responsible manner.

3.4 Opacity Tools

Privacy represents a relatively new development in contemporary law. Its beginnings have been attributed to the American scholars Warren and Brandeis and their writings in the Harvard Law Review at the end of the 19th century[22]. Legal acknowledgement of the Right to Privacy in Europe is found in the European Convention on Human Rights (ECHR) in Article 8 which protects ‘private and family life’ and also in Article 3 which forbids inhuman and degrading treatment[23]. The development of the protection of Article 8 in particular, through case law over time has accorded individuals in Europe a strong level of protection over their privacy[24]. In a series of expansive judgements, the Strasbourg court, charged with upholding the ECHR, has applied a broad definition of the notion of ‘private life’. The principle has been judged not only to apply in the private sphere at home but to certain activities once considered in the public sphere[25]. The court has also used a broad means of interpretation to include within Article 8 protection of privacy involving the use of various methods of communication including telephone conversations[26], telephone numbers[27], computers[28], video-surveillance[29],

[22] The piece was a reaction to the state of American journalism and its alleged lack of respect for personal feelings and sexual relations. See: De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Indivdiual and Transparency of Power. In E. Claes, A. Duff, & G. S, Privacy and the Criminal Law (pp. 61-102). Intersentia.

[23] The prohibition on inhuman and degrading treatment in Article 3 of the ECHR has been used to forbid medical treatment on individuals without their consent (if they have the capacity to give consent. See for example in the UK R (on the application of Burke) v General Medical Council [2004] EWHC 1879 (Admin), 30th July 2004

[24] Gutwirth, S., & De Hert, P. (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & Nouwt, Reinventing Data Protection (pp. 3-44). Springer

[25] See: Amann v Switzeland, judgement of 16 February 2000 where the court re-iterates that the storing of personal data on individuals falls under article 8. In doing so the court pointed out that the term ‘private life’ must not be construed restrictively. In particular the right to private life establishes the right to form relationships with other human beings, therefore there is no reason to exclude relationships formed within a professional context.

[26] Klass v Germany App No. 5029/71

[27] Malone v UK App No. 8691/79

[28] Leander V Sweden App No. 9248/81

[29] Peck v UK App No. 44647/98

voice recording[30] and internet and email[31]. The case law delineated on privacy provides protection for individuals from unwanted invasion into their privacy. It does this by placing barriers to the access of such information on outside parties. In doing so, such tools have been described as placing a level of 'opacity' on individuals and their privacy[32]. The aim is to create a level of opacity making it difficult for outside bodies to access (legally) information on individuals if those individuals have not consented towards such information being accessed. With regards to a project such as PICASO such opacity rules lay down strict requirements concerning the use of medical data, both in terms of the need for appropriate consent and concerning how such data can be processed.[33] Such opacity tools protect individual privacy by creating autonomy of self-determination and in doing so prevent excessive steering of individual lives by outside forces.

Example: I v Finland[34]
I v Finland was a 2008 case that involved a complaint by an applicant that claimed that her medical records had been accessed by non-authorised individuals. She claimed that the dissemination of knowledge of a medical condition has harmed her employment prospects (as a nurse). The court ruled that such matters would fall under Article 8 of the European Court of Human Rights.[35] The court ruled inter alia that were appropriate steps are not taken to safeguard personal data that such actions amount to a breach of Art 8 ECHR. The court furthermore ruled that clear procedures must be in place to log who has accessed the data in question and to report breaches.
Conclusion: Protection of personal data is demanded by and falls within Article 8 of the European Convention of Human Rights.

3.5 Transparency Tools

In addition to making the life of individuals more 'opaque' to outside groups (where individuals desire that) there exists another set of tools that are used in the European arena in order to protect the privacy of individuals. These take the form of Data Protection Laws. Such tools pose important requirements on inter alia the use of medial data (and are thus relevant for a project such as PICASO). On the European level, Data Protection Directive 94/46/EC attempted to harmonise the laws amongst its member states with regards to the processing of personal data[36]. The aim of such laws is to provide limits on the processing of personal data (i.e. the collection use storage of such data). They place various specific procedural safeguards in place in order to protect individual privacy and to promote accountability amongst private and public record holders. The European Data Protection regime has its origins in the principles laid down in Article 8 of the ECHR, but it goes further by limiting what data processors can do with individual data even if consent has been given. Its main requirements are:[37]

1. Everyone has the right to the protection of personal data concerning him or herself (this document will go on to illustrate this includes medical data such as that which will be used by the PICASO project).

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data that has been collected concerning him or herself and the right to have it rectified.

[30] P.G. and G.H. v UK No. 44787/98

[31] Copland v UK No. 62617/00

[32] Gutwirth, S., & De Hert, P. (2008). Regulating Profiling in a Democratic Consitutonal State. In M. Hilderbant, & S. Gutwirth, Profiling the European Citizen. Cross-Disciplinary Perspectives. (pp. 271-291). Springer Science.

[33] E Mantovani and P Quinn, "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements," *International Review of Law, Computers & Technology* DOI:10.1080/13600869.2013.801581 (2013).

[34] (case number 20511/03)

[35] Disucssed further in section 5

[36] It must be acknowledged that a primary motive for the European Commission in drafting the Data Protection Directive was also to aid the promotion of a single market in information. The varying laws on information processing between member states were seen as being harmful to the confidence of individuals in giving their consent to data being sent to and used in other European States. This was thought to be causing economic problems and so harmonisation was therefore needed to remove this problem. See Gutwirth, S. (2002). Privacy and the Information Age. Rowman & Littlefield Publishers P 91. Another primary motive was the acceptance and legitimisation of the fact that public authorites have a right to process personal data on individuals. There are thefore various excemptions in data protection legislations exempting public bodies from many of the obligations that private ones face. See: De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement. Opacity of the Indivdiual and Transparency of Power. In E. Claes, A. Duff, & G. S, Privacy and the Criminal Law (pp. 61-102). Intersentia.

[37] Rouvroy, A., & Poullet, Y. (2009). The Right to Informational Self-Determination and the Value of Self Development: Researching the Importance of Privacy for Democarcy. In S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne, & Nouwt, Reinventing Data Pro P71

3. Compliance with these rules shall be subject to control by an independent authority.

The Data Protection Directive has been dubbed a transparency tool as it is concerned with increasing the transparency of the processing of personnel data.[38]. Transparency tools provide confidence to individuals that if they give their consent for their data to be used that it will only be used in the manner in which they consented and in line with recognised requirements relating to the 'good processing' of personal data.' Such rules mean that PICASO will have to process personal data in a correct manner, subject to important legal requirements, even where they have gained consent for the processing of such data. As section 5.4discusses below Directive 95/46/EC has recently been replaced by Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data known as the General Data Protection Regulation (or 'the GDPR)'. The specific requirements of these regimes will be discussed in further details below.

3.6 Opacity and Transparency in Tandem

The role of opacity tools is quite different in nature to those of transparency tools. Opacity tools embody normative choices about the limits of power; transparency tools come into play after the normative choices have been made in order to channel the normatively accepted exercise of power[39]. The techniques of opacity and transparency are used in tandem by the law in order to protect individual privacy and represent important protections in our democratic society. Transparency tools are particularly useful for regulating relationships between private actors. Such techniques will be important in PICASO in order not only so that PICASO meets the its legal requirements (in terms of Data Protection Legislation) but so that it respects to the greatest extent possible the privacy of its users, something that relates to the ethical demands that will be placed upon the project. By the use of such tools in appropriate circumstance it should be possible to protect the privacy of patients with regards to their ability to practice informational self-determination whilst receiving quality healthcare. At present for example laws across Europe that relate to patient confidentiality which exist alongside data protection. This document will however focus mainly on the latter category for three key reasons. First, they are more extensive and far reaching than laws on patient confidentiality. Second, they are more complex and as a consequence offer more protection to potential data subjects than the more traditional laws on patient confidentiality. Third, laws on data protection are more harmonised across Europe, making them easier to describe in a concise way.

[38] Gutwirth, S., & De Hert, P. (2008). Regulating Profiling in a Democratic Consitutonal State. In M. Hilderbant, & S. Gutwirth, Profiling the European Citizen. Cross-Disciplinary Perspectives. (pp. 271-291). Springer Science.

[39] De Hert, P., & Gutwirth, S. (2006). Privacy, Data Protection and Law Enforcement. Ocity of the Indivdiual and Transparency of Power. In E. Claes, A. Duff, & G. S, Privacy and the Criminal Law (pp. 61-102). Intersentia.

4 Privacy in Law at the European Level

The EU and the ECHR are a complimentary Sources of Privacy Law in Europe. The most prominent source of law relating to privacy at the European level is the case law of the European Court of Human Rights (the ECtHR).[40] This court has ruled that art. 8 ECHR of the convention relates to a wide range of issues including integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, etc. (discussed previously in section 3). The court has confirmed that privacy is a relational concept that goes well beyond a mere right to intimacy, with the important consequence that art. 8 rights may also protect visible and public features and conduct of individuals (public privacy).[41] The Strasbourg Court has over time, acknowledged that individual self-determination or autonomy is an important principle underlying its interpretation of art. 8.[42] A strong tendency has also emerged in the Court's case law toward imposing on European states not only the need to respect privacy, but also to realise those conditions that are necessary to fulfil one's life.[43] Such case law may be relevant for a project such a PICASO which may monitor individuals in the privacy of their own home and make use of the data that arises therefrom.

Unlike the European Convention of Human Rights, the EEC and EC as forerunners to the EU were not established with Human Rights as their primary focus. The original treaties of the European Communities accordingly made no mention of human rights or measures that should be taken in order to secure their protection. The European Court of Justice 'the 'ECJ' (which is responsible for ensuring enforcement of the EU treaties) has however developed a range of approaches that aim at grant protection to the individuals. It has done so by developing a new system that brings the fundamental rights into the general principles of European law mentioned above. These general principles reflect the content of human rights protection found in national constitutions and human rights treaties, in particular the ECHR. In 2000 the EU made a significant step in bringing citizens closer to the EU by proclaiming the Charter of Fundamental Rights. It was a political document, however it entered into force after the enactment of the Lisbon Treaty in 2009 (see art. 6 (1) TEU).

The Charter explicitly recognizes the fundamental right to privacy in art. 7 under the notion 'respect for private and family life', stating: "everyone has the right to respect for his or her private and family life, home and communications." Article 8 also calls specially for the protection of personal data. The application of the Charter is however intended to be upon the activities of European Institutions and the implementation of EU law.[44] In areas that are not related to these, this will be of little concern.[45] The content of the ECHR and the CFR is similar, furthermore the latter refers to the former as well. Art 52. (3) Charter states that as it "contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention."

[40] In accordance with art. 52(3) of the EU Charter, the meaning and scope of this right are the same as those in the corresponding article of the ECHR. Consequently, the meaning is the same and the limitations which may legitimately be imposed on this right are the same as those allowed by art. 8 of the ECHR

[41] For example: Rotaru vs Romania of 4 May 2000, § 43; P.G. & J.H. vs U.K., of 25 September 2001, § 57, Peck vs U.K.,of 28 January 2003, § 58.

[42] Pretty vs U.K., of 29 April 2002, § 61, Judgment: "As the Court has had previous occasion to remark, the concept of 'private life' is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (X. and Y. v. the Netherlands judgment of 26 March 1985, Series A no. 91, 11, § 22). It can sometimes embrace aspects of an individual's physical and social identity (Mikulic v. Croatia, no. 53176/99 [Sect. 1], judgment of 7 February 2002, § 53). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by art. 8 (see e.g. the B. v. France judgment of 25 March 1992, Series A no. 232-C, § 63; the Burghartz v. Switzerland judgment of 22 February 1994, Series A no. 280-B, § 24; the Dudgeon v. the United Kingdom judgment of 22 October 1991, Series A no. 45, § 41, and the Laskey, Jaggard and Brown v. the United Kingdom judgment of 19 February 1997, Reports 1997-1, § 36). Art. 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, Burghartz v. Switzerland, Commission's report, op. cit., § 47; Friedl v. Austria, Series A no. 305-B, Commission's report, § 45). Though no previous case has established as such any right to self-determination as being contained in art. 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees."

[43] ECtHR, Botta v. Italy (1998) 26 EHRR 241; ECtHR, Kutzner v. Germany (2002) EHRR 653. 1991) 14 EHRR 319

[44] This is described by art. 51 (1), which says: "The provisions of this Charter are addressed to the institutions and bodies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law. They shall therefore respect the rights, observe the principles and promote the application thereof in accordance with their respective powers."

[45] Ibid. In ERT case the Court found that EU human rights law applies to Member States not only when they are implementing EU law, but whenever they are „acting within the scope of Community law." If this is the criterion, then the Charter applies not only when States directly implement an EU norm, but also when they derogate therefrom, maybe even when their acts may simply affect Union law at large. The external limits of the Charters' effects are still to be delineated, admittedly, and will probably remain unresolved unless the Court of Justice of the EU (CJEU) sets up a new test to identify them.

Fundamental rights (such as the right to private life) are not absolute rights, their limitation is possible, however the limitation "must be provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality… are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[46]

It must be underlined that privacy and data protection are not only protected by legal means. A number of extra-legal tools – i.e. methodologies, best practices and standards, among others – have been developed since the early 1990s to supplement the former. The most important tools are Privacy Enhancing Technologies (PETs),[47] Privacy by Design[48] and Privacy Impact Assessments[49]. These privacy protection tools are not meant to replace the legal means of protection, but rather to supplement and support them. Indeed such requirements are also slowly becoming part of the legal systems (i.e. as part of the GDPR) and are acquiring the status of enforceable obligations for public authorities, organizations and corporations (discussed further in section 5).[50]

Example of ECJ case law: C-101/01, Lindquist, 6.11.2003
In this case the court ruled that posting information online that a worker had fractured her foot constituted the processing of medical data and therefore was subject to all the requirements that apply to such data. In this case the employer did not realise that simply posting the details of such an innocuous event could amount to the processing of sensitive medical data.
Consequence: It is necessary to realise that many forms of data may represent health data which by its nature is sensitive data and demanding of extra protection.

[46] Art. 52 (1) Charter.

[47] PETs refer to a "system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system."

[48] PbD can be understood as a manifestation of a strong precautionary approach in privacy protection which motivates organisations to take proactive measures to privacy and data protection. PbD helps to make privacy the default setting, affecting both IT systems, business practices, and networked infrastructure. It is in strong connection with PIA, since it identifies the privacy risks, and Privacy by Design can provide mitigating measures in the developing phase.

[49] According to Wright and De Hert Privacy Impact Assessment is "a process for assessing the impacts on privacy a project, policy, programme, service, product or other initiative and, in consultation with the stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts"

[50] *Article 25 of the GDPR for examples demands that data controllers implement the engineering requirement of 'data protection by design'.*

5 The EU's data protection approach

At European level, the most important elements of legislation in the field of data protection are article 8 of the Charter, the EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, referred to as the Data Protection Directive, and, as its successor, the Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, commonly known as the General Data Protection Regulation. Provisions, relating to data protection, can be found both in primary and secondary law of the EU. The former refers to the EU treaties (TEU and TFEU) and represents general principles and commitments that often serve as cornerstones for more precise legislative and judicial initiatives. The latter refers to the aforementioned legislative initiatives (such as Regulations and Directives) and represents more complex and detailed, binding provisions that can be applied in a wide range of circumstances. The most important elements of this framework will be emphasised in details below.

5.1 Fundamental commitments in primary law

The Charter of Fundamental Rights was originally a political document, but it became legally binding as EU primary law with the Lisbon Treaty in 2009. The Charter not only guarantees the right to private and family life (art. 7) but also establishes the right to the protection of personal data (art. 8):

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Additionally, the Treaties include explicit reference to the right to the protection of personal data as well. Art. 16 TFEU and art. 39 TEU both recognise the aforementioned right. The CJEU ensures the uniform application of this right.

5.2 Current EU legislative initiatives (secondary law)

The EU has taken numerous specific legislative initiatives with regard to data protection. Most of these are in a form of directives which have been implemented or transposed into national law. This process of implementation allows member states some variation along national lines whilst preserving the essential context of the directive. Currently the most important instruments are:

- Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data
- Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws
- Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters[51]

[51] This Framework Decision aimed to fill the gap left by the restricted scope of the Data Protection Directive, by providing a regulatory framework for the protection of personal data in the area of police and judicial cooperation, or what was called the "third pillar" before the entry into force of the Lisbon Treaty.

- Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[52]

It is also very important to take note of the opinions expressed by the Article 29 Data Protection Working Party. Formed of a representative from each Member State's national data protection authority, the European Data Protection Supervisor and the European Commission, this body gives expert advices regarding data protection, and promotes common application of the Data Protection Directive and from 2018 the Regulation with changed duties and powers, as the European Data Protection Board. It must be underlined that all of the above mentioned legal documents will be affected by the data protection framework reform, which concluded recently. The next chapter will provide a brief summary regarding the most important elements of this reform with special attention to the General Data Protection Regulation which as of May 2018 will become the most important piece of EU legislation concerning data protection.

5.3 The Role of Data Protection

Data Protection is one of the most important elements of privacy protection. It represents one of the most important legal approaches towards safeguarding individual privacy. Data protection approaches protect privacy primarily in three main ways.

(i) Promoting autonomy over the use of one's personal data[53]
(ii) Laying down rules concerning how and when such personal data can be used
(iii) Providing transparency over the use of personal data

Data protection frameworks normally contain elements that are related to all three of these principles. Often these principles work in a symbiotic or complimentary manner. Providing transparency for example is indispensable if individuals are to be able to exercise autonomy over the use of their data i.e. provide consent. In the same manner individuals can only be expected to consent where they can be sure that their data will only be processed in accordance with well established rules (hence the need for data protection frameworks in the form of binding law).

The relevance of such rules in the medical context (including in trials such as those envisaged in PICASO) is obvious. Many forms of medical treatment produce and make use of personal health data. As discussed below with reference to European data protection law health data is seen as sensitive data, meaning that its incorrect use poses an elevated threat to individual privacy and should be subject to strict control. Part of this control is ensuring that consent has been obtained in the correct form.[54] In order to provide such consent however individuals must be 'informed', meaning that they must provide sufficient clarity about what is going to occur with their data, including what will be done with it and by whom.[55] The application of EU data protection legislation to such a context will be discussed further below.

5.4 The EU Data Protection Reform

The drafting of the data protection reform package (which will replace the 95/46/EC Data Protection Directive) was concluded in December 2015. The drafting of the General Data Protection Regulation was a long and exhaustive process. In 2010 the Commission announced its plans to reform the EU data protection framework. The Directive was then 15 years old, thus technologically out of date, and the level of harmonisation between Member States was not sufficient. With the Lisbon Treaty and the Charter the EU has given the reinforced emphasis on data protection as a fundamental right.[56] After the public consultation the Commission released a communication, followed by the Council, the Parliament, the European Data Protection Supervisor and the Working Party.[57] Two years later, in January 2012 the Commission released the first draft of the General Data

[52]. This Regulation is particularly important because, inter alia, it created the European Data Protection Supervisor, an autonomous EU institution with the powers of supervision, consultation and co-operation (art. 41).

[53] Such a Principle is not absolute – both Directive 95/46/EC and the GDRP recognize that there are other basis for the processing of personal data than just consent (e..g. for scientific research). Such exceptions come with important conditionality however and must be read narrowly).

[54] For more in depth analysis of this requirement see the WP 29 Opinion on the Electronic Health Record. (WP 131) 2007

[55] *See section 5.17 for a discussion on the informational requirements upon data controllers under the GDPR*

[56] *This is discussed futher in section 5.1*

[57] *For more on the EDPS and its views on the GDPR see https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation*

Protection Regulation and started the second phase where the Council and the Parliament was given the chance to comment and amend the draft. After considering 3999 amendments to the draft Regulation the Parliament released its views in March 2014. The Council reached a common position in the first reading and published it in June 2015. Due to the relatively late response, the Council based its work not only on the version of the Commission but on the version of the Parliament and on the recent CJEU case law as well. After the draft of the Council the tripartite negotiations, between the Parliament, the Council and the Commission, began. An almost six-year long process ended, when the three institutions announced the final outcomes of the EU data protection reform package in December 2015. The finalised language was approved in April 2016, thus the Regulation will come into force on 25 May 2018.

One of the main aims of the Regulation is to provide an adequate response to the contemporary challenges of the information society. The Regulation will, to a certain extent, solve the harmonisation problems, caused by the Directive, as it will be directly applicable.[58] This will enhance the effectiveness of the framework, not to mention the qualitative change it evokes. This is an important and far reaching development as the new instrument is expected to affect the way Europeans work and live together. To underline its importance, data protection will move to EU level from the level of Member States. As Recital (9) GDPR underlines: *"Directive 95/46/EC… has not prevented fragmentation in the way data protection is implemented across the Union, legal uncertainty and a widespread public perception that there are significant risks for the protection of individuals..."*

Given that the GDPR will come into force (25 May 2018) before the end of PICASO as a project, it will be necessary to ensure that the project is compliant with both the regime set forth by Directive 95/46/EC and the GDPR. As a consequence, this deliverable will also take into account the new Regulation, with special attention to its new or newly developed data processing principles. As the following section will make clear, the GDPR has a number of new requirements that were not present in Directive 95/46/EC.

5.5 Important Definitions in Data Protection law

For a better understanding of the EU data protection framework there are some core definitions which must be taken into account. It is important to be aware of such definitions in order to discern where and how PICASO might engage personal data and what requirements may therefore exist relating to such data:

- **Personal data** – Art. 4 (1) GDPR provides a definition of personal data: any information relating to an identified or identifiable natural person. The definition is strongly connected to the notion of the data subject. In the Lindqvist[59] case the European Court of Justice (ECJ) argued, that the fact that it was mentioned in an Internet web site that an individual had injured her foot and was on half time leave on medical grounds constituted personal data.
- **Genetic data** – Genetic data is a special type of personal data which relates to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question. According to Recital (34) “genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained.”
- **Biometric data** – This type of personal data might be relevant in PICASO, as it relates to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person
- **Personal data concerning health** – Data concerning health relates to the physical or mental health of a natural person. It should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. Data relating to health is always classed as sensitive data and attracts a stricter regime of data protection. (The requirements in terms of the necessary legal base for the processing of health data are described in article 9 of the GDRP).
- **Data subject** – Art 4 (1) in its definition of personal data also refers to the data subject (identified or identifiable natural person). Although exceptions exist, European data protection law protects the living

[58] *As section 5.18 however discusses, article 9(4) of the the GDPR means that harmonisation in the area of health data will be limited.*
[59] *See section 3.6*

being, should he be identified or identifiable through any information relating to him. The Data Protection Directive does not clarify when a natural person should be considered identified, however the role of identification is to describe a person in a way that he becomes “distinguishable from all other persons and recognised as an individual”.

- **Data controller** – In the interpretation of the Regulation data controller is someone who „alone or jointly with others determines the purposes and means of the processing of personal data”.[60] The definition is based on three separate building blocks: personal aspect (the data controller can be either a natural or legal person, however, according to the Working Party preference should be given to the latter), possibility of pluralistic control (referring to the joint controllership, whereas different parties act as controllers), and the elements which distinguish the controller from other actors (as the controller is able to determine the purposes and means of the processing[61]).
- **Data processor** – according to art. 4 (8) processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Compared with the controller, the processor is not able to determine the purposes and means of the processing operations.
- **Data processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

5.6 The importance of the 'Data Controller'/'Processor Distinction'

(i) The concepts are more clearly defined in the GDPR.

As described above the GDPR defines both the terms 'data controller' and 'data processor. The GDPR marks a change where the obligations concerning both the involvement of a data processor and data controller are more clearly described. In directive 95/46/EC the concept of a data processor was more vague, as was his or her responsibilities. This led to a lack of clarity as to the responsibilities of 'data processor', particularly in situations where the relationship with the data subject was only vicarious (i.e. there was no direct relationship between the two). In such situations the rights of the data controller *viz-á-viz* such third parties were not clear. Such a relationship could arise where the data controller subcontracts out particular processing activities to specialist third parties that are able to carry out the desired processing in a manner that the data controller is not able to or in a less expensive manner. A more and more prominent example of this involves cloud computing services. In such situations data controllers my make use of third party cloud services to store or process the relevant personal data in a way that the data controller may not be able to. This could for example be because the cloud service, is cheaper, more secure or allows access to multiple users in a way that would not otherwise be possible.

This concept of 'data controller' and 'data processor' will be important from the perspective of the PICASO project. This is because 'PICASO as an exploitable product' likely foresees some use of cloud based storage and processing. Whilst it is not possible to know at this stage what form such processing would take (or indeed if it would for certain involve the use of personal data) it is worth considering what requirements 'data controllers' and 'data processors' would likely face. Perhaps one of the most important implications of the GDPR is that a data controller must enter into a contract with all data processors to ensure that personal data is processed both in a way that is compatible with the GDPR and which allows data subjects to exercise their rights *viz-á-viz* 'data processors'.[62]

(ii) Defining the processor and controller

[60] Art. 4 (7) GDPR

[61] This element had a big importance in the SWIFT case. The Society for Worldwide Interbank Financial Telecommunication (SWIFT), transferred personal data to the government of the United States. SWIFT stated that it officially operated as a data processor, although it was rejected since the company behaved as if it were a controller.

[62] *See section 5 where data subject rights are discussed.*

The definitions described in the GDPR make clear that the controller is the entity (can be a natural or legal person) that decides upon the 'purposes and means of processing' (see section 5.5). This does not necessarily mean the entity that collected the legal data but relates to the entity that decided what will happen to the data and who will do it (i.e. the identity of other data processors. The GDPR also makes it clear that there can be more than one data controller.[63] This will depend on a particular context and must be decided taking into account the exact relationship and responsibilities of each party involved. For both 'PICASO as a research project' and 'PICASO as an exploitable product' it will be necessary to discern, given the particular context that exists in each, which partners are controllers or processes and what obligations apply to each.

(iii) Responsibilities upon data controllers and data processors

According to Article 24 from the EU GDPR,

“Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.”

Meeting such requirements may include the following:[64]

- A data protection impact assessment and a risk mitigation plan;
- Implementation of pseudonymization (the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information);
- Data minimization in order to meet the requirements of this Regulation and protect the rights of data subjects.[65]

In terms of data processors, article 28 of the GDPR states

“Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.”

This article thus places an obligation upon controllers to only select potential processors based upon their ability to comply with the requirements of the GDPR, including all of the requirements discussed in this document. This includes requirements relating to territoriality (i.e. that the processing occurs in the EU).[66] For data processors there is the requirement that they act only in a way that is compatible with the instructions issued by the data controller.[67] Given that the controller must instruct the processor to act in a way that is compatible with the GDRP, this effectively imposes a requirement to follow the data protection framework, including facilitating the rights of all data subjects.

(iv) The need for a data processing contract.

Data processor activities must be governed by a binding contract with the controller. Data processors must accordingly be bound with terms that cover the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the controller. The contract must include specific requirements

[63] Article 26 GDPR

[64] For more see the ISO27001 and ISO 22301 blog available at: https://advisera.com/27001academy/blog/2017/01/30/eu-gdpr-controller-vs-processor-what-are-the-differences/

[65] *For more on data minimization see: section 5.10*

[66] As the above source identifies This means that if any EU or non-EU company wants to stay in business, as controller or processor, it will have to implement the necessary controls to ensure that they comply with the EU GDPR, because the fines can be applied to both controllers and processors.

.

[67] Article 28(2)

including *inter alia* "that the personal data is processed only on documented instructions from the controller, and requirements to assist the controller in complying with many of its obligations. The data processor has an obligation to tell the controller if it believes an instruction to hand information to the data controller breaches the GDPR or any other EU or Member State law".[68]

(v) Implications for PICASO

For both 'PICASO as a research project' and 'PICASO as an exploitable product' it will be necessary to define whether both data controllers and processors exist and who they are. In doing so it will be important to remember that a data controller is not necessarily the party collecting the data in question but the party that decides on what is done with it, how and by whom.

In PICASO as a research project the answer to this question depends on the precise arrangement decided upon and whether the respective hospital partners retain total possession over patient data or whether it is passed to other partners for further processing. Where this is the case other partners may be classed as data processors, and in such circumstances, it will be necessary to conclude a contract between the hospital partners and the other partners that are concerned in order to ensure that data is processed correctly. This will also be the case where the services of local cloud providers are used. In such cases it should be ensured that the binding contact is created between data controller (i.e. the local hospital) and data processor. Such a contract should include the specified requirements as described in the GDPR pertaining to Data Processing Contracts.

In 'PICASO as an exploitable product' it may be important to remember that there may be more than one data controller. Depending on exact circumstances (to be decided) this may be the hospitals or health institutions where they decide how the data is to be processed etc. Where there are other entities involved in processing (e.g. cloud service providers), such entities may be classed as data processors. Once again, in such instances it will be important for the relevant institution to enter into a contract with any data processors in order to ensure that the requirements of the GDP are met and that data subjects are able to exercise their rights. This may for example include requirements that such processors provide data subjects with the relevant information they need in order to exercise their rights. Such a contract should be fully considered in order to ensure that all requirements under the GDPR will be met. In addition, the data controller must take measures to ensure that any data processors are indeed able to fulfil their requirements under the GDPR.

5.7 The Possible Use of Anonymised Data in PICASO[69]

The question of the use of anonymised data is important to address in the context of the PICASO project and relates very much to the definition of personal data described above (i.e. it is linked to potential identifiability of individuals from a certain data set. The use of anonymised data is important from a legal perspective because anonymised data does not fall under the remit of the data protection framework. This is confirmed by the GDPR which states:[70]

"The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

This reflected the opinion of the Article 29 working party in its opinion on anonymisation techniques.[71] In that opinion it set what can be considered an extremely ‘high bar’ to be met for actual anonymisation to occur. If PICASO as a project opts to use anonymisation (in order to avoid compliance with the data protection framework), it will be important to ensure that the data is correctly anonymized from a legal perspective.

[68] https://www.taylorwessing.com/globaldatahub/article-obligations-on-data-processors-under-gdpr.html

[69] *Portions of this section are taken from a recent paper written by one of the authors: P Quinn, "The Anonymisation of Research Data — a Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the Eu Data Protection Framework?," European Journal of Health Law 24 (2017).*

[70] GDPR Recital 26

[71] See Article 29 Working Party Opinion on Anonymisation Techniques (April 2014) 0829/14/EN WP216,

In particular, the working party was concerned that anonymisation was not to be confused with processes of 'pseudonymisation'.[72] This has long been an issue in efforts to improve compliance with data protection demands.[73] Pseudonymisation implies that efforts have been made to reduce the possibility that a particular data set can be identified as belonging to a particular individual. This may involve removing unique identifiers such as names, social security numbers and dates of birth.[74] Whilst intuitively such measures may seem to anonymise the data in question, the reality is that they just make identification of the data subject more difficult.[75] Those in control of such (pseudonymised) datasets may be able to take certain measures to allow 're-identification' of the data subjects in question. This could for example include referencing pseudonymised datasets to master datasets where cross referencing will allow data subjects to be identified. Even where the controller of the pseudonymised dataset does not have access to such a master dataset (as is the case in more stringent forms of pseudonymisation) it may be possible, without an inordinate amount of difficulty, to identify data subjects by reference to other datasets that the data controller may be able to gain access to or which are even publicly available.[76] One common example may include records that are made public such as records of births, deaths or electoral registers. Given that the efforts required to perform such re-identification are not very onerous, such data cannot be considered as being anonymised, but merely pseudonymised.[77] Pseudonymised data may also be more vulnerable to deanonymisation by malevolent third parties.[78] Indeed, it is the effort required to re-identify (or 'deanonymise' as the working party terms it) data subjects that the working party uses as one of its primary criteria, stating that it is necessary to look at the '*means . . . that are reasonably [sic] to be used*' to deanonymise data in order to determine whether the efforts made to anonymise the data in question are sufficient.[79] This test essentially requires a determination of whether identification of individuals using the anonymised data is '*reasonably impossible'*.[80] Whilst the use of the word 'reasonably' may seem to imply a low standard for anonymisation, the working party has made it clear, in particular with its juxtaposition to the word 'impossible', that the standard is actually very high. Several factors identified by the working party are testament to this (especially when taken in combination).

First, it requires data controllers to focus on the means that would be necessary to bring about deanonymisation.[81] This requires a consideration of evolving technical possibilities in terms of computing power and the availability of algorithms that are able to deanonymise data that was thought to be anonymous. In doing so it is necessary to balance anonymisation effort and costs (in terms of both time and resources required) against the increasing availability of technical means to identify individuals in datasets and the increasing public availability of other datasets (such as those made available in connection with open data policies) that may be of use in such deanonymisation.[82]

Second, the working party has stated that, in making such a determination, it is necessary to take into account the fact that many types of publicly available datasets that are claimed to be anonymised may not meet the requisite standards of anonymisation. Such a standard requires that the party anonymizing data, not only consider their own ability to deanonymise the data in question, but also the ability of other known and unknown parties given the state of technological development and other potential sources of data that may be publicly available. Given the rapidity with which computing power is increasing and the increased availability of research data online, the threshold for true anonymisation to occur may be extremely high. Imagine for instance the use of genetic data or its publication online following research. Given the nature of the data

[72] Article 29 Working Party Opinion on Anonymisation Techniques (April 2014) 0829/14/EN WP216, p3

[73] See for example B. Clarehout and C. Demoor, 'Privacy protection for clinical and genomicdata. The use of privacy-enhancing techniques in medicine', International Journal of Medical Informatics 74 (2005) 257-265, p. 259.

[74] Whilst pseudonymisation may not constitute anonymisation it can nonetheless be an important process in protecting the privacy of individuals. See: S. Lusignan, 'Effective pseudonymisation and explicit statements of public interest to ensure the benefits of sharing health data for research, quality improvement and health service management outweigh the risks', Informatics in Primary Care 21(2) (2014) 61-63.

[75] Supra note 54, p. 414. For a discussion on the need to avoid such confusion in the proposed EU data regulation see: E. Kosta and C. Cuijpers, 'The Draft Data Protection Regulation and the Development of Data Processing Applications', in: M. Hansen, J. Hoepman, R. Leenes and D. Whitehouse (eds.), Privacy and Identity Management for Emerging Services and Technologies, IFIP Advances in Information and Communication Technology vol. 421 (Heidelberg: Springer, 2014).

[76] For an illustrative example see: L. Sweeney, Simple Demographics Often Identify People Uniquely (Pittsburgh: Carnegie Mellon University, Data Privacy Working Paper 3, 2000). Also discussed in supra note 59, pp. 403-404.

[77] Supra note 55 in Annex. In its opinion on anonymisation the working party suggested several examples of methods that could be considered as anonymisation and not just pseudonymisation.

[78] E. Khaled and C. Alvarez, 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymisation techniques', International Data Privacy Law 5(1) (2015) 73-87, p. 83. Khaled and Alvarez use the term 'third party adversary'.

[79] Article 29 Working Party Opinion on Anonymisation Techniques (April 2014) 0829/14/EN WP216, p. 3.

[80] Ibid., p. 8.

[81] Such a focus is drawn from recital 26 of Directive 95/46/EC

[82] Article 29 Working Party Opinion on Anonymisation Techniques (April 2014) 0829/14/EN WP216, p. 9.

involved (where even small DNA sequences may provide a link to specific individuals) and the potential for related information concerning the individual or a family member to exist in an accessible version elsewhere, it may be difficult to speak of genetic data as ever being truly anonymous.[83]

A third important factor is that one cannot depend upon the 'good motives of the data controller'.[84] This means that the data controller, when assessing whether a dataset he or she possesses is truly anonymous, must take into account what other data they have access to. If the controller of the supposedly anonymised data set has access to other data that will allow the identity of individuals to be decided through cross referencing the two, then it is not correct to speak of anonymised data. Given this, the data controller must make sure that those with access to anonymised data (even within their own organization) do not have access to other datasets that might facilitate deanonymisation or, must employ such a level of anonymisation so that, even with reference to other datasets, deanonymisation will not be possible. Once again, such measures where employed are likely render the dataset in question less valuable in terms of its research potential (or even remove such value altogether).

Fourth, the working party confirmed that in its opinion, the act of anonymisation itself constitutes an act of processing of personal data.[85] This is logical as in order to anonymise data the data controller must have been in possession of data that was not anonymised i.e. personal data.[86] Given this it is also logical to expect that the original dataset in question was obtained in accordance with one of the legal bases described above. This may create a 'catch 22' because it means that in order to collect personal data, even if the intention was to immediately anonymise it, it would be necessary to have the consent of the data subjects involved. Where the purpose of anonymisation is to avoid the need to obtain consent, this will present immediate problems because, where such consent has not been obtained, it may not be possible to gather the data in the first place.

The above discussion is very relevant where it is decided that PICASO (or an exploitable product that arose therefrom) will use 'anonymised data'. This could be for instance be the case in 'PICASO as an exploitable product' for example concerning data that may be held on a central cloud/orchestration unit that would be used to refer potential users of patient health records to the relevant institution. Where this is the case it will be important to apply the considerations discussed above in order to determine whether the data indeed is anonymized or not. Where this is not the case the relevant rules of data protection (at both the European and national levels will apply). Bearing this in mind it is important to remember (as the Article 29 working party has emphasized) that pseudonomised data does not constitute anonymized data. Where pseuduonymised data is used one must consider such data as personal data and apply all relevant rules of data protection.

5.8 Principles, rights and obligations in data protection law - the bedrock of data protection

The objective of the Regulation is stated in art. 1 (2), i.e. the protection of 'the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.' The main principles of data protection law must be applied in any instances of data processing where the data protection is applicable i.e. whatever the legal basis in question.[87] As a consequence, these principles will be of direct relevance to PICASO and must be applied whenever personal data is processed.[88] Such principles cannot be consented or contracted away. They must therefore be implemented no matter what the selected legal base is. This is important because it means that the data protection principles must be observed in all instances of data processing even if explicit consent has occurred. In the context of 'PICASO as research project' it is therefore important to remember that data processing principles apply even if explicit consent has been gained by the

[83] H. Schmidt and S. Callier, 'How anonymous is 'anonymous'? Some suggestions towards
a coherent universal coding system for genetic samples', Journal of Medical Ethics 38(5) (2012), doi:10.1136/medethics-2011-100181; J. Bohannon, 'Genealogy Databases Enable Naming of Anonymous DNA Donors', Science 339 (2013), doi: 10.1126/science.1339.6117.1262.

[84] Article 29 Working Party Opinion on Anonymisation Techniques (April 2014) 0829/14/EN WP216, p. 10

[85] Ibid., p. 2. The working party states 'Anonymisation constitutes a further processing ofpersonal data; as such, it must satisfy the requirement of compatibility by having regard to the legal grounds and circumstances of the further processing'.

[86] E. Khaled and C. Alvarez, 'A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymisation techniques', International Data Privacy Law 5(1) (2015) 73-87, p 79. As Khaled states: 'In order to anonymise data, it is necessary for an anonymisation engine to ingest personal data, apply anonymisation techniques to it, and then output anonymised data. The input is personal data'.

[87] The question of possessing the correct legal basis for the processing of personal data is discussed in section 5.18

[88] Most of the key data processing principles within the context of the GDPR are described in Article 5

data subject. In this way consent should not be seen as a 'carte blanche' that allows the data controller/processor to process personal data how they see fit. Rather it should be seen as a licence to allow personal data to be processed according to data protection principles as described in law. It is therefore imperative that all processing of personal data meet the requirements described below.[89] The main principles are discussed below together with their relevance for PICASO.[90]

5.9 Fairness, lawfulness and transparency of processing –

(i) Principle Content

This principle data subjects (i.e. patients in the context of PICASO) should be able to know what information has been collected about them, the purpose of its use, who can access and use it. Users should also be informed about: how to gain access to information collected about them and how they may control who has access to it. To achieve this the transparency of data processing should be ensured. Data controllers should be clearly identified and be able to respond to requests of e.g. data subjects. Controllers must therefore inform data subjects before the processing of their personal data about the main components of the processing (e.g. purpose of processing, identity and address of the controller, etc.). This principle is also linked to the notion of consent (discussed further in section 5.5) and the right of the data subject to receive adequate information (discussed in section 5.18).

(ii) Implications for PICASO

- 'PICASO as a Research Project' - In order to fulfil the requisite requirements of transparency it will be necessary to fully explain to potential data subjects in an understandable way, why their data it is being collected, what will happen with it. In the context of the 'PICASO as a research project' trials this will entail ensuring that such processes are fully disclosed on the consent form that all participants must sign. In doing so it must be ensured that information is tailored to be understandable to the relevant audience taking into account their age, level of education, cognitive capacity and their respective language.[91]
- 'PICASO as an Exploitable Project' - With regards to 'PICASO as an exploitable product' the same conditions will apply but given that consent will probably be expressed though other forms than just signed consent forms the modalities of obtaining such consent may be more complex given the need to secure consent in a granular way (this is discussed in more detail in section 5.17where the issue of explicit consent is addressed.) will have to be carefully considered.

5.10 'Data minimisation' and 'purpose limitation

(i) Principle Content

This fundamental principle of data protection is an expression coined by legal doctrine to refer to two key data protection principles, namely, the purpose limitation and the data minimisation principles. The purpose of use limitation, or purpose binding principle92 prohibits further processing which is incompatible with the original purpose(s) of the collection. The data minimisation principle must act as a general principle policy for any technological development: information systems and software shall be configured by minimising the processing of personal data. In simple terms this means that no more data is collected and processed than is strictly necessary. The purposes for which personal data are collected should be specified at the time of collection. In addition, the use of those data should be limited to those previously defined purposes.

[89] Such requirements would not however apply to the processing of anonymized data as such data is not considered to be personal data. See recital 26 of the General Data protection Regulation and section 5.3 of this document.

[90] These principles represent the principles as described in the General Data Protection Regulation which contains additional data processing principles (when compared to Directive 95/46/EC).

[91] As PICASO deliverable 3.3 discusses all consent forms have been translated into the local language i.e. Italian or German. They have also been created in line with local ethics requirements.

[92] Art. 6 (1) b) Directive

(ii) Implications for PICASO

- 'PICASO as a Research Project' - For 'PICASO as a research project 'data minimisation' and 'purpose limitation' are actually two separate but closely linked principles. In most instances however, it is not possible to fulfil one without fulfilling the other. The most important element for PICASO as a project is to be aware of the its goals as a project so as to know what data is required. Once the ultimate goals of the project are known it quickly becomes apparent which types of data are needed and which are not (relevant to data minimisation). They are also relevant in understanding what constitutes acceptable use of individual data and what goes beyond (relevant to purpose limitation). Essentially PICASO as a project must not collect data that is not needed and must not subsequently use data for purposes that went beyond the original reasons for collection. This most notably will apply to the medical institutions involved in data processing in PICASO, who will need to ensure that patient data is not kept for any longer than is strictly necessary. This will however need to be decided taking into account national data protection laws on the use of medical data.[93]
- 'PICASO as an Exploitable Project' - In terms of 'PICASO as an exploitable product' it is not possible to describe precisely what type of data is needed and what purposes it is used for. This would to a large extent depend upon the exact type of system that had been opted for (taking into account the types of patients involved, the types of chronic conditions or comorbidities involved and also the planned scope of any project). An essential task in designing the architecture in question will therefore involve designing the architecture and interfaces in such a way that will not permit unnecessary data collection. Depending upon the type of architecture used, such obligations would also be important for any party that stored data arising from PICASO and wished to use it for further purposes. This could be for example important for parties that wished to make further use of the data for commercial purposes or for scientific research. Where such purposes were not in line with the original consent that was provided further (explicit)[94] consent for the processing of data will have to be sought (for more discussion see 5.17).

5.11 Accuracy of data

(i) Principle Content

This principle implies that data must be adequate, up to date, relevant and not excessive for the purposes for which it is collected. Irrelevant data must not be collected and if it has been collected it must be discarded.[95]These key principles have been codified at constitutional level by art. 8 of the EU Charter, which states that personal data “must be processed fairly for specific purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law”.[96]

(ii) Implications for PICASO

- For both 'PICASO as a research project' and PICASO as 'an exploitable product' it will be necessary to ensure that best procedures and devices are used to ensure that data is correct. This will involve where necessary using trained staff so as to ensure that data is stored correctly. In addition, it will be essential to ensure that any devices used will be of sufficient quality in order to ensure that data is accurate to the required level of sensitivity (as section 6 discussed this may often mean that it is necessary to use devices that have been correctly certified with the CE mark).[97]

5.12 Storage limitation

(i) Principle Content

In principle data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which data were collected or for which they are further processed. This requirement may however be subject to certain requirements relating to national law that require the

[93] Discussed with important examples in Annex (section 7)

[94] See section 5.17 for a discussion of the concept of explicit consent.

[95] Art. 6 (1) c) Directive

[96] As the *travaux préparatoires* indicate, art. 8 codifies and must be read in the light of Council of Europe and European Union legislation, in particular Directive 95/46/EC.

[97] See discussion on medical devices.

retention of medical data used in clinical practice or research for defined periods.[98] Where possible data should be anonymised.

(ii) Implications for PICASO

- 'PICASO as a Research Project' - It will be necessary to ensure that all necessary precautions are taken to ensure that data is kept for no longer than is necessary. Where that data is stored solely on the hardware and under the control of the trial providers (i.e. the hospital partners) it will be the responsibility of the partners to ensure this obligation is met. This will have to be performed however in the light of specific national legal obligations that may apply to the storage of medical of clinical research data for a specific amount of time further.[99] If data is stored with online cloud providers a specific clause in the data processing contract between data controller and data processor.
- 'PICASO as an exploitable product' – For PICASO as an exploitable product it will be necessary to device procedures and systems that will identify data that is no longer needed and delete it. The specifics of such a requirement would depend upon the specific context and would also have to take into account local laws on the continued storage of health data in addition to particular context and exploitable project was designed for.

5.13 Data security

(i) Principle Content

Appropriate technical and organisational measures should be taken into consideration when personal data is processed in order to ensure the security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

(ii) Implications for PICASO

- For 'PICASO as a research project' it will be necessary to consider all relevant threats to security and take appropriate technical measures. This includes threats that arise through malevolent action or otherwise. Any contract with a data processor (including an cloud service provider) will have to ensure a legally binding requirement exists to ensure that the principle of data security is met.
- For 'PICASO as an exploitable product' it is not possible to describe specific demands without seeing the context that will be involved. Meeting this demand will demand a thorough contextual analysis taking into account the potential risks to data security that could be posed by the system in question.[100]

5.14 Data Protection by Design

(i) Principle Content

The new regulation confirmed 'data protection by design' as a data protection principle in its own right. This principle demands that data processing systems must be designed in a way from the outset that ensures data protection requirements are carried out. This includes ensuring that the data protection principles described here are implemented, that data is only processed where there is a correct legal base, and that the rights of any data subject will be respected. Of crucial importance is that data protection and its requirements are considered throughout the project including in the conceptualization, design and implementation stages of any project.

[98] Discussed with important examples in Annex

[99] *This is further discussed in* section see also annex

[100] See for the example the guidance provided by the UK Data protection supervisor at https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

(ii) Implications for PICASO

- For 'PICASO as a research project' it is necessary to ensure therefore that at each stage of design the requirements of data protection are taken into account. This means that all design partners must consider these requirements both when designing the PICASO trial infrastructure and when implementing it. This includes the legal requirements as described within this document. In order to ensure that such requirements are being implemented the PICASO foresees the internal deliverable ID3.7 Annual Compliance Monitoring Report 1 (due M28) that will review the progress made so far and where necessary make recommendations for alterations where there is a danger that data protections requirements will not be met.
- For 'PICASO as an exploitable project' it will also be necessary to take such factors into account in a contextualised manner. This starting point for any analysis should be a data protection impact assessment (IA) as is demanded by the new data protection regulation. The conclusions of the IA should be followed up at regular intervals throughout the life cycle of the project.

5.15 Privacy by Default

(i) Principle Content

This is another principle that has been introduced by the new regulation. [101] *It essentially demands that any system designed to process personal data should be designed to use the least intrusive basis as a starting point. Only with the approval of the data subject (preferably on a step-by-step and granular basis) should the processing of personal data be broadened to include further forms of processing.*

(ii) Implications for PICASO

- For 'PICASO as a research project' this principle has a lesser relevance. This is because the envisaged forms of processing are fixed from the outset. The possibility for granularity in the trial phase of the project is thus in reality limited. As a consequence, consent has been sought at the beginning of the project from the data subjects for all forms of processing that are likely to occur (through signed consent forms – see deliverable D3.3). Implementing granularity at this stage of the project would not be practical given that consent will be paper based – meaning that it would be very burdensome for both the patient and from an administrative point of view to be constantly signed new consent forms for each new data processing operation.
- The principle would however be more relevant for 'PICASO as an exploitable product'. This is because such a product would likely have granularity at its core.[102] In such a system, data subjects should be able decide on a granular basis upon their level of participation in any 'PICASO like system'. This should ideally start out from a basis of minimum participation and through processes of granular consent allow expansion. Such forms of granular consent should be in conformity with the legal requirements for explicit consent (i.e. in the case of sensitive data).[103]

5.16 Accountability[104]

(i) Principle Content

The final principle under the GDPR states that data controllers must be able to demonstrate compliance with the other principles. This is a short sentence with major implications. One of the notable changes under the GDPR compared with the DPD, is the increased compliance burden, much of which is sparked by the accountability principle. It is not enough to comply, you have to be seen to be complying. The range of

[101] *See article 25 of the GDPR.*
[102] See description in introduction to this deliverable
[103] See section 5.17 for further discussion of these requirements.
[104] The description of this principle has been taken directly from Law Firm TaylorWessing. The authors would like to convey their thanks to the this firm for its concise yet, accurate description. Available at: https://www.taylorwessing.com/globaldatahub/article-the-data-protection-principles-under-the-gdpr.html

processes that organisations have to put in place to demonstrate compliance will vary depending on the complexity of the processing but may include:

- assessing current practice and developing a data privacy governance structure which may include appointing a Data Protection Officer;
- creating a personal data inventory;
- implementing appropriate privacy notices;
- obtaining appropriate consents;
- using appropriate organisation and technical measures to ensure compliance with the data protection principles;
- using Privacy Impact Assessments; and
- creating a breach reporting mechanism.
- The use of legally binding data processing agreements where applicable.

(ii) Implications for PICASO

For both PICASO as a research project and PICASO as an exploitable project it will be necessary to implement practices associated with accountability. For the purposes of PICASO as a research project this document, together with some of the more ethical themed documents in work package 3 (including for example D3.3 The PICASO Ethical Guidelines) can be considered as an impact assessment.[105] In their entirety these documents consider the range of legal and ethical issues that are mandated by article 35 GDPR. The follow up assessment (i.e. in ID3.7) of this document will also help to ensure that the relevant requirements are met. In other regards the data controllers involved in the project must ensure that efforts are made at addressing the relative accountancy mechanisms described here.

5.17 The Legal bases for the Processing of Sensitive data

The data protection principles (whilst applying to all forms of processing of personal data) are not the only elements of data protection that must be applied. In addition, it is necessary to have a legal base for the processing of the personal data in question. Without such a base, it is not possible to process personal data, even if such processing were to be in line with data processing principles. ‘PICASO as a research project’ will process data relating to health. This constitutes sensitive personal data.[106] As a consequence it is necessary to have a relevant legal base pertaining to this type of data. The relevant legal bases are described in (laid down in art.9 GDPR):[107]

- Freely given, specific and informed consent of the data subject
- Processing for preventive or occupational medicine.[108]
- Performance of a contract to which data subject is a party
- Compliance with the legal duties of the controller
- Protection of the vital interests of the data subject (e.g. in an accident and emergency context).
- Activity carried out in the public interest or exercise of official authority
- Legitimate interest pursued by the data controller

The following sections will discuss the likely legal basis to be used by both 'PICASO as a research project' and 'PICASO as an exploitable product'.

(i) 'PICASO as a research project'

For 'PICASO as a research project' the legal basis relied upon will be informed consent. This will be secured through the use of signed consent forms to be issued to patients at each of the hospital sites.[109] In general,

[105] This is also required under art 35 GDPR

[106] . Art. 9 (1) of the Regulation prohibits “processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.” This prohibition is subject to to the exceptions decribed elsewhere in article 9.

[107] They are also described in article 8 of directive 95/46/EC

[108] For more indepth analysis of this requirement see the WP 29 Opinion on the Electronic Health Record. (WP 131) 2007

[109] For more information see deliverable 3.3

the data protection regulation makes a number of points about what is required for consent to occur. These notably include:[110]

- Data subject must give his consent freely, without undue pressure. The consent is freely given „if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent".
- Data subject must be duly informed about the consequences of giving consent. To have sufficient information before giving consent data controller must provide easily accessible information in an easily understandable language.
- The consent must be specific, reasonably concrete, which relates to the reasonable expectations of an average data subject.
- The data subject must be able to revoke consent.
- The data subject must be provided with the requisite information as described in articles 13-14 of the GDPR (this information is described further in section 5.18 below).

Given however that PIASO will be handling sensitive data the requirements for consent are stricter. Article 9(1) states:

*"the data subject has given **explicit** consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject"*[111]

The key word here is 'explicit', which denotes a higher and more formal standard for consent. However, it has not been defined what exactly this may require for various forms of electronic consent. There is however little doubt the use of signed consent forms as proposed by PICASO would meat such a requirement if it meets certain conditions:

- The person giving consent must clearly state that his actions specifically constitute an act of consent.
- The consent should be revocable
- It must be informed, i.e. the individual must be provided with the requisite information to make a decision.
- The individual must be provided with the additional information as demanded by data protection law.[112]

It should be noted that further principles relating to national law (i.e. in the case of the PICASO trials, Germany and Italy) may apply to formalities concerning consent. Relevant laws in this area are described in the annex to this document.

(ii) 'PICASO as an exploitable project'

For 'PICASO as an exploitable product' the situation is more complex. This is because two of the legal grounds used above may allow for the use of personal data as envisaged in PICASO. These are (i) 'explicit consent' and (ii) for 'processing for preventive or occupational medicine'.[113] The issues that would arise in using these two legal bases are briefly discussed below.

(i) Explicit consent – Whilst the same legal requirements (as discussed in (B) above would apply the environment in which consent is likely to be sought is likely to be different. Indeed, one of the main purposes of PICASO (see section 2) is to allow a high level of level of flexibility for patients in deciding to what extent they participate, replacing more traditional black and white forms of consent.[114] Given the use of a simple consent form (as envisaged in 'PICASO as a research project') would not be suitable. Given this, it is likely that any such system would opt for forms of digital granular consent, whereby patients would be allowed to

[110] Details are described in article 6 of the GDPR
[111] Emphasis added by author
[112] The relevant provisions describing the informational requirements upon the data controller are described in article 12-14 of the GDPR.
[113] These are described in Article 8(3) of directive 95/46/EC and Article 9(2) of the GDPR respectively.
[114] See section 2 for more description of the various formats of PICASO.

stipulate which of their data was to be shared and who with.[115] It is important however to ask what forms of granular, digital based consent would meet the requirements of 'explicit consent'. In asking this question it is necessary to look at that which separates 'normal consent' from explicit consent. In answering this question, the GDPR (in its recitals) indicates that for the former 'indications' are sufficient, this could include changing privacy settings or clicking continue after having being presented with a list of conditions.[116] With 'explicit consent' however the GDPR indicates that there must exist unambiguous consent. This does not preclude consent being given in a digital manner but seems to demand that the consent is more formalized and unmistakeably recognizable as an act of consent. Given this it is sensible that for all acts in an eHealth context to be marked as consent. This means that where a patient would alter settings in a manner synonymous to forms of granular consent he or she should be reminded that his actions constitute an act of explicit consent for legal purposes. This could be through the present of some text or a pop up box which the patient would have to acknowledge. As always is the case there is a fine balance to be drawn between the granularity of the consent and the amount and complexity of the information that is to be present. Such a line should take into account the data protection requirements described in this document.

(ii) 'Consent for processing for preventive or occupational medicine'. It is this form of consent which forms the mainstay of consent in most medical institutions. Imagine for instance the visit of a patient to see a specialist at a large hospital. In the course of his visit he may be directed to have an x-ray and to have blood tests. Additionally, he may visit two specialists at the same hospital given that he or she may have several co-morbidities. In such a situation a patient is not expected to sign a consent form for the new use of his data in each specific situation (even if it was originally unforeseen). Rather this exception allows medical professionals within the same institution to carry out further processing of patient data when it is for treatment purposes. There is however a number of conditions that have been attached to this legal ground which may limit its use, including in a situation as one might envisage in 'PICASO as an exploitable product'. This include the requirement that it only covers use within a single institution (i.e. one hospital) and that all those taking advantage of this grounds for processing are subject to professional requirements of confidentiality.[117] Given therefore that PICASO is precisely intended for use by medical professionals that are not based in the same institution and also potentially by carers (who are not subject to requirements of professional secrecy) this potential grounds for processing may be of little use.

5.18 Data Subject rights under the GDPR

(i) The importance of data subject rights

A third pillar of importance (in addition to the need to comply with data protection principles and to possess a legal base for the processing of data) is the need to ensure that individuals can utilize their rights under the data protection framework. These rights are rights that are guaranteed by law and which the data subject(s) can use *viz-á-viz* the data controller. For the data subject this provides extra possibilities to both understand what his happening to his data and also where so desired take steps to prevent certain activities from occurring. For the data controller the existence of the data subject rights will require organization efforts to ensure that such rights can be realized. This will involve looking at all processing activities and discerning how they might be impacted by the rights in question. It is also necessary to consider how such rights may be facilitated. This may involve the provision of certain forms of information. In this way there is an important link between the data subject rights and the data processing principles (which often relate to the provision of information). The

[115] For further reflection on the concept of Informed consent and issues associated with granularity in the area of mHealth see: E Mantovani and P Quinn, "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements," *International Review of Law, Computers & Technology* (2013).

[116] Recital 32 states: Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

[117] For more in-depth analysis of this requirement see the WP 29 Opinion on the Electronic Health Record. (WP 131) 2007

following sections describe the data subjects' rights as described in the GDPR. These have been expanded from those that were contained in Directive 95/46/EC. It should be noted that, given the existence of article 9(4) (which allows further measures at the Member State level) that some of the following measures will have to be read in conjunction with the existence of Member State law concerning the use of medical data (as is discussed below concerning certain rights that may be affected).

(ii) A Right to basic information and information required for the purposes of consent[118]

The GDPR demands that data subjects are furnished with sufficient information to be able to properly understand the means of and the purpose for the processing in question. The GDPR presents a list of items that are needed and which must be described to the data subject in order inter alia for consent to be gathered. In 'PICASO as a research project' it will be necessary to ensure that the information required is presented on the relevant consent forms. In 'PICASO as an exploitable product' it will be necessary to ensure that they are present in the various mechanisms of granular consent that will be used. These include:[119]

- The identity and the contact details of the controller and, where applicable, of the controller's representative
- The contact details of the data protection officer, where applicable
- The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- The recipients or categories of recipients of the personal data, if any
- Where applicable, the fact that the controller intends to transfer personal data to a third country or international organization
- The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- The existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- The existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- The right to lodge a complaint with a supervisory authority.

Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

(i) The Right of Access[120]

Data subjects are entitled to access their personal data. Such access is important for the data subject in order to discern whether his or her rights are being complied with. Data subjects have the right to receive not only access to their data but also to information concerning their data (as described above). Data controllers may charge a reasonable fee for such access (in order to deter vexatious claims for access). Whilst to comply with such a right will be relatively straightforward in 'PICASO as a research project', it may be more complicated in 'PICASO as an exploitable product' where data may be held with third parties, e.g. in online data clouds. In such instances the data controller will be obliged to ensure that a contract exists with this third party (or data processor) to ensure that data subjects are able to exercise their rights (including rights to access) against third parties.

(ii) A Right to Rectification.

[118] See GDPR Recitals 58, 60 and Articles 13 - 14

[119] Further rights in terms of information apply where the personal data is not gathered directly from the data subject but is taken from an intermediate party.

[120] Article 15 GDPR

Data subjects have a right to rectify their data where it is incorrect. Such a right is closely related to and dependent on the right to access.[121] Whilst to comply with such a right will be relatively straightforward in 'PICASO as a research project', it may be more complicated in 'PICASO as an exploitable product' where it may data may be held with third parties, e.g. in online data clouds. In such instances the data controller will be obliged to ensure that a contract exists with this third party (or data processor) to ensure that data subjects are able to exercise their rights (including a right to rectification) against third parties.

(iii) A Right of Erasure

In the negotiations for the GDPR the right of erasure was commonly touted as the so called right to be forgotten and was often discussed in the context of relationships with social media. This right allows data subjects to demand the detention of their data when its retention is no longer justified. Where the legal base for the processing of such data was consent, data subjects are entitled to withdraw their consent. This article does however make allowance for instances where the Data Controller must maintain data in order to comply with other EU or national laws. This may be important within the context of PICASO where national laws may demand that clinical or research data be kept for a longer period.[122] Similarly as with the rights described above, it will be necessary to ensure (using a data processing contract) that any third party data processors comply with such a right.

(iv) Data Portability

Data subjects are also provided with a right of data portability. More specifically this relates to a "right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format".[123] This right seemingly is limited by the use of words "which he or she has provided" which seems limit the extent of the right to the data that has been provided by the data subject and therefore not further data that has been created from subsequent processing. In a project such as PICASO this would seemingly relate to the raw data that is gathered from the patient concerned and not any specialist analysis that has been performed on top of it. According to the GDPR such data should be provided in a way that is transferable to a third party or even transferred directly to another controller where that is possible.

(v) Notification of Third Parties

Where necessary data controllers are expected to notify any third parties that may have acted as data processors in order that data subjects may utilize their data protection rights viz-a-viz such parties.[124] Such a right may be particularly important in the interlinked world of cloud computing and thus consequently of 'PICASO as an exploitable product'. In the context of the 'PICASO as a research project' however this is unlikely to be as all data will be stored on the severs of the sole data controllers, i.e. at the various hospital sites. As discussed in the section concerning the difference between data controllers/processor such arrangements should be regulated according to a contract between the two parties.

[121] See articles 5 and 16 of the GDPR.

[122] For more GDPR article 17. Article 18 also describes circumstances where processing may be restricted upon demand of the data subject (these may apply were for instance national law demands deletion.

[123] See GDPR Article 20

[124] See GDPR article 17 and 19

6 The Medical Device Framework

6.1 *Raison d'etre*

Where manufactures wish to place a new medical device on the European Market the design, manufacture and testing of the product in question will likely have to comply with the EU framework on medical devices.[125] The same may also be true where medical devices are used for solely research purposes. Given that a PICASO platform is likely to employ medical devices (e.g. in the form of monitoring devices or apps), the existence of the Medical Device Framework (MDF) is of importance. The Medical Device Framework is extremely complex and, given its flexibility, is of an ever evolving application. It can represent a significant regulatory barrier to those wishing to innovate in the area of medical devices. This complexity has been increased by the fact that the framework is currently under revision, with a new regulation currently being released. The implementation time for this new regulation is however likely to be at least 3 years (i.e. it will not be in force before 2019 at the earliest).[126]

6.2 Background

As with other areas of its intervention into healthcare regulation the MDF acts primarily so as to protect the internal market i.e. the free movement of goods[127] within the Union.[128] Prior to the introduction of the EU framework on Medical Devices in the 1990s, the regulation of medical devices was subject to the differing regimes of each member state. This created barriers to the functioning of the single market and the free circulation of medical devices. As a consequence, the Commission decided to harmonize regulation in the area of medical devices so as to remove obstacles to the internal market. In addition, the Medical Device Framework also aims to provide users in the European Single Market with a higher degree of protection than that which existed previously. This occurs by requiring that the same basic safety requirements are present throughout Europe. This was implemented by the harmonization of essential requirements and certification and inspection procedures.[129] The three EU directives, which represent the Medical Device Framework lay down numerous different requirements and basic safety standards which a product must meet before it can receive approval to be placed upon the European market. The directives in question are [130]:

- The Medical Devices Directive (MDD) 93/42/EEC amended by Directive 2007/47/EC;
- The Active Implantable Medical Devices Directive (AIMD) 90/385/EEC[131];
- The In Vitro Diagnostic Medical Devices Directive (IVDMD) 98/79/EEC.

The MDD is applicable to most medical devices, with the AIMD[132] and the IVDMD[133]
applying in only more narrowly defined circumstances. As described above, this framework will be largely

[125] P Quinn, "The Eu Commission’s Risky Choice for a Non-Riskbased Strategy on Assessment of Medical Devices," Computer Law and Security Review 31 (2017).

[126] More information on the new regulation, including the process of its formation can be found at https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/revision_it

[127] The main treaty provisions related to the freedom of movement for goods are Articles 34–36 TFEU

[128] The recitals of the Medical Devices Directive (MDD) 93/42/EEC begin by referring to the Single Market as a justification for action.

[129] Single Market Regulation on Innovation: Regulatory Reform and Experiences of Firms in the Medical Device Industry” Institute for Prospective Technological Studies Seville, October 2000 P28

[130] Note: The Medical Devices Directive (MDD) has been subsequently amended by four directives and one regulation. These are; Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998; Directive 2000/70/EC of the European Parliament and of the Council of 16 November 2000; Directive 2001/104/EC of the European Parliament and of the Council of 7 December 2001; Regulation (EC) No 1882/2003 of the European Parliament and of the Council of 29 September 2003 and Directive 2007/47/EC of the European Parliament and of the Council of 5 September 2007.[130]

[131] The Active Implantable Medical Device Directive (90/385) regulates powered implants or partial implants that are placed in and left in the human body. The definition of active implantable devices is based on the definition of medical devices and is defined as follows; 'Active medical device' means any medical device relying for its functioning on a source of electrical energy or any source of power other than that directly generated by the human body or gravity. 'Active implantable medical device' means any active medical device which is intended to be totally or partially introduced, surgically or medically, into the human body or by medical intervention into a natural orifice, and which is intended to remain after the procedure.

[132] This Directive covers all powered medical devices implanted and left in the human body, such as pacemakers, implantable defibrillators, implantable infusion pumps, cochlear implants and implantable neuromuscular stimulators. The Directive also covers implanted passive parts of active devices such as pacemaker leads and adapters, and external parts that are an essential part of the systems, e.g. pacemaker programmers.

[133] This Directive covers any medical device, reagent, reagent product, kit, instrument, apparatus or system which is intended to be used for the in vitro examination of substances derived from the human body, such as blood grouping reagents, pregnancy testing and Hepatitis B test kits.

replaced by the new Medical Device Regulation amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. In addition to this there will also be a new Regulation on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

6.3 Potential Application to PICASO

As with the discussion on data protection, given that we are presently in a period of transition it is necessary to consider the potential impact of two different legal frameworks. In both 'PICASO as a research project' and 'PICASO as an exploitable product' it will be necessary to consider the relevance of the MDD framework. This task is somewhat simpler than is the case for the data protection framework however given that the new medical device framework will not come into force before the PICASO project is over. This means in terms of the project itself (i.e. as two clinical trials) it is only necessary to consider the current framework. It is necessary however to briefly consider the new framework given that it would apply to any exploitation of the PICASO project (this will be discussed below).

In asking what aspects of PICASO could involve the use of (novel) uncertified medical device one could look at the remote monitoring aspects of the project. This will include any wearable sensors and sensors in the individual's immediate environment. It could also however include any apparatus that is used to interpret and display information. This could include for example tablets or touch screens, apps on smart phones or even the patient dashboard depending on what exactly it does (i.e. whether it merely presents existing information or interprets it in some way to allow it to perform another function). As the paragraphs below discuss depending on what function each of these devices may perform they may be subject to classification as a medical device.

6.4 The definition of a 'Medical Device'

In order to decide whether a device is even capable of being the subject matter of the Medical Device Framework (let alone which specific requirements it may be subject to) it is necessary to meet the definition of a medical device. The definition of what exactly a medical device is described as any[134]

"instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application". Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, "diagnosis, prevention, monitoring, treatment or alleviation of disease".

Devices not used for these purposes, including software, would therefore not be classed as a 'medical device' and therefore not be governed by the MDF. This means for example an IT system that merely presents medical data without extra analysis will not be considered a medical device. It will inter alia therefore be necessary to discern whether or not the items such as the 'PICASO dashboard' will actually be a medical device or not.

With regards to monitoring devices or apps, they may be considered as medical devices where "they are to be used for purpose of diagnosis, prevention, treatment or the alleviation of disease". Given the role of such devices in PICASO is to improve their medical care i.e. in diagnosing, monitoring and treating various conditions it is likely that such aspects can themselves be considered medical devices. Furthermore, software that does not perform one of the above functions itself will still be considered a medical device if it is used in combination with another medical device that does meet the above definition. Meeting the definition of a 'medical device' is therefore likely to entail the need to comply with a more onerous set of regulations[135] than might have otherwise been the case. This will entail a greater investment of money and time for those

[134] Directive 93/42/EEC Article 2(a)

[135] Other more general regulatory regimes will still however apply. One such directive that has a very general application to all products placed on the European market place is the Directive on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC). Another very generalized directive that applies to low voltage equipment is Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits. Additionally equipment that utilizes portions of the electromagnetic spectrum must often meet the conditions of the EMC Directive, i.e. Council Directive of 25July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

manufacturers concerned.[136]

6.5 Software alone or in combination with a physical apparatus can be a medical device.

Directive 2007/47/EC represented an important innovation to the MDD framework, not least because it introduced software as a technology category that could also be classified independently as a Medical Device. This applies not only to standard medical devices but also to active implantable medical devices. This innovation had become important because in the years since the original directives were enacted, the prominence of software as a medical device has increased dramatically. Indeed, in many cases, the software itself can now represent all or perhaps the most important and complicated part of the medical device in question. The range of functions that such software could perform is enormous, in some cases calculating the dose of a particular drug that should be administered to a patient but not actually being involved in such administration, whilst in other cases the software might be built into an implanted device that plays a role within the body itself. Indeed, the use of software has allowed an ever greater increase in the complexity of medical devices. With such an increase in complexity however comes an increase in dangers to those that are using such devices.[137] The wide range of possible roles software can play as a medical device made its explicit introduction by Directive 2007/47/EC necessary.

The expansion in the definition of what exactly constitutes a medical device means that manufactures of software in/for medical devices will have to take care to ensure that the device in question meets the requirements of the directive.[138] Additionally, if the software in question is not itself a medical device but is responsible for controlling another physical device that fits within the definition of a medical device, then such software itself will be classified as a medical device. Other types of software that will be caught by the device include software used in analyzing patient data generated by a medical device with a view towards diagnosis and monitoring. This could include software used to provide images from scans or even data analysis tools that interpret data provided from other devices. Software that meets such criteria must be approved under the MDD criteria and itself carry the CE mark of approval.

Manufacturers of software that can be categorized as medical devices face several important problems that do not occur as commonly for manufactures of other more conventional medical devices. One such example is software updates. Such updates are a common feature of many computer programs including those used in medical devices. Such updates may be installed regularly during maintenance or possibly even uploaded automatically through the Internet. Though easy to miss, it is important for manufacturers to follow correct procedures for such updates, making sure that the update in question complies with the MDD.[139] This may entail once again following all the rigorous regulatory testing requirements (and placing of the CE mark) that were required when the original program was developed.

6.6 Software that falls outside of the Medical device framework

(i) Devices that carry out a function not found in the MDF

Whether or not a potential innovation is likely to meet the definition of a medical device will be an important consideration for manufacturers, one which they are likely to give careful consideration to. Although the

[136] For example trial of medical devices must obtain the strict informed consent of all participants. This rules out all trials on individuals that are medically incapacitated for example. See: Singer., E, (2002) “Implications of the EU directive on clinical trials for emergency medicine”, British Medical Journal, 324, (7347), 1169–1170

[137] Mc Caffery., F and Coleman., G, (2007), “Developing a configuration management capability model for the medical device industry”, International Journal of Information Systems and Change Management, 2, 139-154

[138] Forsström., J (1997) “Why certification of medical software would be useful?”, The International Journal of Medical Informatics, 47, 3, 143-151. “The main argument to resist all attempts to regulate medical software has been that it is impossible to guarantee that software is error-free. This is true of all software. However, in medical software the correctness of medical knowledge is at least as important as the correctness of the code itself. The medical contents of the software could usually be evaluated but the end-users do not have the time or possibilities to do so”.

[139] This means ensuring that changes are well documented, validated and approved. All significant changes must be reported to the relevant notified body. If the changes made alter the classification of the Medical device manufacturers will have to perform a new conformity assessment for the device in general. If a CE certificate was issued for previous versions of software i.e. where the software itself was considered a device the manufacturer must nonetheless contact the notified body informing it of the changes that have been carried out. Standard EN 60601-1-4 provides guidelines on how this can be done.

definition in the MDD Framework is extensive there will be numerous types of software which may have a pseudo medical function and that will not fit within the definition above of a medical device. Such program will escape the need for compliance with the MDD Framework. Such software could come in many forms. Examples could include educational software designed to train medical professionals or software designed to manage databases such a patient records. Where such devices do not involve monitoring, diagnosis or treatment (as speculated by the MDF definition) they will not constitute medical devices for the purposes of the MDF.

(ii) The Importance of the intended purpose concept[140]

Given that compliance with the MDF is onerous, it may seem intuitive that manufacturers that are making products that are not actually intended to be used as medical devices are not required to comply with the requirements of the MDF (though they may be required to comply with other types of regulation related to consumer protection in general).[141] This may be relevant for example, where although manufacturers had not intended that their product would be used as a medical device, it was conceivable, given its respective properties, that it could be used as such. Imagine for instance a manufacturer that had created a thermometer for use in industrial contexts. It would seemingly be unfair to subject such a manufacturer to the rigors of the MDF because such a device could also be used incidentally for medical purposes. The MDF framework (both current and prospective) recognises this issue by incorporating the concept of 'intended purpose' into its definition of what actually constitutes a medical device. In the current Medical Device Directive for example, a medical device is defined in Article 1(2) as (emphasis added by author):

"Any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software ***intended by its manufacturer*** *to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application". Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, "diagnosis, prevention, monitoring, treatment or alleviation of disease."*[142]

According to Article 1(2)(g), intended use (or purpose) is defined as:

"intended purpose' means the use for which the device is intended according to the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials;"

A broadly similar concept exists in the proposal for the new regulation in Article 2(1).[143] It states:

"'medical device' means any instrument, apparatus, appliance, software, implant, reagent, material or other article, intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the specific medical purposes of: diagnosis, prevention, monitoring, treatment or alleviation of disease,. . ."[144]

Once again (as indicated by the author's own emphasis), the concept of intended use is central to the definition of what exactly a medical device is. A simple reading of both definitions means that without the explicit intention

[140] Much of this section is taken from Quinn, "The Eu Commission's Risky Choice for a Non-Riskbased Strategy on Assessment of Medical Devices."

[141] There are a variety of legislative instruments that are potentially applicable to mHealth products. These instruments vary in terms of the severity of the regulation in which they impose. At one end, these range from all-encompassing directives on product safety that apply to all products (including electrical products e.g. The Low Voltage Directive 2006/95/EC) sold on the European market which impose lesser, though still important requirements. At the other end of this spectrum are the directives that form the Medical Device Framework; these impose tougher regulatory hurdles only on products that meet the definition of medical devices. Even where the MDF does not however apply, other important frameworks related to consumer protection are likely to apply. These include Council Directive 85/374/EEC on the Approximation of the Laws, Regulations and Administrative Provisions of the Member States Concerning Liability for Defective Products. OJ L210/29, which offers general protection to consumers purchasing or using products within the EU. Such general protection would therefore apply to mHealth apps even if the MDF does not.

[142] Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare Within the Regulatory Framework of Medical Devices MEDDEV 2.1/6 July 2016.

[143] Proposal for a Regulation of the European Parliament and of the Council on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009.

[144] This article also includes the following activities – "diagnosis, monitoring, treatment, alleviation of or compensation for an injury or disability", "investigation, replacement or modification of the anatomy or of a physiological process or state", "control or support of conception – disinfection

of a manufacturer to create a medical device, there is no medical device, even if essentially the device seemingly meets all other types of criteria. Article 14 provides further protection for manufactures who do not intend to produce medical devices stating:

"A distributor, importer or other natural or legal person shall assume the obligations incumbent on manufacturers if he . . . changes the intended purpose of a device already placed on the market or put into service"

The EU Commission has itself confirmed such a vision, including in the context of potential medical devices that take the form of 'stand-alone' software. In its guidance on the qualification and classification of stand-alone software to be used for healthcare purposes, it simply referred to Article 1(2) of Directive 93/42/EC (discussed above) and the need to consult labelling, instructions and promotional materials.[145] In the case of Brain Products GmbH[146] the European Court of Justice confirmed that the concept of 'intended purpose' represented the desire of the legislator to require the express intention of the manufacturer of a device that it be intended for a medical purpose. The court also confirmed that this applies to software stating:

"As regards software, the legislature thus made unequivocally clear that in order for it to fall within the scope of Directive 93/42 it is not sufficient that it be used in a medical context, but that it is also necessary that the intended purpose, defined by the manufacturer, is specifically medical."[147]

The Brain Products case was noteworthy given it involved a device that would allow human brain activity to be recorded. This is something that a potential competitor argued would fall within the definition of Article 1(2), in particular under the category of devices that are concerned with "investigation, replacement or modification of the anatomy or of a physiological process".[148] In response, the court explicitly underlined the effects of the Directive 2007/47,[149] which explicitly underline the importance of the 'intended purpose' concept concerning medical devices that consist of software. The explicit role of the 'intended use' concept in this amendment to the medical device framework was taken by the court as an affirmation of the legislators' intention to apply it across the whole of the framework.[150]

6.7 The Use of Medical Devices in a Research Project (such as PICASO).

Given the foregoing discussion it likely that the MDF would apply to most medical devices in PICASO were they to be placed on the Market. Within the context of 'PICASO as a project' however this is of indirect concern. Of far more pertinence is how the MDF will apply to those devices that are used within the project. Of potential relevance within the PICASO project are for example the software components used within the patient dashboard. Given that they are novel and are being demonstrated for the first time they are uncertified (i.e. they do not possess the CE Mark). This raises the question of whether it is necessary to apply for such certification in the manner that is demanded by the MDF. This would entail a rather onerous requirement in terms of testing the devices in question and the necessary administrative work that would accompany certification. Given the nature of the PICASO trial and their ultimate purpose however it does not seem likely that this will be the case for the potential medical devices that are to be used within this project. This is because the devices used in PICASO will only be used for demonstration purposes and not for actual treatment purpose. Such thinking is described clearly in Recital 8 of the IVD Directive 98/79/EC states:

"Whereas instruments, apparatus, appliances, materials or other articles, including software, which are intended to be used for research purposes, without any medical objective, are not regarded as devices for performance evaluation."

[145] Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare Within the Regulatory Framework of Medical Devices MEDDEV 2.1/6 July 2016.
[146] Brain Products GmbH v Bio Semi VOF, Case C-219/11,
[147] Brain Products GmbH para 17.
[148] Brain Products GmbH para. 11–15. It had been argued that such a purpose was different than the other defined versions in Article (2)1 in that it did not necessarily relate to a medical process (given that it is possible to monitor healthy individuals) and that as a result the non-inclusion of the term 'intended' in this particular paragraph. The court however rejected a finding that the concept of intended purpose applied to all definitions of a medical device found within Article 2(1).
[149] Directive 2007/47/EC of the European Parliament and of the Council amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EC concerning the placing of biocidal products on the market.
[150] Brain Products GmbH para. 17, 34.

Whilst this directive itself is not likely to be relevant to the project it is useful in illustrating the scope of application of the MDF in general terms. *"'For research use only products do not have an intended medical purpose. When a medical purpose has been established based on sufficient and broadly agreed upon scientific, diagnostic and clinical evidence, then the product must comply with the requirements of the Directive before the manufacturer can place it on the market…"*[151] Given that in PICASO the potential medical devices and system architecture are for demonstration purposes only (and will not be used to alter the actual diagnosis or treatment of any patients involved in the trials) they will not meet the definition of intended purpose described above. As a consequence, these devices will not have to comply with the essential requirements or go through the certification process (an affixing the CE Mark). This will be important for example in the context of 'PICASO as a research project'.

6.8 Exploitation of PICASO or PICASO products – Applicable Requirements

The aim of the PICASO project is to demonstrate potential medical devices and an architecture that could potentially in the future be exploited and placed on the market. In order to be placed on the market however (i.e. subsequent to the competition of PICASO and through further development of the medical devices in question), all products that fall within the scope of the directive and meet its requirements are required to bear an EC conformity mark to show compliance with the MDF. The aim of this is to allow products that conform to the directive's requirements to be sold freely throughout the EEA without hindrance from national governments.

6.9 The role of standards within the MDD Framework

The MDD Framework represents only a limited harmonization of essential device requirements. This harmonization is restricted to adoption of certain essential safety criteria with which all products must conform to. The requirements are worded in a general manner so as to be adaptable to as wide as possible a range of situations. In order to ensure that the MDD Framework aids in creating a single market for medical devices where such essential requirements are not expressed within the directive a system of mutual recognition is employed. Under such a system, devices recognized by the relevant body in one Member State as meeting its standards, must be recognized in others. The directive therefore uses a dual approach, one that utilizes both the concepts of mutual recognition and harmonization.

The MDD recognizes that medical device manufacturers can demonstrate adherence to the directives' essential requirement by following standards relevant to their area of expertise. Manufacturers can use standards to set out objective definitions of what the necessary requirements would be for a particular device. The European Standards bodies CEN and CENELEC have the role of ensuring that further technical guidelines are produced within harmonized European standards.[152] These bodies are tasked with producing European standards that, once formed, are binding on all bodies within the Member States. This reduces the possibility of conflicts between different standards, such as those that might have been produced by bodies in the Member States before the establishment of a single European set of standards. Despite the importance and the potential benefit of using standards, their use is voluntary. This voluntary nature of standards within the MDD framework is important. This is because standards are primarily based upon previous experience with medical devices. Given that novel, innovative products might be very different than those products that have proceeded them, the need to meet pre-existing standards designed with different medical devices in mind might hamper further innovation. The voluntary nature of these standards means that manufacturers are able to use alternative methods to demonstrate the safety of their products.[153] Such flexibility will be important for innovations in m-Health that will often be in domains that do not have clear precedents. There are a number of software standards available that manufacturers can use to demonstrate compliance with the MDD's essential requirements. Despite this possible flexibility, it is, in order to facilitate a regulatory process more

[151] IVD Guidance : Research Use Only products - A Guide For Manufacturers and Notified Bodies MEDDEV. 2.14/2 rev.1. Feburary 2004

[152] Single Market Regulation on Innovation: Regulatory Reform and Experiences of Firms in the Medical Device Industry" Institute for Prospective Technological Studies Seville, October 2000 P28

[153] These include national and international standards that have not been given the status of
harmonized, industry standards, internal manufacturer standard operating procedures developed by an individual manufacturer and not related to an international standard and also where possible current state of the art techniques related to performance, material, design, methods, processes or practices. See Single Market Regulation on Innovation: Regulatory Reform and Experiences of Firms in the Medical Device Industry" Institute for Prospective Technological Studies Seville, October 2000 P28

conducive to innovation, important that standards for m-Health are developed and regularly updated. This is because adherence to such standards is a certain method of ensuring compliance with the essential requirements of the MDD.[154] This makes the task of manufacturers easier as available standards mean the availability of clear roadmaps to follow. Where existing standards are not suitable, manufactures do not have to follow them if they are able to demonstrate using other methods that the medical device in question meets such standards. This freedom is important in allowing innovators the flexibility to bring new products to the market, though it can entail, in effect, a greater burden of proof for manufacturers.

6.10 The New Medical Framework would be applicable to any future exploitation of PICASO

As discussed above in section 6.2the current Medical Device regimes dates from as far back as 1993. There was therefore a self-evident need to review and reform the framework. This process has been underway since 2012 and has involved a major exercise in consultation with patients, the medical device industry and medical professionals. The main element of the new MDF will be the Medical Device Regulation. The importance of opting for a regulation in place of a directive (as was formerly the case) is that it will be directly applicable in Member State legal systems (unlike a directive that must be transposed. General agreement over the text reached between the Council was reached in Many 2016 and the finalized version has been released in May 2017. Some of the most striking changes are summarized briefly below:

- The scope of the regulation will be extended to non medical devices - this will involve covering some products that do not have an intended medical purpose but which carry a risk that is analogous to certain medical devices. This includes contact lenses and certain instruments use in cosmetic surgery.[155]

- Post market surveillance will be boosted, requiring the manufacturer to monitor developments related to the device once it has been placed on the market. [156] Manufacturers will also have to make a periodic safety report.[157]

- Devices will be easier to trace. They will receive a unique identification number. They will also have to be entered on a Euramed data base that is centrally maintained. This will allow potential users across Europe to access details about a particular device.[158]

- A requirement on notified bodies to better scrutinize conformity assessments will be introduced.[159] This will entail looking for evidence that corroborates conformity assessments. Such a requirement will apply to class IIb and class III devices.

- Device Classifications will change. Whilst the same classes will remain (i.e. I, IIa, IIb and III) the rules concerning them will be modified. Such changes concern primarily active implantable devices (which are not relevant to PICASO) but also relate to medical devices that are essentially software and medical devices (discussed further below)

- In terms of the clinical investigations required to gain certification stricter rules will apply to the types of clinical investigations that are necessary in order to demonstrate conformity.[160] This will inter alia require making sufficient data available concerning the clinical investigations undertaken. And demonstrating that the endpoints of the clinical investigation relates to aspects such as intended purpose, clinical benefits, performance and safety.

[154] The following standards have already been harmonised throughout the EU and are available for use by manufacturers in showing conformity with the MDD's essential requirements. These include EN 60601-1:2005 – relating to general requirements for basic safety and essential performance, EN60601-1-4 relating to programmable electrical medical systems, EN 60601-1-6 relating to useability and EN 62304 relating to standards for risk-management-driven life cycle requirements for medical device software.

[155] Medical Device Regulation Chapter I Article 1

[156] Medical Device Regulation Chapter 5

[157] Article 86

[158] Medical Device Regulation Chapter III Article 27

[159] Medical Device Regulation Chapter IV Article 44

[160] Medical Device Regulation Chapter VI, Articles 49 - 60

6.11 The Importance of Device categorization

The MDD framework recognizes that different classes of medical devices exist, to which different levels of stringency should be applied.[161] Such variety means that it would not be conducive to innovation in general to apply the most stringent sets of standards to all products as some will by their very nature carry less risk than others. This means that manufacturers' products may face different regulatory hurdles depending upon the type of device in question. These potential differences are important because, depending on the class of medical device involved, the regulatory burden can vary enormously. It is therefore important for the PICASO project to be aware of what class of device it may be developing in order to understand what kind of regulatory burden may exist. In doing so this deliverable will consider the system of classification to be employed under the new regulation given that it is those requirements that are likely to be in force by the time any commercialization would could about.

Class I represents the class with the least stringent form of regulation. This is because manufacturers of devices in this class merely have to make a declaration of conformity concerning the medical device in question. In doing so they declare that the device meets the essential requirements for that class. They do not however have to deal with the notified bodies, nor will assessment of the application of the medical device essential requirements be scrutinised. Given this, this can be considered as the least onerous category. It is unlikely however that the potential devices that may be developed from a PICASO project would fall into this category. This is because class I devices do not include active devices. These are devices that use electrical energy. Given that the potential devices used in PICASO will all be electrical in nature (e.g. monitoring devices, apps or the patient dashboard) they will not likely fall within class II.

The types of medical devices use within the PICASO project would likely fall within Class IIa or IIb. The question of which is important because the conditions attached to class IIb are more onerous. Whilst for both, some level of investigation is required, the requirements for the later are more onerous.[162] One of the most important differences is the level of scrutiny that notified bodies must apply with the regulation requiring that applications falling in class IIb are scrutinised more in depth and more often.[163] The requirements for notified bodies in terms of their audit responsibilities are described in depth in Annex IV of the regulation.

Rule 10a of the new regulation states that software intended to provide information which is used to take decisions with diagnosis or therapeutic purposes is in general Class IIa except:

- if such decisions may have an impact capable or directly or indirectly bringing about the death or an irreversible deterioration of the state of health, in which case it is in class III;
- Where such decisions are capable of bringing about a serious deterioration of the state of health or a surgical intervention, in which case it is in class IIb.
- The general regime laid out in the regulation (also in rule 10) concerning software 'intended to monitor physiological processes' states that it shall fall in class IIa, except:
- Where the software is intended for monitoring of vital physiological parameters, or;
- where the nature of variations is such that it could result in immediate danger to the patient, in which case it is in class IIb.
- All other software is in class I.

[161] The classification of medical device products follows criteria outlined in Annex IX of Directive 93/42 EEC. It contains definitions and 18 rules that are a set of broad statements relating to product properties, functions and intended purpose rather than a list of products. This has the advantage of being more flexible and better able to take new technological developments into consideration. A list of products on the other hand would only require constant updating.

[162] The requirements for the conformity assessment for class IIa devices are described in Chapters I and III of Annex IX

[163] The frequency and the sampling basis of the assessment of the technical documentation on a representative basis as set out in the third paragraph of Section 2.3 and in Section 3.5 of Annex IX in the case of class IIa and class IIb devices, and in Section 10.2 of Annex XI in the case of class IIa devices;

Whilst any determination at this stage (i.e. during the life of the PICASO project) is conjectural, it may be helpful to theorize as to what type of medical devices may be involved in PICASO like a system were it to be exploited after the project has concluded. At the point of writing this deliverable it is not possible to state whether any medical devices that would arrive as a result of PICASO would fall into the category of Class IIa or IIb. The answer to this question will depend whether such devices would be intended for use in decisions that are "capable of bringing about a serious deterioration of the state of health", promoting "a surgical intervention" or "could result in immediate danger to the patient". Whilst it is not possible to answer this question definitively at this stage (i.e. during the context of a research project that merely intended to demonstrate feasibility, it seems probable from the perspective of the author of this deliverable that class IIb would be the most likely categorization). This is because the type of use described in PICASO envisages deployment in order to coordinate healthcare for individuals with potentially multiple chronic health conditions and potential serious co-morbidities. Given this it seems likely the information from such medical devices especially for example the patient dashboard or the software behind it (if that is indeed a medical device) would be used in ways that have been described here and are indicative of a class IIb device. In such case the procedures in terms of conformity assessment (described above) and the essential requirements referred to in the Annex of this deliverable should be complied with.

7 ANNEX I Specific Legal Requirements Present in Italy and Germany.

As section 5 discusses, at present data protection law is highly heterogeneous across Europe. The reason for this is that that the legislative instrument originally opted for was a directive (i.e. Directive 95/46/EC). A directive allows Member States to implement its content in a manner of their choosing (so long as the broad requirements of the directive are met). The result of the varying transposition into national law that occurred meant that although data protection law is broadly similar, it differs from Member State to Member State in fine detail. Unfortunately for technology developers however such fine detail is extremely important and often makes it extremely difficult to develop a single technological solution and/or practice that I likely to be compliant in all member states.

Whilst the GDRP is a regulation (which does not require transposition to have legal effect) the situation may not change to a great extent for health data. This is because article 9(4) seeing allows Member States to maintain and enact further provisions that would be applicable to sensitive data. This includes health data. The result of this is that is still necessary to take into account Member State laws when one intends to process health data.

For both 'PICASO as a research project' and 'PICASO as an exploitable product' it will be necessary to take into Member State Laws on the processing of health data. In 'PICASO as a research project' it will be necessary to take into account the laws of both Germany and Italy on such matters (given that they are the locations of the PICASO trials. For 'PICASO as an exploitable product' it will be necessary to take into account the laws of each Member State where use is intended (unfortunately an overview of such laws is beyond the scope of this report).

The rest of this document represents sections that were taken from reports provided to the EU Commission concerning the the laws concerning Electronic Health Records in each EU Member State. They have been selected because the provide a good overview of the relevant law in the two Member States where the PICASO trials will take place. The two respective reports are:

"Overview of the national laws on electronic health records in the EU Member States - National Report for Germany"[164]

"Overview of the national laws on electronic health records in the EU Member States - National Report for Italy"[165]

7.1 2. Legal requirements applying to EHRs in Italy

[164] This Report wad prepared by Milieu Ltd and Time.lex under Contract 2013 63 02. *This report was completed by Prof. Dr. Nikolaus Forgó and Ass. iur. Fritz-Ulli Pieper. The views expressed herein are those of the consultants alone and do not necessarily represent the official views of the Consumers, Health and Food Executive Agency (Chafea).*

[165] *Ibid*

2.1. Health data to be included in EHRs

The table below provides a comprehensive description of the legal requirements applying to EHRs in Italy. The EHRs is regulated by the d.l. of 18 October 2012, No. 179. The Decree of implementation of the D.L. 179/2012 has not been adopted yet.

7.2 Table on health data

Questions	*Legal reference*	*Detailed description*
Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)	*D.L. 179/2012* *2011 Ministry of Health Guidelines*	*Article 12(1) of D.L. 179/2012 defines the EHR as "a set of health and socio-health digital data and documents related to present and past clinical events regarding a patient". The d.l. No. 179 of 18 October 2012, does not enumerate the information that should be included in the EHRs.* *Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish the content of EHRs.* *Pending the adoption of the implementing ministerial decree, it may be worth recalling that the 2011 Ministry of Health Guidelines set out recommendations on the content of EHRs, which should include:* *- patient identification data;* *- administrative information regarding the patient's history in the National Health Service;* *- socio-health and health documents (reports, emergency reports, discharge letters);* *- patient summary (a document created by the general practitioner who collects the clinical history of the patient);* *- patient's personal notebook (a document created by the patient);* *- patient's statement on the donation of organs and tissues.*
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	*D.L. 179/2012*	*Article 12(1) of D.L. 179/2012 states that EHRs contain, in addition to health data, "socio-health" data. However, there is no clear definition of socio-health data in the D.L. 179/2012.* *Article 12(7) of D.L. 179/2012 provided that implementing ministerial decree(s) shall establish the content of EHRs.* *The "pharmaceutical dossier" is also part of the EHRs.* *The patient may also upload the medical data in his possession into the system.*

Questions	***Legal reference***	***Detailed description***
Is there a definition of EHR or patient's summary provided in the national legislation?	*D.L. 179/2012* *2011 Ministry of Health Guidelines*	*Article 12(1) of D.L. 179/2012 defines the EHR as "a set of health and socio-health digital data and documents related to present and past clinical events regarding a patient".* *The D.L. 179/2012 does not lay down a definition of patient's summary.* *A definition of "patient's summary" is laid down in section 3.4 of the Guidelines. Article 4 (1) of implementation decree, defines the patient summary.*
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	*D.L. 179/2012* *2011 Ministry of Health Guidelines*	*Article 12(1) of D.L. 179/2012 states that EHRs contain health data as well as socio-health. Article 12(7) provides that implementing ministerial decree(s) shall establish the content of EHRs.* *The D.L. 179/2012 does not enumerate the information that should be included in the EHRs. A list of the relevant information will be contained in the Decree of implementation of the d.l. No. 179. A more detailed provision is contained in the National Guidelines on Electronic Health Records of 2011.*
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	*.D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not contain any provision on common terminology or coding. Article 12(7) provides that implementing ministerial decree(s) shall establish data codification systems.*
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?	*D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not specify whether creating separate categories of data with different levels of confidentiality in EHRs is necessary. However, Article 12(7) provides that implementing ministerial decree(s) shall establish different levels and modalities of access to EHR data, depending on the role of the person exercising the access and the purpose of access.*

Questions	***Legal reference***	***Detailed description***
		Special safeguards apply in relation to health data and documents regarding HIV-positive persons, women who underwent abortion or decided to give birth anonymously, victims of sexual violence or paedophilia, persons with addictions to drugs or alcohol. Relevant data and documents may only be made visible with an explicit consent of the person concerned.
Are there any specific rules on identification of patients in EHRs?	*D.L. 179/2012* *Digital Administration Code*	*Article 12(7) of D.L. 179/2012 states that the patient's unique identification code (to be made operational by the implementing ministerial decree(s)) shall not allow the direct identification of the patient. Identification data in EHRs may not be used for purposes other than prevention, diagnosis, treatment and rehabilitation of patients.* *Insofar as identification for the purposes of accessing EHRs is concerned, the patient may access his EHR by means of the electronic identity card, national service card, or the public system for the management of the digital identities of citizens and business described in Article 64 of the Digital Administration Code (Articles 10(1) and 24(2)).*
Is there is a specific identification number for eHealth purposes?	*D.L. 179/2012*	*Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish unique identification codes which do not allow the direct identification of the patient, as regards to purposes of studying, scientific researching and health planning.*

7.3 Requirements on the institution hosting EHRs data

Main findings

The D.L. 179/2012 does not lay down specific requirements on the institutions hosting EHR data. However, in mandating the adoption of implementing measures, it states that the criteria of the Public Connectivity System established by the Digital Administration Code must be observed.

The Digital Administration Code (and other relevant sources specified in the table) stipulates that the IT services underpinning the Public Connectivity System may only be provided by suppliers who meet certain requirements. Insofar as the EHR system will be integrated into the Public Connectivity System, those safeguards will be relevant for the purposes of this study.

In addition, certain rules set out in the Personal Data Protection Code – notably as regards encryption of health data – are applicable, as are the security measures established by the Digital Administration Code.

Lastly, there are the Guidelines for regional project plans presentation on the Electronic Health Record, issued by Agency for Digital Italy and Ministry of Health.

Questions	*Legal reference*	*Detailed description*
Are there specific national rules about the hosting and management of data from EHRs?	*D.L. 179/2012* *Digital Administration Code* *Personal Data Protection Code*	*The D.L. 179/2012 does not lay down any specific rule regarding the hosting and management of EHR data.* *General principles contained in the Digital Administration Code and in the Personal Data Protection Code apply.* *However, these rules are not specific to EHRs.*
Is there a need for a specific authorisation or licence to host and process data from EHRs?	*D.L. 179/2012* *Digital Administration Code*	*The D.L. 179/2012 does not require any specific authorisation or licence to host and process EHR data.* *However, the D.L. 179/2012 makes reference to the fact that EHR systems must comply with the rules of the Public Connectivity System established by the Digital Administration Code (Articles 12(7) and 26(2), respectively). Under that Code, only suppliers meeting certain criteria may provide relevant IT services. Although they would enter into a contract with the public authorities, as opposed to receiving an authorisation or licence, they are still scrutinised in accordance with legal criteria.* *Also see answer to the next question.*
Are there specific obligations that apply to institutions hosting and managing data from EHRs (e.g. capacity, qualified staff, or technical tools/policies on security confidentiality)?	*Digital Administration Code* *2008 decree* *Personal Data Protection Code*	*The D.L. 179/2012 does not lay down any particular provision regarding the characteristics of the institution hosting or managing EHR data. However, it requires implementing ministerial decrees to define guarantees and security measures and to ensure compliance with the technical rules of the Public Connectivity System.* *Both the Digital Administration Code, the 2008 decree and the Supplier Qualification Regulation envisage that suppliers of services for the purposes of the Public Connectivity System must have certain characteristics, notably in terms of infrastructure, experience, commercial network and technical assistance, financial soundness.*

Questions	*Legal reference*	*Detailed description*
		Moreover, general rules on security of personal data (Title V of the Personal Data Protection Code) apply. Personal data must be hosted and protected in such a way as to reduce the risk of destruction, loss, unauthorised access or processing, taking into account technical progress and the nature of the data (Art. 31, Personal Data Protection Code). As a minimum, the rules on the processing and hosting of personal data by electronic means laid down in Article 34 and Annex B to the Personal Data Protection Code must be complied with. These include secure authentication, the use of an authorisation system for access, the keeping of back-up copies of data, as well as data encryption.
In particular, is there any obligation to have the information included in EHRs encrypted?	*D.L. 179/2012* *Personal Data Protection Code* - *Annex B*	*Article 12 of D.L. 179/2012 provides that the implementing ministerial decree(s) must establish guarantees and security measures applicable to the processing of patients' personal data (processing includes the holding of personal data). However, it does not expressly require that data must be encrypted.* *Nevertheless, a requirement for encryption of personal data concerning health is laid down in Article 34(1)(h) of the Personal Data Protection Code.* *The Point 24, Annex B, of the Personal Data Protection Code, shall in particular require that "Health care bodies and professionals shall process data* *disclosing health and sex life as contained in lists, registers or data banks in accordance with the mechanisms referred to in Section 22(6) of the Code also in order to ensure that said data are processed separately from the other personal data allowing data subjects to be identified directly"*
Are there any specific auditing requirements for institutions hosting and processing EHRs?	*Digital Administration Code* *2008 decree* *Supplier Qualification Regulation*	*D.L. 179/2012 does not lay down any specific rule regarding auditing of institutions hosting and processing EHRs.* *However, both the Digital Administration Code, the 2008 decree and the Supplier Qualification Regulation clarify that suppliers of the Public Connectivity System are subject to controls by the Coordinating Commission of the Public Connectivity System and the regions.*

Questions	***Legal reference***	***Detailed description***
	2011 Ministry of Health Guidelines	*A requirement on operators tracking and audit is laid down in section 6 of the Guidelines.*

7.4 Patient consent

Main findings

The D.L. 179/2012 expressly provides that the free and informed consent of the patient is necessary in order for information to be included in the EHR. Freedom of consent is preserved by the rule that refusal to give consent can never prejudice the patient's right to health services.

The D.L. 179/2012 does not specify what information must be given to the patient in order for his consent to be considered as "informed".

The D.L. 179/2012 does not lay down any specific requirement of form for the patient's consent. The general rule of the Personal Data Protection Code therefore applies, to the effect that consent may also be given orally. In this case, it is recorded in writing by the health operator.

It is noteworthy that the D.L. 179/2012 does not make any distinction between internal and cross-border situations. The rules summarised above are therefore applicable to both cases.

Finally, there is no provision specific to the sharing of (as opposed to access to) EHR data.

Questions	*Legal reference*	*Detailed description*
Are there specific national rules on consent from the patient to set-up EHRs?	*D.L. 179/2012* *Personal Data Protection Code* *2011 Ministry of Health Guidelines*	*Article 12(3-bis) of D.L. 179/2012 states that data may be uploaded into the EHRs only if the patient consents. The patient may also decide which health data shall not be included in the EHR.* *According to general principles on data protection, consent must be informed. The patient shall receive complete information on the processing of personal data in EHRs. The consent is also required by the Guidelines on the Electronic Health Record and the Health File of the Italian Data Protection Authority. Moreover, according to the Guidelines, the consent must specifically refer to the processing of data in EHRs and it is always possible to withdraw it.* *Consent must also be free. Therefore, Article 12(5) of D.L. 179/2012 adds that failure to consent access to EHR data does not prejudice the patient's right to health services. The patient can freely refuse or give the consent to the processing as the D.L. 179/2012 provides that the lack of consent does not affect the right to health.* *On the Guidelines there is a specific section (section 5.1.2) about the consent, wich requires that the consent must be "explicit".*
Is a materialised consent needed?	*Personal Data Protection Code*	*Article 12 of D.L. 179/2012 does not lay down any specific requirement of form for consent to the processing of personal data in the EHRs.* *The general rule of Article 81 of the Personal Data Protection Code therefore applies, according to which consent may also be oral. In such a case, it has to be registered in written form by the health professional.*
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the	*Personal Data Protection Code*	*Article 12 of D.L. 179/2012 does not lay down any specific requirement to inform the patient about the purpose of EHRs and the consequence of his consent or refusal to give consent.*

Questions	*Legal reference*	*Detailed description*
consent or withholding consent to create EHRs?	*D.L. 179/2012* *Italian Data Protection Authority, Guidelines on the Electronic Health Record and the Health File* *2011 Ministry of Health Guidelines*	*The D.L. 179/2012 states that data can be uploaded on the EHRs only with the patient's consent (Art. 12, par. 3 a).* *Pending the entry into force of the implementing decree, general rules apply, notably Articles 78, 79 and 80 of the Personal Data Protection Code. These provisions set out simplified requirements under which general practitioners, paediatricians, public and private health centres, and other public bodies have to inform the patient about the processing of personal data in a clear and easily comprehensible manner. Such information must highlight, in particular, the processing of personal data which poses specific risks for fundamental rights and freedoms, or the dignity of the patient (express examples include telemedicine). The patients shall be fully informed on the processing of personal data in EHRs prior to his or her consent. The information must get across to the patient with a clear and simple language. All elements of Art. 13 of d. lgs. No. 196 of 30 June 2003 shall be disclosed. The patient should also be informed that the lack of consent does not affect his or her right to the health. Information shall include the aims and modalities of processing, the consequences of a refusal, the persons or categories of persons to whom data may be communicated or who may access them.*
Are there specific national rules on consent from the patient to share data?	*D.L. 179/2012* *2011 Ministry of Health Guidelines* *Personal Data Protection Code*	*Article 12(5) of D.L. 179/2012 provides that the EHR may only be accessed if the patient consents, except for the case of health emergency.* *However, consent properly regards access to (not sharing of) EHR data.* *It may also be worth recalling Article 79 of the Personal Data Protection Code, according to which private and public health bodies may seek consent in relation to several health services even if they are provided by different units of the same bodies – whether or not in the same location – provided they are specifically*

Questions	*Legal reference*	*Detailed description*
		identified.
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	*D.L. 179/2012* *Personal Data Protection Code*	*As explained above, patient consent to the processing of personal data in the EHRs has to be specific and explicit.* *No opt-out rules are in place.*
Are there any opt-in/opt-out rules for patient consent with regard to sharing of EHRs?	*D.L. 179/2012* *Personal Data Protection Code*	*As explained above, access to data in EHRs is subject to the patient giving consent. The patient may decide not to allow certain persons to access EHR data. No opt-out rules are in place.*
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?	*D.L. 179/2012* *2011 Ministry of Health Guidelines*	*General principles apply: the patient must be informed about the persons who will have access to his EHR (Article 7(2)).* *On the Guidelines there is a specific section (section 5.1.1) with a few requirements.*
Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?	*D.L. 179/2012*	*The D.L. 179/2012 does not lay down any specific provision in this regard. Article 12(5) of D.L. 179/2012 requires the patient's consent for accessing EHR data, without making a distinction between internal and cross-border situations. Therefore, patient's consent should be equally required in both internal and cross-border situations.*
Are there specific rules on patient consent to share data on a cross-border situation?		*See previous answer.*

7.5 Creation, access to and update of EHRs

Main findings

The D.L. 179/2012 requires regions and autonomous provinces to establish EHRs by 30 June 2015. It will then be for the persons taking care of the patient within the National Health Service or regional health services to insert information into EHRs, if the patient consents. There is no clear obligation for relevant operators to actually feed information into EHRs, however.

The patient's consent is also required for accessing the EHR, save in the case of emergencies. The exception notably includes situations in which the relevant risk does not regard the patient individually, such as public health emergencies. Moreover, consent is not needed where EHRs are accessed for the purposes of research, health planning and evaluation, as in these cases identification data may not be utilised.

The D.L. 179/2012 foresees that different persons should have different rights to access or modify EHR data.

Article 12 (2) of the D.L. 179/2012 states that the patient must be able to access his EHR, in accordance with general rights derived from the Personal Data Protection Code
In order to facilitate interoperability, including at European level, D.L. 179/2012 requires implementing measures to establish relevant codification and interoperability systems.

Questions	*Legal reference*	*Detailed description*
Are there any specific national rules regarding who can create and where can EHRs be created?	*D.L. 179/2012*	*Article 12(2) of the D.L. 179/2012 states that regions and autonomous provinces shall establish EHRs by 30 June 2015. This provision refers to the systems necessary to implement EHRs.* *The subsequent paragraph 3 provides that the persons taking care of the patient within the National Health Service or the regional health services shall feed information into the EHR. The patient may also request that health information in his possession be included in the EHR.* *Article 12(7) further mandates the adoption of implementing ministerial decree(s) which shall, among other things, define the tasks of persons participating in the implementation of EHRs.*
Are there specific national rules on access and update to EHRs?	*D.L. 179/2012*	*Access to EHR data for health care purposes is only allowed if the patient has given is consent, save for emergency situations (Article 12(5), D.L. 179/2012). Access for other purposes (research, health planning and evaluation) does not require the patient's consent because his identification data may not be utilised in these cases (Article 12(6), D.L. 179/2012).* *Information may only be included in the EHR by persons offering health care treatments to the patient in the framework of the National Health Service or regional health services. Patient's consent is required (Article 12(3)-(3-bis), D.L. 179/2012). Moreover, the patient may request that health information in his possession be included in the EHR (Article 12(3), D.L. 179/2012).* *It may be worth noting that the revocation of consent for the inclusion of data into the EHR does not prevent the correction of information already included in the EHR.*
Are there different categories of access for different health	*D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not specify whether creating separate categories of access for different health professionals is necessary.*

Questions	***Legal reference***	***Detailed description***
professionals?	 *2011 Ministry of Health Guidelines*	*However, Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish different levels and modalities of access to EHR data, depending on the role of the person exercising the access and the purpose of access.* *On the Guidelines there is a specific section (section 6.2) about different categories and different access profiles.*
Are patients entitled to access their EHRs?	*Personal Data Protection Code*	*Article 12 (2) of D.L. 179/2012 specifies that the patients must be able to access their EHRs.* *Moreover, the general rule of the Personal Data Protection Code is that persons have the right to access their personal data (Article 7).*
Can patient have access to all of EHR content?	*Personal Data Protection Code*	*See previous answer.*
Can patient download all or some of EHR content?	*Personal Data Protection Code*	*Article 12 of D.L. 179/2012 does not specify whether patients must be able to download EHR data.* *However, implementing ministerial decree(s) shall establish different modalities of access to EHR data.*
Can patient update their record, modify and erase EHR content?	*D.L. 179/2012* *Personal Data Protection Code*	*D.L. 179/2012 only states that the patient may request the inclusion of health data in his possession into their EHR (Article 12(3)).* *Only in relation to his personal notebook included in the EHR may the patient make autonomous changes (Article 13(2)).* *According to general provisions on data protection, the patients have the right to supplement, update, and rectify, if necessary, their personal data. It is not possible to change the health information uploaded by doctors.*
Do different types of health professionals have the same rights	*D.L. 179/2012*	*Every professional can only process necessary and relevant data to perform his or her duties. This is one of the fundamental principles*

Questions	Legal reference	Detailed description
to update EHRs?	*Personal Data Protection Code* *2011 Ministry of Health Guidelines*	*applied in the processing of personal data.* *Pending the entry into force of the draft implementing decree, the rule of differential rights may be derived from the general provision that the processing of personal data (which includes their amendment) must comply with the principle of relevance, completeness and necessity with regard to the purposes for which personal data are collected or processed* *(Article 11(1) of the Personal Data Protection Code).* *Article 12 of D.L. 179/2012 does not specify whether different categories of health professionals must have different rights to update EHRs. However, Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish different levels and modalities of access to EHR data, depending on the role of the person exercising the access and the purpose of access.* *On the Guidelines there is a specific section (section 6.2) about different access profiles (and consequently about "right to update").*
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	*D.L. 179/2012* *Italian Data Protection Authority Guidelines on the Electronic Health Record and the Health File*	*Article 12 of D.L. 179/2012 does not lay down any explicit prohibition to access EHR data based on certain specific professions. However, insofar as Article 12(2)-(4) only allow access for certain specific purposes (notably prevention, diagnosis, treatment and rehabilitation) and to certain categories of health professionals (those within the framework of the National Health Service and regional health services), access by other entities and for other purposes should be excluded.* *On the Guidelines a specific section (section 4), defines the exclusion of "expert witnesses, insurance companies, employers, associations".*
Are there exceptions to the access	*D.L. 179/2012*	*In this case, Art. 82 of d. lgs. No. 196 of 30 June 2003 is applicable.*

requirements (e.g. in case of emergency)?		*According to this provision, the consent to the processing of personal data may be given after the processing in case of serious, imminent and*

Questions	***Legal reference***	***Detailed description***
		irreparable risk for the health or bodily integrity and when providing medical care may be negatively affected -in terms of its timeliness or effectiveness- by the need to obtain the data subject's prior consent. Article 12(5) of D.L. 179/2012 explicitly excludes that prior consent is necessary for accessing EHR data in health emergency situations.
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	*D.L. 179/2012* *2011 Ministry of Health Guidelines*	*Article 12 of D.L. 179/2012 does not set out any rule on the identification or authentication of health professionals. However, Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall define the modalities of access to EHRs.* *The Decree of implementation of the d.l. No. 179 of 18 October 2012 will establish different levels of security to access to EHRs. Among the security measures that should be adopted, the Italian D.P.A. Guidelines includes "suitable authentication and authorization systems for the employees depending on the roles and needs of accessing and processing".* *On the Guidelines there is a specific section (section 6) about "Definition of roles, profiles, and access mode".*
Does the patient have the right to know who has accessed to his/her EHRs?	*D.L. 179/2012* *Data Protection Code*	*There is no a specific prevision. General principles apply.*
Is there an obligation on health professionals to update EHRs?	*D.L. 179/2012*	*As far as the d.l. No. 179 of 18 October 2012, the answer is no. However, an obligation to update the information contained in EHRs might arise from contractual provisions, professional duties and ethical principles.* *It cannot however be excluded that rules introduced by regions or autonomous provinces, or internal rules to the National Health Service or regional health services may introduce such an obligation.*
Are there any provisions for accessing data on 'behalf of' and for	*Personal Data Protection Code*	*Article 12 of D.L. 179/2012 does not provide for the possibility of accessing EHR data on behalf of someone else or for providing a second*

Questions	***Legal reference***	***Detailed description***
request for second opinion?		*opinion.* *The d.l. No. 179 of 18 October 2012 does not expressly regulated the situation. However, general principles apply.*
Is there in place an identification code system for cross-border healthcare purpose?	*D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not contain any provision on code systems for cross-border health care purposes. However, Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish data codification systems and criteria for interoperability at European level.*
Are there any measures that consider access to EHRs from health professionals in another Member State?	*D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not contain any provision on access to EHRs from health professionals in other Member States. However, Article 12(7) of D.L. 179/2012 provides that implementing ministerial decree(s) shall establish data codification systems and criteria for interoperability at European level.*

7.6 Liability

Main findings

National legislation does not set out liability rules specific to EHRs. However, a few general rules are relevant and worth mentioning.

First of all, the Personal Data Protection Code provides that whoever causes damage as a consequence of the processing of personal data must restore the damage. "Processing" includes the registration of personal data, as well as their deletion. Both economic and moral damages may be restored. A special rule on burden of proof typical of dangerous activities applies – the person who carried out the processing is presumed to be liable, unless he can prove that the damage occurred despite him having taken all appropriate measures to avoid it.

Secondly, the Personal Data Protection Code and the Criminal Code sanction certain behaviours such as abusive access to IT systems, failure to adopt certain minimum measures to ensure the security of data, etc.

Finally, it is worth mentioning that no obligation is placed on health professionals to access EHRs before treating a patient.

Questions	*Legal reference*	*Detailed description*
Does the national legislation set specific medical liability requirements related to the use of EHRs?	*D.L. 179/2012*	*National legislation does not set specific medical liability requirement related to the use of the EHRs.*
Can patients be held liable for erasing key medical information in EHRs?	*D.L. 179/2012*	*Article 12 of D.L. 179/2012 does not address this matter.*
Can physicians be held liable because of input errors?	*Civil code* *Personal Data Protection Code*	*National legislation does not set specific medical liability requirements related to the use of the EHRs.* *Professional liability might arise from the uploading a incorrect information (whether it was negligent, reckless, or intentional). However, a diagnosis cannot be based only on EHR.* *General rules apply. In particular, Article 15 of the Personal Data Protection Code* *states that whoever causes a damage as a consequence of the processing of personal data must restore the damage. Both economic and moral damages may be restored. A special rule on burden of proof typical of dangerous activities applies – the person who carried out the processing is presumed to be liable, unless he can prove that the damage occurred despite him having taken all appropriate measures to avoid it.* *For the purposes of this question, it may be worth recalling that, according to Article 4(1)(a) of the Personal Data Protection Code, "processing" includes the registration of personal data.*
Can physicians be held liable because they have erased data from the EHRs?	*Personal Data Protection Code* *Criminal Code*	*See previous answer.* *For the purposes of this question, it may be worth recalling that, according to Article 4(1)(a) of the Personal Data Protection Code, "processing" includes the deletion of personal data.* *If the fact is committed with for the purposes of gaining a profit or harm someone, the criminal penalties of Article 167 of the Personal Date Protection Code may*

		apply.

Questions	*Legal reference*	*Detailed description*
		Destruction of EHR data may also integrate several crimes, depending on the circumstances of the case, notably those sanctioned by Articles 615 ter and 635 ter of the Criminal Code.
Are hosting institutions liable in case of defect of their security/software systems?	*Personal Data Protection Code* *Digital Administration Code*	*The software and the applications used must comply with legislation on the personal data protection. At least the minimum security measures set out in the Personal Data Protection Code and in an Annex thereto shall be adopted. The risks to prevent are: unauthorised access to EHR data, inconsistent processing in relation to the purposes of the EHRs, accidental loss or destruction of EHR data.* *The processing of personal data in violation of minimum technical rules is punished with an administrative sanction from €10.000 to €120.000 (Article 162(2-bis) of the Personal Data Protection Code), without prejudice to other applicable sanctions or liability for damages.* *Failure to take minimum technical measures can also result in up to two years of arrest (Article 169(1) of the Personal Data Protection Code).* *The public administrations have to provide data availability and business continuity, as described in Article 50 and 50 bis of the Digital Administration Code.*
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?		*Doctors and health workers who have access to the EHRs should be in charge for the processing. According to Art. 30 of d. lgs. No. 196 of 30 June 2003, people in charge must dictate specific instructions for the data processing.* *Suitable authentication, authorization, traceability, login and transactions systems, as well as audit log to control access should be adopted.*
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	*Civil Code* *Criminal Code*	*Both civil and criminal liability may arise in case of violation of any provision on security measures of the d. lgs. No. 196 of 30 June 2003. According to par. 1 of the Art. 169 of the d. lgs., whoever fails to adopt the minimum measures referred to in Section 33 shall be punished by detention for up to two years. There is no liability rule specifically laid down for unauthorised access to EHRs. General rules apply.*

Questions	***Legal reference***	***Detailed description***
	Personal Data Protection Code	*The Civil Code provides for the restoration of damages, be them economic (Article 2043) or not (Article 2059).* *The Criminal Code sanctions abusive access to protected IT systems (Article 615 ter).* *Moreover, the criminal penalties set out in the Personal Data Protection Code may apply in certain circumstances (Article 167).*
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?		*There is not such an express requirement. General principles apply.*
Are there liability rules related to the misuse of secondary use of health data?	*Personal Data Protection Code*	*Although there is no specific liability rule regarding secondary uses of health data, general rules apply. In particular, Article 15 of the Personal Data Protection Code states that whoever causes a damage as a consequence of the processing of personal data must restore the damage. Both economic and moral damages may be restored. A special rule on burden of proof typical of dangerous activities applies – the person who carried out the processing is presumed to be liable, unless he can prove that the damage occurred despite him having taken all appropriate measures to avoid it.*

7.7 Secondary uses and archiving durations

Main findings

The D.L. 179/2012 permits "secondary uses" of EHR data (i.e. use for the purposes of research, health service planning and evaluation) by the Ministries of Employment and Health, the regions and autonomous provinces within the limits of their respective competences. The patient's consent is not required in relation to secondary uses, as direct identification information may not be utilised in these cases.

The D.L. 179/2012 does not lay down any specific provision on archiving EHR data.

Questions	***Legal reference***	***Detailed description***
Are there specific national rules on the archiving durations of EHRs?	*Circular No. 19 Italian Ministry of Health of 19 December 1986*	*There is no specific provision in this regard.* *In relation to the paper health records, the Circular No. 19 of the Italian Ministry of Health of 19 December 1986 provides that "health records, and the related reports should be kept indefinitely, as they represent an official act necessary to ensure legal certainty. It also represents a valuable document for historical health research".* *Finally, the legislation on the personal data protection provides that data cannot be stored for a longer period than the one necessary to achieve the processing purpose.*
Are there different archiving rules for different providers and institutions?		*There is no specific provision in this regard. General principles apply.*
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?		*There is no obligation to destroy data at the end of the archiving period or in case of closure of the EHR. General principles apply.*
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?		*There is no specific rule about the use of data at the end of the archiving duration or in case of closure of the EHR. General principles apply.*
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	*D.L. 179/2012* *Personal Data Protection Code*	*Article 12(2) of D.L. 179/2012 states that EHRs are established, inter alia, for the purposes of medical and epidemiological research, as well as health service planning and evaluation. Where EHR data is used for such purposes, patient identification data may not be utilised (Article 12(6)).* *Article 12(7) of D.L. 179/2012 provides that the implementing ministerial decree(s) shall establish, inter alia, the modalities and access levels for the purposes referred to above.*
Are there health data that cannot be used for secondary use?	*D.L. 179/2012*	*See answer to previous question.*

Questions	***Legal reference***	***Detailed description***
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	*D.L. 179/2012*	*See answers to the previous two questions.*
Does the law say who will be entitled to use and access this data?	*D.L. 179/ 2012*	*Article 12(6) of D.L. 179/2012 entitles regions and autonomous provinces, as well as the Ministry of Employment and the Ministry of Health, within the limits of their respective competences, to use EHR data for secondary purposes.* *Article 12(7) of D.L. 179/2012 provides that the implementing ministerial decree(s) shall establish, inter alia, the modalities and access levels for the purposes referred to above.*
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	*D.L. 179/2012*	*There is no opt-in/opt-out system regarding secondary uses of EHR data.* *It may also be worth clarifying that the requirement of consent only applies for the purposes of prevention, diagnosis, health treatment and rehabilitation, but not for secondary purposes (Article 12(5)-(6) of D.L. 179/2012. This can be explained in light of the fact that identification data may not be utilised in the context of secondary uses of EHR data.*

Questions	***Legal reference***	***Detailed description***
Are there obligations in the law to develop interoperability of EHRs?	*D.L. 179/2012*	*Article 12(7) of D.L. 179/2012 provides that the implementing ministerial decree(s) shall establish criteria for the interoperability of EHRs at regional, national and European level.*
Are there any specific rules/standards on the interoperability of EHR?	*D.L. 179/2012* *2014 Ministry of Health and Agency for Digital Italy Guidelines*	*No specific rules/standards on the interoperability of EHR systems are currently in force.* *A few preliminary indications of technical nature are defined in paragraph 6 of Guidelines for regional project plans presentation on the Electronic Health Record.*
Does the law consider or refer to interoperability issues with other Member States systems?	*D.L. 179/2012*	*See answer to the first question in this table.*

7.8 Links between EHRs and ePrescriptions

Main findings

The e-Prescription system predates, and it is not dependent on, the EHR system. Legal sources relevant to e-Prescription include:

- *The Decree of the President of the Council of Minister of 26 March 2008 on the modalities for the transmission of prescriptions by IT means by the doctors of the National Health Service;*
- *The Ministerial Decrees of 14 July 2010, 21 February 2011, 21 July 2011 and 2 July 2012 promoting e-prescriptions;*
- *The Ministerial Decree of 2 November 2011, replacing traditional prescription with on e-prescription*
- *Article 13 of D.L. 179/2012. validity of e-prescription on the whole national territory.*

The D.L. 179/2012 provides that persons operating within the National Health Service or the regional health services who provide health services to the patient may access his EHR, but it does not add further detail.

The table below describes the Italian legal framework on ePrescriptions. The transition paper to electronic prescriptions is one of the specific goals of the Italian Ministry of Health.

D.p.c.m. of 26 March 2008 regulates the electronic transmission of the data contained in the prescriptions made by the doctors in the National health service.

Art. 13 of d.l. No. 179 of 18 October 2012 regulates the gradual replacement of paper prescriptions with ePrescriptions in the regions and autonomous provinces.

The regions and autonomous provinces shall gradually replace the paper prescriptions with the electronic ones. According to par. 2 of Art. 13 of D.L. 179/2012, the pharmaceutical electronic prescriptions will have full legal value on the national territory starting from 1 January 2014.

- ***Infrastructure***

Questions	*Legal reference*	*Detailed description*
Is the existence of EHR a precondition for the ePrescription system?		*The e-Prescription system predates, and it is not dependent on, the EHR system. According to the implementation decree, the prescription (hence the e-prescription as well) is a part of EHR.* *Legal sources relevant to e-Prescription include:* - *The Decree of the President of the Council of Minister of 26 March 2008 on the modalities for the transmission of prescriptions by IT means by the doctors of the National Health Service;* - *The Ministerial Decrees of 14 July 2010, 21 February 2011, 21 July 2011 and 2 July 2012 promoting e-prescriptions;* - *The Ministerial Decree of 2 November 2011, replacing traditional prescription with on e-prescription* - *Article 13 of D.L. 179/2012. validity of e-prescription on the whole national territory..*
Can an ePrescription be prescribed to a patient who does not have an EHR?		*The e-Prescription system predates, and it is not dependent on, the EHR system*

- ***Access***

Questions	*Legal reference*	*Detailed description*
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?	*D.L. 179/2012*	*Article 12(4) of D.L. 179/2012 only provides that persons operating within the National Health Service or the regional health services who provide health services to the patient may access his EHR. However, Article 12(7) states that implementing ministerial decree(s) shall establish the modalities and levels of access to EHR data for different persons.* *In any case, consent from the patient is necessary to access the EHR.*
Can those health professionals write ePrescriptions without having access to		*The e-Prescription system predates, and it is not dependent on, the EHR system.*

Questions	*Legal reference*	*Detailed description*
EHRs?		

7.9 Other requirements

Restrictions deriving from the regulations on the personal data protection may require a few more considerations. The Guidelines on the Electronic Health Record and the Health File adopted by the Italian D.P.A. for the protection of personal data state that "the EHR is a logical set of health care information and records that aims at documenting a person's clinical history and can be shared by several data controllers; accordingly, the highest transparency should be featured both in terms of its structure and in terms of its operation. Hence, the processing of personal data performed via an EHR should be notified to the Italian D.P.A. with an ad-hoc communication".

Great attention is also paid to the security requirements. Given the importance of the personal data processed via EHRs, specific technical arrangements should be adopted in order to ensure the appropriate security level (art. 31 of the Italian Data Protection Code) - without prejudice to the minimum measures that data controllers are required to take according to the Data Protection Code. In particular, in order to protect data against unauthorised accesses, theft and/or loss, in whole or in part, the following measures should be taken:

- *suitable authentication and authorisation systems should apply to those in charge for the processing as a function of the respective access/processing requirements (e.g. as for browsing, changing and adding records);*
- *procedures to regularly check quality and consistency of the authentication credentials and authorisation profiles should be implemented and should apply to the people in charge for the processing;*
- *criteria to encrypt and/or keep separate those data that are suitable for disclosing health and sex life from any other personal data should be outlined;*
- *accesses and operations should be logged;*
- *audit logging to control database accesses and detect abnormalities should be implemented.*

7.10 Legal requirements applying to EHRs in Germany

This section will give a comprehensive description of the legal requirements applying to EHRs in Germany by answering specific questions on several EHRs related topics. This information will be used to identify potential legal barriers and good practices for the development of EHRs in Germany.

The focus in the context of EHRs and ePrescriptions clearly lies on § 291a SGB V, since it regulates the EHC as the primary structure for the implementation of EHRs and ePrescriptions. Where necessary, other relevant legislation shall be observed within the comprehensive descriptions in the tables. In order to put the answers to the questions into a broader context, a short introduction to the setup of the SGB V as the main piece of legislation relevant for EHRs and especially the provisions specifically dealing with EHRs is given.

The SGB V contains various chapters and mainly regulates the correlations between the health insurance companies and the insurants, as well as the various care providers[8] There is a general conflict between the general right to self-determination and the corresponding right to social data protection on the one hand, and the advancement of the health sector to fit the information society as well as according cost-effectiveness motivations on the other hand. Therefore, § 291a (1) SGB V states the goal of the EHC: to improve the cost effectiveness, quality and transparency of medical treatment. At the same time, patient sovereignty and individual responsibility of an insured person shall be strengthened. § 291a SGB V is located in the tenth chapter, "Insurance and benefit data, data protection, data transparency". It contains general principles of data usage, regulations concerning the processing of data, data transparency, erasure and duties to give information.

Transmissible data are hence regulated under an own, detailed, sector specific social data protection law regime[1] This sector-specific law usually supersedes the more general regulations of the BDSG. The BDSG is only applicable where no other regulations govern personal data, pursuant to § 1 (3) sentence 1 BDSG.

Where deemed necessary or applicable, an apportionment between the two acts is being carried out. However, since the regulations on the setup of the telematics infrastructure, and therefore also the ones taking into account data protection measures, are still rather broad and do not yet stand in relation to a functioning §291a-EHR scheme, the relationship between the sector specific SGB V and the BDSG remains yet to be fully ascertained.

Since the EHR and the ePrescription in Germany are rooted within the setup of an EHC, it is also advisable to give an overview of the clauses regulating this card. Most of the general regulations also apply to EHRs and the ePrescriptions, since they are a applications of the EHC. A very basic example:

An insurant's master data (like for example the name, sex and date of birth) must be stored on the card, pursuant to §§ 291 (2a) sentence 3, 291a (2) sentence 1 SGB V. These data would then also be available to serve as master data when working with the EHR of the insurant. However, since there is no functioning EHR scheme in place in relation to the regulations within the SGB V, the concrete setup of EHRs might as well be a completely *separate one within the EHC framework, where all applications function completely independantly. The explanations in this study partly need to take into account hypothetical or anticipatory principles.*

This report shall keep a focus on EHR and ePrescriptions (and therefore the EHC) regarding data protection regulations. Even though there might be regulations according to the Cross-Border Healthcare Directive 2011/24/EU, this report therefore only takes into account the relevant legislation concerning EHRs and the ePrescription, mainly the SGB and partially the BDSG.

The basic setup of § 291a features 16 subparagraphs (§ 291a (1) - § 291a (8)). Subparagraph 1 stipulates the objectives and purposes of the advancements towards the EHC. Subparagraph 1a foresees that most provisions are applicable also to private health insurance schemes, should these envisage to implement a similar card concept. Subparagraph 2 states the mandatory applications of the card, Subparagraph 3 the voluntary applications as well as information and consent duties. Subparagraph 4 regulates the access rights of different persons to the card. Subparagraph 5 statutes further data protection requirements and further technical necessities for access. Subparagraph 5a is tailored to specific applications of the EHC not including EHRs or ePrescriptions. Subparagraph 5b stipulates specific duties for the gematik. Subparagraph 5c obliges the German states to determine the centres responsible for acknowledgement of the validity and permission to conduct a medical profession as well as the handout of special professional ID cards. Subparagraph 6 states a right to erasure and logging obligations for data protection purposes. Subparagraphs 7 to 7e constitute the groundwork for the setup of the gematik as well as important financial provisions for its undertakings and also regulative measures for the supervisory body, the German Federal Ministry of Health. Subparagraph 8 finally states a protection right of the card holder regarding forbidden disadvantages for denial of access to the card.

2.2. Health data to be included in EHRs

Main findings

The rules on which health data are to be included in EHRs are rather vague. That complies with the lawmaker's approach of setting up a general framework and leaving the concrete arrangement of EHRs to the self-governing bodies in a formalised procedure. However, the content clearly focuses on medical data only. Furthermore, the lawmaker stipulates a legal definition of what an EHR actually is within the law, which can serve as an important classification criterion where needed. It should be noted, however, that, as explained in Section 1 and 2 above, an EHR within the meaning of an interoperable system where different health service providers share the data on the respective patient is not in place in Germany yet.

Questions	Legal reference	Detailed description
Are there specific rules on the content of EHRs? (or regional provisions, agreements, plans?)	§ 291a (3) Sentence 1 point 4 SGB V	The German legislator provided for the groundwork of EHRs, which includes a legal definition of the term itself. This definition refers to "medical findings, diagnoses, therapy measures, treatment reports and immunizations" as content of an EHR.
Are these data restricted to purely medical information (e.g. physical or mental health, well-being)?	§ 291a (3) sentence 1 point 4 SGB V	"Medical findings, diagnoses, therapy measures, treatment reports and immunizations" solely refer to medical (treatment) data.
Is there a definition of EHR or patient's summary provided in the national legislation?	§ 291a (3) sentence 1 point 4 SGB V	EHR (in the SGB referred to as 'electronic patient record') is defined as a n application that supports the collection, processing and utilization of data concerning medical findings, diagnoses, therapy measures, treatment reports and vaccinations for a comprehensive documentation of various medical cases [of one patient] between different medical institutions.
Are there any requirements on the content of EHRs (e.g. detailed requirements on specific health data or general reference to health data)?	§ 291a (3) sentence 1 point 4 SGB V	The legal definition in § 291a (3) sentence 1 point 4 SGB V is wide (see above first question). A statement from the German Medical Association from mid-July furthermore states that with regard to the eHealth-Governance-Initiative guidelines for EHRs, a collocation of a non-exhaustive list of specific EHR content "is not reasonable at this point in time".[33]
Are there any specific rules on the use of a common terminology or coding system to identify diseases, disorders, symptoms and others?	-	Since the legislator has only set out ground rules and EHRs are not part of the basic rollout procedures, no specific rules exist. In any case, there is the obligation laid down in the law to design the EHC in an interoperable and compatible way (see below 2.7.2).
Are EHRs divided into separate categories of health data with different levels of confidentiality (e.g. data related to blood type is less confidential than data related to sexual diseases)?	-	The definition of EHRs contains only a general statement about content: "medical findings, diagnoses, therapy measures, treatment reports and immunizations" are part of it. Even though access is regulated in an own section of § 291a SGB V (see below 2.4.2), a differentiation between different kinds of data is not provided by law.
Are there any specific rules on identification of patients in EHRs?	-	-

[33] Stellungnahme der Bundesärztekammer zu den geplanten Inhalten einer elektronischen Patientenakte auf Basis des epSOS-Datensatzes vom 16.07.2013, available at http://www.bundesaerztekammer.de/downloads/BAeK-Stellungnahme_zu_den_geplanten_Inhalten_einer_elektronischen_Patientenakte_auf_Basis_des_epSOS-Datensatzes_16.07.2013.pdf.

Questions	***Legal reference***	***Detailed description***
Is there a specific identification number for eHealth purposes?	*§§ 291a (2) sentence 1 Clause 1, 291 (2) sentence 1 point 6 SGB V*	*The EHC has to contain the insurant's master data, pursuant to §§ 291a (2) sentence 1 Clause 1 SGB V, which consists of the data which was also foreseen to be available on the old health insurance card (HIC), under § 291 (2) point 6 SGB V. Therefore, the health identification number was originally not designed for eHealth purposes. But as the EHC is supposed to fully replace the old card and will function as the pioneer practice for telematics in the health sector also containing an individual identification number, it can be argued that this number serves a specific function for eHealth purposes.* *Since this number is unique and potentially easily relatable to a certain person, this number would have to be regarded as (under certain circumstances even sensitive) personal data. There are no specific rules on constraints of usage because of, for example, a potential easy interoperability. However, § 290 (2) sentence 2 SGB V states that the identification number has to be issued by a centre of trust, separated spatially, organisationally and regarding staff from the card-issuing health insurance companies. Furthermore, § 291 (1) sentences 3, 4, 5 SGB V state that the health insurance identification number may not be the same as the separate pension insurance identification number, or that if the pension insurance identification number is used to create a health insurance identification number, when according to the state-of-the-art of science and technology it is not possible to draw conclusions about the person behind the numbers from the interconnection of the two.*

7.11 Requirements on the institution hosting EHRs data

Main findings

Since a fully functioning EHR scheme is not yet in place, requirements on the institutions hosting EHRs data only exist in a broader sense. Institutions, however, will have to comply with specific autorisation requirements.

Questions	***Legal reference***	***Detailed description***
Are there specific national rules about the hosting and management of data from EHRs?	-	*Since the German legislator laid down only the basic rules of the development of a telematics infrastructure and the gematik has until now only begun with the basic rollout which does not include EHRs and the ePresciption, no specific rules exist. Specifically, § 291a (2) SGB V does not provide for rules regarding the storage location of data on EHCs.*[34] *It hence also remains unclear whether hospitals, physicians or health insurance companies would have to provide the hosting and management infrastructure.* *However, there is an obligation to store emergency data, which is another application of the EHC, on the card itself, § 291a (3) sentence 1 SGB V so that they can be accessed without network access. In reverse, this would mean that there is at least no obligation to store data (other than emergency data) on the EHC itself. In any case, this would not be very likely as these data can easily sum up to large amounts of memory size.*
Is there a need for a specific authorisation or licence to host and process data from EHRs?	-	*Services and provider have to be authorised by gematik (§291b, 1b).*
Are there specific obligations that apply to institutions hosting and managing data from EHRs (e.g. capacity, qualified staff, or technical tools/policies on security confidentiality)?	-	*Services and provider have to be authorised by gematik (§291b, 1b).*
In particular, is there any obligation to have the information included in EHRs encrypted?	-	*No specific legal regulations. However encryption of data or equivalent measures to prevent unauthorized data access might be required by gematik for authorisation of EHR Services and providers*
Are there any specific auditing requirements for institutions hosting and	-	*No specific legal regulations. However auditing might be required by gematik for authorisation of EHR Services and providers*

[34] Pitschas, NZS 2009, 177 (182) indicates that the German legislator only provided for the basic groundwork in that matter to be able to conduct the concrete setup of new applications according to the current technical state-of-the-art and also implement new findings. On the other hand, this would lead to serious safety hazards, especially regarding the ePrescription, which would pose high demands towards the availability of the system, which could be contradicted by for example server timeouts. An open implementation scheme would not help in that matter, since only realtime exploitation would show implications beyond testing measures.

Questions	*Legal reference*	*Detailed description*
processing EHRs?		

2.3. Patient consent

Main findings

The German legislator made consent an essential requirement for the use of the EHC (which includes the future use for EHRs). There are specific rules on consent not only for the initial use of the EHC but also for the use of specific applications, meaning that there has to be a first consent to use the card and another, second consent for the specific use of different applications on the card. The regulations on consent are accompanied by further informational obligations for the involved stakeholders, such as the card distributing institutions or institutions working with applications of the EHC. The answers provided in the following tables refer to the EHC.

Questions	*Legal reference*	*Detailed description*
Are there specific national rules on consent from the patient to set-up EHRs?	*§ 291a (3) sentences 4, 5 SGB V*	*Persons with authorized access may only start data processing when the patient has given his or her consent..* *There is a general obligation to cooperate in social security law in order to claim benefits, § 60 SGB I. It has been argued that a denial of consent therefore might lead to the denial of benefits also in relation to EHRs.*[35] *However, since the consent rules for EHRs are more specific and provide for the right to revoke it, no disadvantages may derive from not consenting. Furthermore, the legislator clearly states that the patient can decide whether or not he wants to use the different applications. Finally, § 291a Abs. 8 SGB V suggests that patients should suffer no disadvantages in case they do not want specific stakeholders to access their EHC.*
Is a materialised consent needed?	*§ 291a (3) sentence 4 SGB V*	*Patient consent is to be documented on the card (electronically) at the first time of usage of the EHC for the EHR and other medical applications..*
Are there requirements to inform the patient about the purpose of EHRs and the consequences of the consent or withholding consent to create EHRs?	*§ 291a (3) sentence 3 SGB V*	*Before the first use of the EHC the patient has to be informed in a comprehensive manner and in a generally understandable way about the functionality of the EHC, including the possible data to be collected and processed by it. Furthermore, § 291a (3) sentence 7 SGB V states that also § 6c BDSG is applicable, which stipulates further rules on information duties.* *However, it can be seen as problematic that EHR functionality was not in place*

		when the EHC was introduced, making it questionable how comprehensive and understandable information can be given out to the patient, because the original information duties have already been fulfilled when the EHC was delivered to the insurants, potentially making it necessary to inform separately about the EHR as soon as a functioning scheme is in place.
Are there specific national rules on consent from the patient to share data?	*§ 291a Abs. 3 S. 3, Abs. 5 S. 1 SGB V*	*Data on the EHC may only be processed if the patient has generally given his consent, § 291a Abs. 3 S. 3 SGB V. Moreover, every single access or processing measure, and this would include sharing ("Erheben, Verarbeiten, Nutzen" in the German terminology seeks to cover every possible act of working with the data), needs to be done in accordance with the patient, § 291a Abs. 5 S. 1 and 2 SGB V.*

[35] *Pitschas, NZS 2009, 177 (182)*

Questions	***Legal reference***	***Detailed description***
Are there any opt-in/opt-out rules for patient consent with regard to processing of EHRs?	*§ 291a (3) sentence 3SGB V*	*By using the EHC data may only be collected, processed and used if the patient has generally given his consent, pursuant to § 291a (3) sentence 3 SGB V.*
Are there requirements to inform the patient about the purpose of EHRs and the consequences of consent or withholding consent on the sharing of EHRs?	*§ 291a (3) sentence 7 in conjunction with § 6c of the Federal Data Protection Act*	*§ 291a (3) sentence 7 SGB V provides that § 6c of the Federal Data Protection Act is applicable The latter prescribes that data controllers need to inform, inter alia, on the functionality of the system.*
Can the patient consent to his/her EHRs being accessed by a health practitioner or health institution outside of the Member State (cross-border situations)?	*§ 291a (3) sentence 3 SGB V, §§ 4 (1), 4a, 4b, 4c (1) point 1 BDSG*	*There is no restriction of the right to consent in § 291a (3) sentence 3 SGB V. The general rules for sharing data outside the EU, namely §§ 4b, 4c BDSG, also allow for cross-border sharing within the EU when a patient has given his or her consent, § 4c (1) point 1 BDSG. Please note that the patient needs his/her EHC, a PIN code and the doctor a health professional card in order to access a EHR based on §291 a, which means that currently it is not possible for a foreigner doctor to have access to the system.*
Are there specific rules on patient consent to share data on a cross-border situation?		*No.*

7.12 Creation, access to and update of EHRs

Main findings

The German legislator provides for specific rules on access to EHRs within the setup of the EHC. However, concrete determinations for different categories of health data are not in place yet, since only the legal groundwork is regulated. The insurants have access and erasure rights. Access for health professionals is generally connected to further requirements, e.g. ensuring they only get access via a health professional ID card secured by electronic signature measures.

Questions	***Legal reference***	***Detailed description***
Are there any specific national rules regarding who can create and where can EHRs be created?	*§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V*	*EHRs based on §291a can be created by the following professions if it is necessary for the medical care of the patient:* • *doctors (lit. a),* • *dentists (lit. b),* • *pharmacists, pharmacist assistants, pharmacy engineers, pharmacy assistants (lit. c),* • *persons that work under a professional mentioned in lit a) - lit c) or in a hospital as assistants or in preparation for their assisting occupation, insofar as this is permissibly required for their occupational tasks and their access is being carried out under supervision of the persons mentioned in lit a) to lit c).* • *psychotherapists (lit. f)* .
Are there specific national rules on access and update to EHRs?	*§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V*	*Access is allowed for the following professions as long as it is necessary for the medical care of the patient:* • *doctors (lit. a),* • *dentists (lit. b),* • *pharmacists, pharmacist assistants, pharmacy engineers, pharmacy assistants (lit. c),* • *persons that work under a professional mentioned in lit a) - lit c) or in a hospital as assistants or in preparation for their assisting occupation, insofar as this is permissibly required for their occupational tasks and their access is being carried out under supervision of the persons mentioned in lit a) to lit c).* *psychotherapists (lit. f)*
Are there different categories of access for different health professionals?	*§ 291a (4) sentence 1 point 1, point 2 SGB V*	*The clause regulating access rights lists different types of health professionals (see above) but does not set limitations for different categories concerning EHRs (but does so for other applications of the EHC).*
Are patients entitled to access their EHRs?	*§ 291a (4) sentence 2 SGB V*	*§ 291a (4) sentence 2 SGB V specifically states that insurants have the right to access their "data according to Abs. 2 S. 1 und Abs. 3 S. 1" [(2) sentence 1 and (3) sentence 1], which includes EHR data.*

Questions	***Legal reference***	***Detailed description***
Can patient have access to all of EHR content?	*§ 291a (4) sentence 2 SGB V*	*See above. There is no restriction to certain kinds of data.*
Can patient download all or some of EHR content?		*Since a functioning EHR system is not yet in place, the question where the data should be stored is also not (yet) answered (by law). However, the law regulates the right to access the data for an insurant, § 291a Abs. 4 S. 2 SGB V.*
Can patient update their record, modify and erase EHR content?	*§§ 291a (3) sentence 6, 291a (6) sentence 1, sentence 2 SGB V*	*Patients cannot modify or update the content of an EHR based on §291a.* *§ 291a (6) sentence 1 SGB V states data relating to EHRs have to be deleted when so required by the insurant, indicating that not the insurant himself can delete but only express the request. This interpretation is backed by § 291a (6) sentence 2 SGB V, which states that data from particular applications on the EHC mentioned in § 291a (2) sentence 1 point 1 and (3) sentence 1 point 5, point 7, point 8, point 9 (so not point 4 which regulates EHRs) can be deleted independantly by insurants. In any case, data relevant for accounting purposes must be kept, § 291a (6) 1.*
Do different types of health professionals have the same rights to update EHRs?	*§ 291a (4) sentence 1 point 2 lit. a) - lit. f) SGB V*	*See row 2.*
Are there explicit occupational prohibitions? (e.g. insurance companies/occupational physicians…)	*§ 291a (8) sentence 1 SGB V*	*Even though there are no specific restrictions to explicit occupations, § 291a Abs. 8 S. 1 SGB V states that it is not allowed to demand from the owner of the EHC to give access to other professionals than the ones mentioned in § 291a Abs. 4 S. 1 Nr. 2 lit. a) - lit. f) SGB V (see above). An agreement between the patient and other persons than the ones listed therein to provide access to the data is prohibited by law.*
Are there exceptions to the access requirements (e.g. in case of emergency)?	*§ 291a (4) sentence 1 point 2 lit. e) SGB V*	*No, there are no exceptions. However, there are plans for a separate emergency data set with special rules of access in case of emergency..*
Are there any specific rules on identification and authentication for health professionals? *Or are they aggregated?*	*§ 291a (5) sentence 3 SGB V*	*See table 2.2.2, row 2: Access to EHRs may only be concluded in conjunction with an electronic health profession ID card, § 291a (5) sentence 3 SGB V, which has to provide for secure authentification measures and have the technical infrastructure of qualified electronic signatures available.*
Does the patient have the right to know who has accessed to his/her EHRs?	*§ 291a (6) sentence 3 SGB V*	*See table 2.6.1, row 1: It is to be ensured by technical measures that at least the last 50 access activities on the EHC are logged in a protocol for purposes*

Questions	*Legal reference*	*Detailed description*
		of data protection monitoring. The access right of § 291a (4) sentence 2 SGB V is limited to specific EHR data, not protocol data. § 291a (6) does not statute an independent access right. But since the protocol duty specifically refers to "data protection monitoring" purposes, it can be argued that also the *patient needs to be enabled to carry out this control.*
Is there an obligation on health professionals to update EHRs?	-	*There is no specific obligation to update data in EHRs*
Are there any provisions for accessing data on 'behalf of' and for request for second opinion?	-	*No*
Is there in place an identification code system for cross-border healthcare purpose?	-	*No*
Are there any measures that consider access to EHRsfromhealth professionals in another Member State?	-	*There are no specific regulations on cross-border access within EHRs. However, the general data protection rules of the BDSG state in relation to data transmission (which would imply access) that the regular permissive regulations apply, § 4b BDSG. In addition, the general rules of the law on electronic signatures on cross-border usage apply, in particular § 23 BDSG.* *Please note that the patient needs his/her EHC, a PIN code and the doctor a health professional card in order to access a EHR based on §291 a, which means that currently it is not possible for a foreigner doctor to have access to the system.*

7.13 Liability

Main findings

There are no specific medical negligence rules related to the use of EHRs. More generally, there are various grounds for liability for medical malpractice. Patient and physician usually conclude a treatment contract, out of which the breach of duties by the physician can constitute medical liability. Furthermore, medical negligence can lead to compensational duties according to tort law. Since there are no specific regulations regarding medical negligence related to the use of EHRs and neither are there any functioning EHR systems in place which would be needed to specifically point out obligations and duties of the treating physician, statements on a possible liability would be highly speculative and therefore should not deemed to be conclusively feasible at this time.

Liability		
Questions	***Legal reference***	***Detailed description***
Does the national legislation set specific medical liability requirements related to the use of EHRs?		*General liability legislation (e.g. under the German Civil Code) may apply, for example, in cases where doctors who directly supervise and control staff members (e.g. nurses, assistants) entitled to fill EHRs, are liable for injuries associated with inaccurate or deficient summary reports provided by these staff members (see also § 291a (4) sentence 1 point 2 mentioned above in 2.4.2, row 2). However, there is no specific liability legislation relating to EHRs in place.* *§ 7 BDSG sets out a standard rule for compensation covering misuse of personal data: "If a controller harms a data subject through collection, processing or use of his or her personal data which is unlawful or improper under this Act or other data protection provisions, the controller or its supporting organization shall be obligated to compensate the data subject for damage suffered. The obligation to provide compensation shall be waived if the controller exercised due care in the case". This regulation specifically takes into account "other data protection provisions", which would also cover the data protection regulations within the setup of the telematics infrastructure. Since a functioning EHR scheme is not yet in place, it remains open what would be considered improper use of data and how "due care in the case" would be defined.* *As electronic health profession IDs imply the usage of qualified electronic signatures, also the general liability rules of the laws on electronic signatures, in particularar § 11 of the law, can apply.*
Can patients be held liable for erasing key medical information in EHRs?	*§ § 291a (6) sentence 1 SGB V; § 291a (3) sentence 4, 5 SGB V*	*Patient has an explicit right to erasure, § 291a (6) sentence 1 SGB V. A further argument against liability would be that all key medical information in EHRs would only be available on the EHR following the consent of the patient (§ 291a (3) sentence 4 SGB V). This consent may be revoked at any time (§ 291a (3) sentence 5 SGB V), which indicates that data may only be stored for EHR purposes as long as there is valid consent. Therefore, if there is no consent, the data may not be used anymore. Liability for the "erasure" would therefore contradict this basic right of the patient.*
Can physicians be held liable because of input errors?		*Since there is no specific liability legislation in place relating to EHRs, these questions can only be answered hypothetically. It is questionable if an originally*

		Liability
Questions	***Legal reference***	***Detailed description***
Can physicians be held liable because they have erased data from the EHRs?		*recording party could be held liable if input or erasure lead to treatment errors of another physician working with the EHR file. Regarding data protection liability, see row 1.*
Are hosting institutions liable in case of defect of their security/software systems?	-	*See above; if treatment on the basis of an EHR is to be seen as a specific contractual obligation of the treating party, a non-functioning record could potentially lead to contractual liability or liability following tort law. Regarding data protection liability, see row 1.*
Are there measures in place to limit the liability risks for health professionals (e.g guidelines, awareness-raising)?	-	*No*
Are there liability rules related to breach of access to EHRs (e.g. privacy breach)?	-	*No*
Is there an obligation on health professionals to access EHRs prior to take a decision involving the patient?	*§ 291a (5) sentence 1, 2, 5 SGB V*	*See table 2.8.2, row 4: On the contrary, each access to a single application on the EHC has to be approved by the patient. Furthermore, each access has to be authorised by the patient with support from technical measures.*
Are there liability rules related to the misuse of secondary use of health data?	-	*Regarding general data protection liability, which would also cover data usage under secondary use aspects, see row 1.*

Milieu Ltd.- time.lex cvba *Overview of national legislation on EHR in Germany / 31*

7.14 Secondary uses and archiving durations

Main findings

Archiving durations are only regulated generally in different German acts and do not reflect on the use of EHRs. There are no specific rules regulating secondary uses to the use of EHR data.

Questions	*Legal reference*	*Detailed description*
Are there specific national rules on the archiving durations of EHRs?	*§ 291a (6) sentence 3 SGB V*	*There are no specific archiving duration rules regarding EHRs. However, it is to be ensured by technical measures that at least the last 50 access activities on the EHC are logged in a protocol for purposes of data protection monitoring. However, this should not be seen as an archiving requirement; this is rather to be seen as a technical measure for ensuring data protection rights and information for the insurant.*[36]
Are there different archiving rules for different providers and institutions?	-	*§ 291a (6) sentence 3 SGB V refers to all data and applications stored on the EHC and in that context does not specifically differentiate between users of the card.* *However, different archiving specifications may be applicable according to various other archiving regulations concerning medical professionals. For example, § 630f (3) of the German Civil Code and § 10 of the Model Professional Code for Physicians ("Musterberufsordnung Ärzte") establish a general obligation to store basic medical treatment documentation for ten years. This seems to contradict the patients' right to erasure provided in § 291a Abs. 6 SGB V, but since the EHR is just a voluntary application of the EHC, the obligation concerns two different instruments of documentation, meaning that documentation obligations in these areas differ and the right to erasure in the EHC could always be observed. The basic medical documentation and the EHR documentation are two different areas of documentation duties. It is therefore likely that these durations do not apply to EHRs.*
Is there an obligation to destroy (…) data at the end of the archiving duration or in case of closure of the EHR?	*§ 291 (4) sentence 5, 6 SGB V*	*The redemption of the EHC leads to the duty of the health insurance company to assure that the further use of the stored data is possible for and by the insurant. Before the actual redemption, the health insurance company has to give out information about the options of erasure of the data. A specific obligation to destroy the data is not foreseen in the law.* *However, according to the more general § 20 (2) point 2 BDSG, data have to be deleted as soon as the knowledge of these data is no longer necessary for the undertakings of the responsible controller.*

[36] *Becker/Kingreen, SGB V, § 291a, Rec. 16.*

Questions	***Legal reference***	***Detailed description***
Are there any other rules about the use of data at the end of the archiving duration or in case of closure of the EHR?	-	*See above.*
Can health data be used for secondary purpose (e.g. epidemiological studies, national statistics...)?	*§ 28 (7) sentence 1 BDSG*	*No, this is not possible (§291a, data can only be used, if they are necessary for the medical care of the patient.*
Are there health data that cannot be used for secondary use?	-	*See above*
Are there specific rules for the secondary use of health data (e.g. no name mentioned, certain health data that cannot be used)?	-	*See above*
Does the law say who will be entitled to use and access this data?	*§ 28 (7) sentence 1 BDSG*	*Under the general rules, the usage is restricted to health professionals who are subject to the obligation of professional secrecy or by other persons also subject to an equivalent obligation of secrecy.*
Is there an opt-in/opt-out system for the secondary uses of eHealth data included in EHRs?	-	*No*

7.15 Requirements on interoperability of EHRs

Main findings

As there is no specific EHR scheme in place yet, it cannot be assessed how the interoperability of EHRs is regulated. However, the legal setup of a telematics infrastructure in Germany by the legislator shall be "interoperable and compatible", which leads to the conclusion that whenever supporting research is being conducted and ultimately first implementation steps are executed, it could be argued that full interoperability (e.g. between health institutions, health practitioners, different geographical areas in Member States and between Member States, as Germany is also involved in epSOS and the followup project EXPAND), would be aimed for.

Questions	***Legal reference***	***Detailed description***
Are there obligations in the law to develop interoperability of EHRs?	*§ 291a Abs. 7 S. 1 SGB V*	*The telematics infrastructure that stakeholders need to create in the long term for the introduction and application of the EHC specifically needs to be "interoperable and compatible". This interoperability and compatibility has to be applicable especially to EHRs and the ePrescription, since these are each mentioned as examples of that infrastructure.*
Are there any specific rules/standards on the interoperability of EHR?	-	*There are no specific rules/standards on the interoperability of EHR within the law itself. However, most initiatives are aware of the necessity of interoperability and therefore take this into account in their research.*
Does the law consider or refer to interoperability issues with other Member States systems?	-	*No*

7.16 Links between EHRs and ePrescriptions

Main findings

There is a relation between ePrescriptions and EHRs since they are related within the setup of the EHC, i.e. within the setup of the telematics infrastructure. However, EHRs and ePrescriptions are to be seen as two different applications of the EHC. Hence, they both will function independently.

- ***Infrastructure***

Questions	***Legal reference***	***Detailed description***
Is the existence of EHR a precondition for the ePrescription system?	*§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V*	*EHR and ePrescription are two different applications within the EHC and are planned to exist and function independently.*
Can an ePrescription be prescribed to a patient who does not have an EHR?	*§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V*	*Since the ePrescription is mentioned individually and constitutes a unique application within the EHC, it can be used without having the EHR application in place.*

- ***Access***

Questions	***Legal reference***	***Detailed description***
Do the doctors, hospital doctors, dentists and pharmacists writing the ePrescription have access to the EHR of the patient?	*§ 291a Abs. 5 S. 1, 2, 5 SGB V*	*Each access of a single application on the EHC has to be approved by the patient. Furthermore, each access has to be authorised by the patient with support from technical measures. Therefore, each access happens separately and can be controlled by the patient. § 291a Abs. 5 S. 5 even constitutes a unique rule for the access to the ePrescription, which in reverse leads to the conclusion that separate access scenarios must be possible.*
Can those health professionals write ePrescriptions without having access to EHRs?	*§§ 291a Abs. 2 S. 1 Nr. 1, Abs. 3 S. 1 Nr. 4 SGB V*	*Since the ePrescription is an individual application on the EHC, its functions can be used without having access to EHRs (see above).*

8 References

De Hert, P, and S Gutwirth. "Privacy, Data Protection and Law Enforcement. Opacety of the Individual and Transparency of the Power." In Privacy and the Criminal Law, edited by E Claes, A Duff and S Gutwirth, 61-. Antwerp - Oxford: Intersentia, 2006.

Gutwirth, S. Privacy and the Information Age. New York: Rowman and Littlefield, 2002.

Mantovani, E, and P Quinn. "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements." International Review of Law, Computers & Technology DOI:10.1080/13600869.2013.801581 (2013).

———. "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements." International Review of Law, Computers & Technology (2013): http://dx.doi.org/10.1080/13600869.2013.801581.

Quinn, P. "The Anonymisation of Research Data — a Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the Eu Data Protection Framework?". European Journal of Health Law 24 (2017): doi 10.1163/15718093-2341416.

———. "The Eu Commission's Risky Choice for a Non-Riskbased Strategy on Assessment of Medical Devices." Computer Law and Security Review 31 (2017): 361-70.

De Hert, P, and S Gutwirth. "Privacy, Data Protection and Law Enforcement. Opacety of the Individual and Transparency of the Power." In Privacy and the Criminal Law, edited by E Claes, A Duff and S Gutwirth, 61-. Antwerp - Oxford: Intersentia, 2006.
Gutwirth, S. Privacy and the Information Age. New York: Rowman and Littlefield, 2002.
Mantovani, E, and P Quinn. "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements." International Review of Law, Computers & Technology DOI:10.1080/13600869.2013.801581 (2013).
———. "Mhealth and Data Protection – the Letter and the Spirit of Consent Legal Requirements." International Review of Law, Computers & Technology (2013): http://dx.doi.org/10.1080/13600869.2013.801581.
Quinn, P. "The Anonymisation of Research Data — a Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the Eu Data Protection Framework?". European Journal of Health Law 24 (2017): doi 10.1163/15718093-2341416.
———. "The Eu Commission's Risky Choice for a Non-Riskbased Strategy on Assessment of Medical Devices." Computer Law and Security Review 31 (2017): 361-70.