eCare@Home

D1.4a Security and privacy, patients' rights
D1.4b Data storage, collection and access standards

Deliverable id	D.1.4-v2
Document name	eCare at Home - WP1 D1.4
Date	14-10-2013

COVER AND CONTROL PAGE OF DOCUMENT	
Project number	AAL Call 5
Project name	E-care@Home
Document ID	D1.4-v1
Dissemination level	Private
Version	1.0
Date	28-8-2013
Author(s): Organisation: Address:	Dr. Jeroen Ruwaard Vrije University Amsterdam Van der Boechorststraat 1, 1081 BT Amsterdam, the Netherlands

ABSTRACT
WP1 of the eCare@Home project covers needs research, assessment of potential users and requirements specifications. The objective of deliverable D1.4 of WP1 is to recognize and address legal and regulatory issues that may be critical to the development and subsequent deployment of the envisioned system (D1.4a - Security, privacy and patients' rights, and D1.4b - Data storage, collection and access standards). This report considers these themes from a multi-layered perspective, and focuses on 1) privacy & personal data protection, 2) patient rights, and 3) good clinical practice (i.e., clinical research regulations). Mental healthcare is highly regulated, both on the EU and on the national level. EU directives are most explicit with regard to personal data protection and clinical research, and least explicit about patient rights. Specific guidance how to implement the regulatory framework in user-friendly e-health applications is sparse. Recommendations with regard to critical regulatory issues are 1) to prepare for Medical Device Certification (CE-marking), 2) to adopt of a generic privacy framework, 3) to adopt basic EHR quality criteria (EuroRec Seal level 1), and 4) to avoid US servers/organizations for cloud-based storage of personal data.

KEYWORDS
eCare@Home, Privacy, Personal Data Protection, Security, Good Clinical Practice, Medical Devices.

VER	DATE	STATUS, CHANGES	FROM	REVIEW
1.0	28-08-2013	Initial Draft, for internal review	VUA	Alloy / HOAS
2.0	14-10-2013	National perspectives added (UK/Norway) Update of main text and recommendations (after consultation with Alloy and HOAS and feedback from InGeest).	VUA	

Contents

1 Introduction

The eCare@Home project (eCH) aims to enable older patients with mental health problems to play an active role in managing their well-being and daily functioning through the adaptation of an existing self-management and monitoring IT-platform for senior citizens (http://www.inclusionsociety.com/).

ECH aims to integrate self-management, formal care, informal care and socializing options. It is envisioned to support patients, formal carers (i.e., GP's, pharmacists, lab personnel, psychiatrists, psychologists & nurse practitioners), identified informal carers, friends and family as well as third party service providers. Table 2.1 defines identified users and tools. Figure 2.1 provides a graphical overview of the system.

WP1 of the eCH project covers needs research, assessment of potential users and requirements specifications. The objective of deliverable D1.4 of WP1 is to recognize and address legal and regulatory issues that may be critical to the development and subsequent deployment of the envisioned system.

The project proposal identifies two related project deliverables, which are combined in this document (D1.4a - Security, privacy and patients' rights, and D1.4b - Data storage, collection and access standards). The objectives, as stated in the project proposal, are:

- To outline, in general, the requirements towards security, privacy and patient rights in the mental health sector.
- To identify Europe's wide standards towards these issues, including standards towards documentation, data gathering, storage and access control.
- To further investigate and clarify variability and adaptation issues, in particular with regard to the legislation of partner's countries (NL, UK & Norway).

This report will focus these objectives on three themes: 1) privacy & personal data protection, 2) patient rights, and 3) research ethics.

The document covers law and regulations, but also norms and professional standards. Professional standards provide detailed solutions to more general legislative demands. Such standards are consulted by authorities to judge compliance. It is therefore important to follow these standards closely.

The report comprises four sections:

- **Section 2** provides an overview of general principles of *privacy and data protection*. It shows how these principles are grounded in EU directives and national regulations.
- **Section 3** covers regulations and legislation related to *(mental) health practice*, i.e., it covers patient rights.
- **Section 4** discusses good clinical practice: the ethical and scientific quality standards for the design, conduct and record of research involving humans, which is relevant given the intention within eCH to conduct a pilot test of the system.
- **Section 5** provides a synthesis and analysis of the legal and regulatory issues that are critical to the development, test and future deployment of the eCH system.

Table 1-1 eCH System Users and Tools

User	Description	Tool	Description
Patient	Mental health patients	userPad	A tablet computer executing ECH user interface software that can be used at home.
		Sensors	Sensor hardware and UserPad Apps
Formal Carers	Psychiatrist Psychologist Nurse Practitioner GP Pharmacist Blood Lab personnel	Formal Care Portal(s)	Portal suit that will allow formal carers to provide healthcare services. Portals are configured according to their roles in treatment.
Informal Carers	Identified informal carer of patient	Informal Carer Portal	Web Portal providing key health services to support informal care.
		Informal Care App	Mobile phone application providing logistical information
Friends & Family	Friends and family of patient	Friends and Family Portal	Portal providing key health services to identified friends and relatives.
3rd Party service providers	Non-treatment related service providers	3rd Party service portal	Portal allowing local service providers to deliver engaging personalised content and to help with tablet ownership challenges.

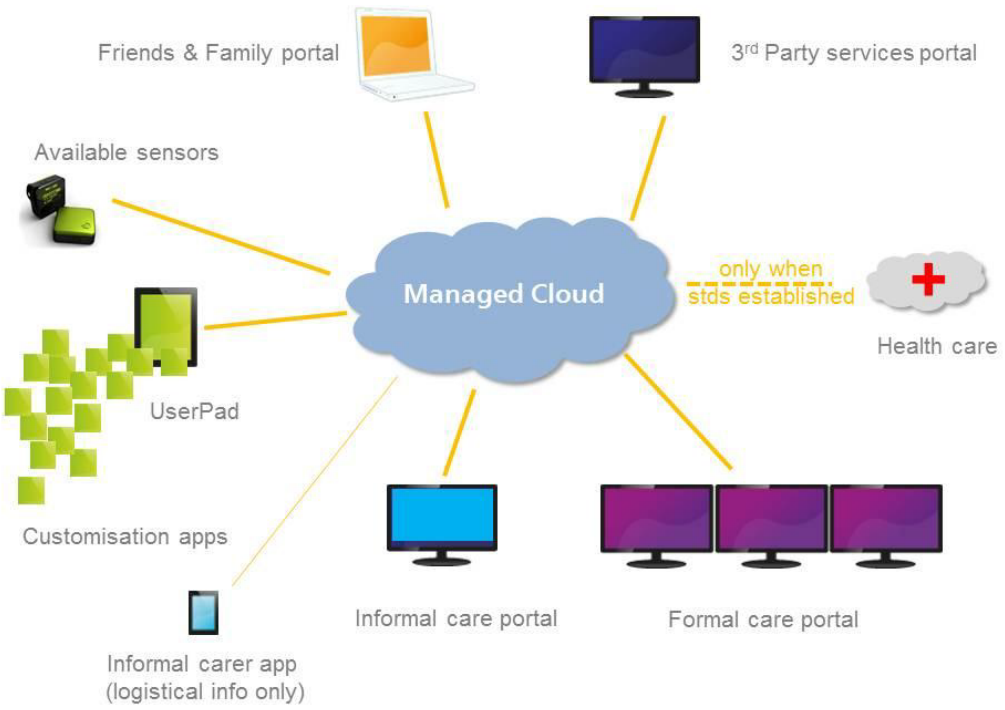

Figure 1-1 Overview of the eCH platform

2 Privacy & Personal Data Protection

2.1 EU

Privacy is a basic human right. Article 8 of *the European Convention on Human Rights* (ECHR; 1950) defines a right to respect for one's "private and family life, home and correspondence".

ECHR: Article 8 – Right to respect for private and family life
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right is reaffirmed and associated with **personal data** in Article 8 of the *Charter of Fundamental Rights of the European Union* (CFREU; 2000/2010).

CFREU: Article 8 - Protection of personal data
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.

In 1980, the *Organization for Economic Cooperation and Development* (OECD) created a comprehensive **data protection** system across Europe. This system identifies seven basic principles of personal data protection:

1. **Notice**—data subjects should be given notice when their data is being collected;
2. **Purpose**—data should only be used for the purpose stated and not for any other purposes;
3. **Consent**—data should not be disclosed without the data subject's consent;
4. **Security**—collected data should be kept secure from any potential abuses;
5. **Disclosure**—data subjects should be informed as to who is collecting their data;
6. **Access**—data subjects should be allowed to access their data and make corrections to any inaccurate data;
7. **Accountability**—data subjects should have a method available to them to hold data collectors accountable for following the above principles.

In 1995, diverging data protection legislation in EU member states led to the *Data Protection Directive* (DPD; *EU Directive 95/46/EC* 1995/2003). DPD includes and extends the principles of the 1980 privacy system of OECD. It covers the protection of individuals with regard to the processing of personal data (i.e., collection, storage, modification, deletion, retrieval, or transmission) and the free movement of such data.

DPD states that personal data can be processed only when the individual has given informed consent or when processing is in the public interest, when the purpose is legitimate, and when the data processed is relevant and not excessive to the purpose for which it was collected. Data must be kept in a form that permits identification of data subjects for no longer than is necessary and only for the purposes for which the data was

collected or is required for further processing. In addition, personal data can be transferred to countries outside the EU only if that country offers adequate levels of protection.

Article 8 of DPD prohibits the processing of **personal health data**, which are considered sensitive. However, "this prohibition does not apply where the processing of health data is required, for example, for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health care services, and where such data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional confidentiality or by another person also subject to an equivalent obligation of confidentiality" (Callens, 2003).

DPD does not consider important aspects like **globalization and technological developments** like social networks and cloud computing sufficiently and new guidelines for data protection and privacy were required. In part, these issues are handled by the *E-Privacy Directive* (Directive 2002/58 on Privacy and Electronic Communications), and its amendment Directive 2009/136 (the EU Cookie Directive). Recently, the European Commission published a *draft European General Data Protection Regulation* (GDPR, 2012) that will supersede the current DPA. The European Commission plans to unify data protection within the EU. The adoption is aimed for in 2014 and the regulation is planned to take effect in 2016 after a transition period of 2 years. (Wikipedia).

2.2 National Perspective

The Netherlands
Privacy as a basic right of all Dutch citizens is stated in Article 10 of Chapter 1 of the Dutch constitution (2008 version).

Dutch constitution – Chapter 1 / Article 10
1. Everyone shall have the right to respect for his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament.
2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data.
3. Rules concerning the rights of persons to be informed of data recorded concerning them and of the use that is made thereof, and to have such data corrected shall be laid down by Act of Parliament.

The law on the processing of personal data is defined in the *Dutch Data Protection Act* (WBP: Wet Bescherming Persoonsgegevens, 1994;1998;2000;2001). Personal data may be collected and processed for specific, explicitly defined and legitimate purposes. Any further processing of those data may - in principle - only take place for purposes which are compatible with the purposes for which the personal data was initially collected. The DPA has a separate section (Section 13) on the use of technology in the protection of personal data.

Compliance to the WBP is regulated by the (independent) Dutch Protection Authority (CBP; College Bescherming Persoonsgegevens; http://www.dutchdpa.nl/), which must be notified of the use of personal data, unless an exemption applies. Through this, the legislator has implemented Article 28 of the European DPD, which provides for the existence of such a supervisory authority which should fulfil its task completely independently.

Norway

The Norwegian Constitution of 1814 does not have a specific provision dealing with the protection of privacy, although Article 102 prohibits searches of private homes except in "criminal cases." Article 110(c) of the Constitution places state authorities under an express duty to "respect and secure human rights." In 1952, the Norwegian Supreme Court held that there exists in Norwegian law a general legal protection of "personality", which

incorporates a right to privacy (https://www.privacyinternational.org/reports/norway/i-legal-framework) .

Currently, privacy and personal data protection in Norway are regulated by the *Personal Data Act (PDA, "Personopplysningsloven", 2000)*, the *Personal Data Regulations ("Personopplysningsforskriften", 2000-2009)* and the *Regulations on the use of Information and Communication Technology ("IKT-forskriften", 2003)*. Norway is not a member of the EU. However, the PDA was designed to bring Norwegian law into compliance with the EU Data Protection Directive 95/46/EC. The Acts are monitored and controlled by the Norwegian Data Protection Authority (http://www.datatilsynet.no/). The Authority must be notified if breaches of these security obligations has resulted in the unauthorised disclosure of confidential personal data.

Personal data refer to any information and assessment that may be linked to a natural person. The information security aspects of personal data consider the assurance of confidentiality, integrity and availability of data. Measures must be taken to protect unauthorized access to personal data where confidentiality is necessary. In this regard, techniques for identification, authentication and authorization must be used to protect sensitive personal data. Proper access control mechanism must be in place. Personal data when transferred electronically beyond the physical control of data controller must be protected through encryption or other means to prevent unauthorized access, use and disclosure of data. Measures should be taken to prevent unauthorized alteration of personal data. Security measures must prevent unauthorized use of information systems. The measure should include the detection of any attempt of misuse. In this regard, temper-proof logs are needed. Institution should establish criteria for acceptable risk with regard to use of ICT systems and should conduct regular risk analyses to ensure that risk is contained within acceptable limits in relation to the institution's business. Above all, all the measures should be documented, and relevant documentation should be available to the Norwegian Data Protection Authority and the Privacy Appeals Board.

UK

Unlike many other nations, the UK has no single constitutional document, i.e., it has an uncodified or "unwritten" constitution. The Human Rights Act (HRA; 1998) provides for a limited incorporation of the European Convention on Human Rights (ECHR) into domestic law, including the right of privacy. The UK House of Lords ruled in October 2003 that there is no general common law tort for invasion of privacy and that the ECHR does not require the UK to adopt one (cf, https://www.privacyinternational.org/reports/united-kingdom/i-legal-framework). Relevant regulations are defined in the *UK Data Protection Act* ("DPA", 1998), the *Privacy and Electronic Communication Regulations* (2003-2011), and the *Freedom of Information Act* (2000). These acts are enforced by the Information Commissioner's Office (ICO; http://www.ico.org.uk), which is an independent agency. The Information Tribunal (formerly the Data Protection Tribunal) can hear appeals of decisions and notices issued by the ICO.

The UK DPA (partially) implements EU Directive 95/46/EC. It applies to personal data held by government agencies and private organisations. The obligations for entities subject to the DPA, or "data controllers," are enshrined in eight data protection principles. These principles cover, inter alia, the obligation to (i) ensure that personal data are used for specific and legitimate purposes, (ii) permit individuals access to their personal data, (iii) provide adequate technical and organisational security for personal data, and (iv) prevent the international transfer of personal data to jurisdictions not recognised to have adequate data protection laws, unless legally recognised mechanisms are deployed to protect the personal data both during and following the transfer. Data controllers are also required to register their processing activities with the Information Commissioner's Office (ICO). The UK DPA is considered to be complex. Furthermore, the European Commission has

expressed concerns about the UK's insufficient implementation of Directive 95/46/EC in a number of areas.

3 Patient rights

3.1 EU

Access to health care and medical treatment is defined as a basic right in Article 35 of the *Charter of Fundamental Rights of the European Union* (CFRE; 2010). This has a bearing to e-health applications, since these applications may potentially lower existing barriers to care.

CFRE: Article 35 - Health care Everyone has the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices. A high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities.

Protection of patient rights is defined in the *European Convention on Human Rights and Biomedicine (ECHRB)*, which was adopted by the Council of Europe in 1997 and entered into force in 1999. Over the years, ECHRB has been signed and/or ratified by many, but not all members of the European Council (e.g., while the Netherlands have signed the treaty, the UK has not). Moreover, the Convention has not been adopted by the European Union.

The Convention intends to "provide a common framework for the protection of human rights and dignity in both longstanding and developing areas concerning the application of biology and medicine". The Convention may therefore be considered as offering protection of the rights of the patient in ordinary healthcare. Relevant articles of the ECHRB are listed in Table 2.1. These encompass five basic patient rights (which incorporate the more general principles of personal data protection in the previous section):

1. Right to informed consent
2. Right to information about health
3. Rights regarding the medical file
4. Right to privacy
5. Right to complain and to compensation

The *European Charter of Patients' Rights* (ECPR) states 14 patients rights that together aim to guarantee a "high level of human health protection" (Article 35 of the Charter of Fundamental Rights of the European Union) and to assure a high quality of services provided by the various National Health Services in Europe. These rights are correlated with duties and responsibilities that both citizens and healthcare stakeholders have to assume. ECPR was drafted in 2002 by the Active Citizenship Network (ACN) in collaboration with 12 Citizens' organizations from different EU countries (see www.activecitizenship.net). ECPR has not been adopted by the EU yet. According to ACN, the 14 rights (listed in Table 3.2) are an embodiment of fundamental rights and, as such, must be recognised and respected in every country.

3-1 Selected Articles of the European Convention on Human Rights and Biomedicine *(as listed, in extended form, on http://europatientrights.eu/)*

#	Article text	Description
5	An intervention in the health field may only be carried out after the person concerned has given **free and informed consent** to it. The person shall beforehand be given appropriate information as to the purpose and nature of the intervention as well as on its consequences and risks. The person concerned may freely withdraw consent at any time	Contains the right of the patient to give his free and informed consent before examination treatment. Implies the right to refuse treatment. The patient has the right to withdraw his consent as long as the intervention has not yet been applied. The consent is often implicit (or non-verbal) as long as the patient is sufficiently informed.
8	When because of an **emergency situation** the appropriate consent cannot be obtained, any medically necessary intervention may be carried out immediately for the benefit of the health of the individual concerned	Provides for an exception to the general rule of article 5, when the consent of the patient cannot be obtained in an emergency situation. In such a case his or her consent may be presumed for any medically necessary intervention which cannot be delayed. Healthcare professionals must make every reasonable effort to determine what the patient would want.
9	The **previously expressed wishes** relating to a medical intervention by a patient who is not, at the time of the intervention, in a state to express his or her wishes shall be taken into account	'previously expressed wishes' ("living wills") may be positive (expressing the wish to an intervention) or negative (expressing refusal). These wishes are not legally binding: they have to be taken into account but not necessarily to be respected or followed. Covers emergencies but also situations where individuals have foreseen that they might be unable to give their valid consent.
10	Everyone has the right to respect for **private life** in relation to information about his or health	Implies: the right to confidentiality; the right to a medical file that is safely kept; the right to access the medical file; the right to copy (parts of) the medical file
	Everyone is **entitled to know** any information collected about his or health	A patient has a right to know all information collected about his/her health status and its prognosis.
	In **exceptional cases**, restrictions may be placed by law on the exercise of the rights in § 2 in the interests of the patient	Exceptionally, a doctor may withhold information from the patient for therapeutic reasons ("therapeutic exception" or "therapeutic necessity").
	However, the **wishes of individuals** not to be so informed shall be observed	The 'right to know' is not an obligation; therefore a patient has a right not to know his/her health status
	In exceptional cases, **restrictions** may be placed by law on the exercise of the rights in § 2 in the interests of the patient	The right not to know is not an absolute one and a law may provide that a doctor informs a patient against his wish not to know in case his ignorance would seriously harm him. A law may provide for the possibility to inform a patient against his wish not to know to protect the interests of a third party, e.g. his/her partner
23	The parties shall provide appropriate judicial protection to prevent or to put a stop to an **unlawful infringement** of the rights and principles set forth in this Convention at short notice	This article covers not only infringements which have already begun and are ongoing but also the threat of an infringement.
24	The person who has suffered undue damage resulting from an intervention is entitled to fair **compensation** according to the conditions and procedures prescribed by law	Compensation conditions and procedures are prescribed by national law. In many cases, this establishes a system of individual liability based either on fault or on the notion of risk or strict liability. In other cases, law may provide for a collective system of compensation irrespective of individual liability (no fault compensation as in Denmark and Sweden).
25	Parties shall provide for appropriate **sanctions** to be applied in the event of infringement of the provisions contained in this Convention	Domestic law must pay attention to the content and importance of the provision to be complied with, the seriousness of the offence and the extent of its possible repercussions for the individual and for society.

Table 3-2 The European Charter of Patients' Rights (Active Citizenship Network, 2002)

Article	Theme	Description
1	**Right to Preventive Measures**	Every individual has the right to a proper service in order to prevent illness
2	**Right of Access**	Every individual has the right of access to the health services that his or her health needs require. The health services must guarantee equal access to everyone, without discriminating on the basis of financial resources, place of residence, kind of illness or time of access to services.
3	**Right to Information**	Every individual has the right to access to all information regarding their state of health, the health services and how to use them, and all that scientific research and technological innovation makes available.
4	**Right to Consent**	Every individual has the right of access to all information that might enable him or her to actively participate in the decisions regarding his or her health; this information is a prerequisite for any procedure and treatment, including the participation in scientific research.
5	**Right to Free Choice**	Each individual has the right to freely choose from among different treatment procedures and providers on the basis of adequate information.
6	**Right to Privacy and Confidentiality**	Every individual has the right to the confidentiality of personal information, including information regarding his or her state of health and potential diagnostic or therapeutic procedures, as well as the protection of his or her privacy during the performance of diagnostic exams, specialist visits, and medical/surgical treatments in general.
7	**Right to Respect of Patients' Time**	Each individual has the right to receive necessary treatment within a swift and predetermined period of time. This right applies at each phase of the treatment.
8	**Right to the Observance of Quality Standards**	Each individual has the right of access to high quality health services on the basis of the specification and observance of precise standards.
9	**Right to Safety**	Each individual has the right to be free from harm caused by the poor functioning of health services, medical malpractice and errors, and the right of access to health services and treatments that meet high safety standards
10	**Right to Innovation**	Each individual has the right of access to innovative procedures, including diagnostic procedures, according to international standards and independently of economic or financial considerations.
11	**Right to Avoid Unnecessary Suffering and Pain**	Each individual has the right to avoid as much suffering and pain as possible, in each phase of his or her illness.
12	**Right to Personalized Treatment**	Each individual has the right to diagnostic or therapeutic programmes tailored as much as possible to his or her personal needs.
13	**Right to Complain**	Each individual has the right to complain whenever he or she has suffered harm and the right to receive a response or other feedback.
14	**Right to Compensation**	Each individual has the right to receive sufficient compensation within a reasonably short time whenever he or she has suffered physical or moral and psychological harm caused by a health service treatment.

The Medical Device Directive

It is increasingly recognized that e-health developers should pay close attention to EU's *Medical Device Directives 93/42/EEC* (MDD; 1993-2007; see, for example, Wolters et al, 2013; GSM Association, 2012*)*. MDD harmonizes the rules pertaining to the free circulation of medical devices in the EU. Manufacturers are obliged to place on the market or to put into service only medical devices that do not compromise the safety and health of patients, users and other persons, when properly installed, maintained and used in accordance. The MDD is intended to harmonize standards that benefit manufacturers, users and patients, and to define the requirements for the clinical testing, design, manufacture, testing/inspection, marketing, installation and service of medical devices sold within the European Union.

Products that fall within the scope of the MDD must meet all applicable **essential safety and administrative requirements** and must bear a **CE-marking** (CE: Communauté Européenne) to show that they comply with MDD. Such products may then be sold and used throughout the European Economic Area without, in principle, being subject to additional national legislation. Conversely, without CE-marking, the use of such products is not allowed.

The MDD defines a medical device as "a*ny instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, together with any accessories, including the software intended by its manufacturer to be used specially for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for, among other things, the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease, injury or handicap and the control of conception*". Software for general purposes, when used in an e-health project, is not a medical device. However, software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device.

Various sets of guidelines ('MEDDEVs') have been compiled to facilitate the implementation and interpretation of the MDD's. These can be found on the European Commission's website (http://ec.europa.eu/health/medical-devices/index_en.htm). Nonetheless, full adherence to MDD requires considerable effort, in terms of understanding, interpretation and application. A short and thorough introduction to MDD can be found in the writings of John Schnoll (1997; available at http://www.qualitydigest.com/sept97/html/ce-mdd.html and http://www.qualitydigest.com/oct97/html/mddprt2.html). A (Dutch) practical summary of MDD and the certifying process has recently been published by the National IT Institute for Healthcare in the Netherlands (NICTIZ; see Ekker, & Van Rest, 2013).

Certifying for CE-marking is, in short, a seven-step process (Ekker, & Van Rest, 2013; Schnoll; 1997):

1	Is the device a medical device?	Determine whether the device is a medical device according to MDD and, if so, what class it falls in (I, II or III; see main text for details).
2	Comply with essential requirements	Comply with minimum essential requirements for the design and manufacture of medical devices. Principles of safety should be integral to the design of the product and that the product should be suitable for its intended purpose.
3	Compile a technical dossier	Prepare the appropriate technical documentation to demonstrate full compliance with the requirements of the directive and associated technical standards.
4	External audit	Seek third-party certification audit of step 2 and 3 (not needed for Class I devices).
5	Register the device	Register the device at the designated national Notifying Body.
6	Attach CE-mark to device	Place CE-marking on the product
7	Aftercare	Ensure appropriate product support after distribution.

The MDD places all medical devices into one of four **classes of increasing risk** to the patient according to their properties, function and intended purpose. The level of control is proportionate to the level of risk to ensure protection of patient health.

- **Class I devices** are those that pose a low risk to the patient and, except for sterile products or measuring devices, can be self-certified by the manufacturer. Generally speaking, these devices do not enter into contact or interact with the body.

- **Class IIa** devices are of a medium risk that may require assessed quality systems to the ISO 9000/EN46000 standards. These devices are invasive in their interaction with the human body, but the methods of invasion are limited to natural body orifices. The category may also include therapeutic devices used in diagnosis or in wound management.

- **Class IIb** devices are of a medium risk that may require assessed quality systems to the ISO 9000/EN46000 standards; third-party certification is required. They are either partially or totally implantable within the human body, and may modify the biological or chemical composition of body fluids.

- **Class III** devices are of high risk and require design/clinical trial reviews, product certification and an assessed quality system. All third-party product and system certification must be conducted by a European Notified Body (or designee through formal agreement). Generally speaking, these devices affect the functioning of vital organs and/or life-support systems.

The MDD requires that the manufacturer of medical devices keeps a product-related, adequate and efficacious quality system. The application of the quality system must ensure that the products conform to the provisions of the MDD. All the elements, requirements and provisions adopted by the manufacturer for his quality system must be documented in a systematic and orderly manner in the form of written policies and procedures such as quality programs, quality plans, quality manuals and quality records.
The ISO 9000 series of standards is the most popular way for the proper organization of a quality management system. EN 46003 in combination with the guidance standards EN 724 or EN 50103 - which all include ISO 9001 - are harmonized European standards. On the other hand even ISO 9001 in combination with the additional requirements of EN 46003, under consideration of EN 724 or EN 50103, does not fully cover the requirements of the MDD.

Additional aspects to be covered by the quality management system include:
- the technical documentation
- reference to the essential requirements according to Annex I of the MDD
- information about harmonized standards and medical device regulations
- risk analysis
- labeling and instruction
- different languages
- post-marketing surveillance
- reporting under the vigilance system
- retention of certain documents

The MDD have been developed to guide developments in the medical domain. Increasingly, partly because of the rise in mental health apps for mobile devices, the MDD are applied to mental health e-health applications as well. Despite interpretative difficulties, it seems correct to consider the MDD for mental health applications as well. Given the ambitions of the eCH-project, it is likely that eCH would be classified as a Class I medical device. However, specific guidance is sparse, which means that the final outcome of classification efforts can not be predicted with absolute certainty.
In the context of MDD, developers and providers of e-health applications may face unclear **liability**. As noted by Callens (2003):

> "In the case of a defective medical device, the *Product Liability Directive* has to be considered. This Directive establishes the general principle that a producer is liable for damages caused by a defect in its product. A product is defective when it does

not provide the safety that a person is entitled to expect, taking all circumstances into account, including the presentation of the product, the use to which it reasonably could be expected to be put and the time at which the product was put into circulation."

"The issue of liability becomes very important in the case of 'telemonitoring', whereby medical devices .. follow the patient. ... These devices send electronic messages about the patient's health situation to the doctor in charge at specific regular intervals. However, the device may not always contain an alarm system for emergency situations and does not always include twenty-four-hour assistance. The question then is whether physicians should hesitate to use these new medical methods, despite their technological efficiency, for fear of the burden of unclear liability. Would the doctor be held liable for not responding immediately to a message received during his absence? Written and oral information about the patient using the device and how information received by the doctor will be handled is important. Patients will have to be informed accurately – and in such a way that they can understand – of the doctor's limited availability and, for example, that the medical device has no alarm."

3.2 National Perspective

The Netherlands

Patient rights
Patient rights in the Netherlands are grounded in the *Act on the Medical Treatment Contract* (WGBO: Wet op de Geneeskundige Behandelovereenkomst, 1994), as part of the Dutch Civil Code (DCC; Book 7). The main purpose of the Act is to clarify and strengthen the legal position of the patient. The Act stipulates the rights and obligations that apply to care providers and patients from the moment when the course of treatment or the examination commences. The Act regulates, among other things, consent to medical treatment, duty of disclosure of the care provider, inspection of medical records (including the right to be forgotten), duty of confidentiality, privacy and liability. A more comprehensive Act, the *Patient Rights Healthcare Act* (Wcz, Wet cliëntenrechten zorg), has been proposed and is currently in development (see: https://zoek.officielebekendmakingen.nl/kst-32402-12.html).

Quality of Care
The 1996 *Quality of Health Facilities Act* (KZi) replaced many detailed quality norms with broadly defined requirements applicable to all health care institutions (Buijsen, 2006). For example, institutions are required to systematically collect data on the effectiveness, patient centeredness and efficiency of the provided care, to set up a quality assurance system and to produce publicly available quality reports annually. The Act transfers the responsibility for quality to health care institutions and gives them the freedom to fulfil the general requirements in a way that results in "responsible care" (Schäfer et al, 2010).

Quality of care provided by individual healthcare workers is regulated through the *Individual Health Care Professions Act* (BIG: Wet op de beroepen in de individuele gezondheidszorg). The BIG aims to safeguard the quality of the practice of professions and to protect patients from incompetent healthcare practitioners. Similar to the Quality of Health Facilities Act (KZi), this Act provides a framework for health care providers while details have to be worked out in lower-level regulation. The BIG contains requirements with regard to (1) competence (requirements for registration and title protection), (2) expertise (the practitioner has to be an expert in the professional domain) and (3) proficiency (stipulated restrictions and functional autonomy). The BIG register is one of the tools for implementing the Healthcare Professionals Act (Schäfer et al, 2010). The "BIG register" (https://www.bigregister.nl/en/), which provides a public list of individual working in the regulated professions, is one of the tools for implementing the Healthcare Professionals Act.

As a main advisory body to the Minister of Health, Welfare and Sport, the Health Care Inspectorate (IGZ) plays an important role in regulating the quality of care. The Inspectorate enforces statutory regulations on public health; investigates complaints and irregularities in health care; and takes measures if deemed necessary and appropriate (Schäfer et al, 2010).

Healthcare Security standards
Confidentiality and protection of sensitive patient data is protected by a series of Dutch standards maintained by het Nederlands Normalisatie-instituut (http://www.nen.nl). *NEN7510, the Netherlands Norm for information security in the health care sector* is the dominant standard. In the past years, many health care organisations have adopted the NEN 7510 standard and supervisory bodies use this and related standards as their **reference security framework**. The objective of NEN 7510 is to create awareness on information security in the health sector and to enable a practical approach to implementing security. The standard requires information security controls to be implemented in a controlled and auditable manner (http://www.standards.org/standards/listing/nen_7510).

NEN 7510 was published in 2004. The standard was based on the *Code of Practice for Information Security*, published as *NEN-ISO/IEC 27002* and aligned to the Dutch Healthcare sector. In 2005 the related standards NEN 7511-1, 7511-2 and 7511-3 were published. These auditable standards are applicable for 3 specific types of healthcare organisations and are supplemental to NEN 7510. NEN 7511-1 covers complex organisations such as hospitals, university medical centres, healthcare centres, municipal health services and mental healthcare services. NEN 7511-2 covers cooperating or associated organisations such as home care services, nursing homes, blood banks, ambulance services and medical rehabilitation organisations. NEN 7511-3 covers solo practices that include pharmacies, general practitioners, physiotherapists, psychiatrists, psychologists and dentists.

Use of Civilian's Service Number
A highly specific regulation related to patient rights is the *Law on the use of the Civilian's service number in healthcare* (wBSN-z; Wet gebruik burgerservicenummer in de zorg). As of 2008, Dutch healthcare is obliged to use the *Civilian's service number* (Burgerservicenummer; BSN) as the **distinguishing ID property** for cross-enterprise communication.

Medical Devices
EU Medical Device Directives are anchored in the *Dutch Medical Device Act* (WMH: Wet op de Medische Hulpmiddelen), which, since its initial publication in 1970, has been amended several times. **The Dutch Healthcare Inspectorate** (IGZ: Inspectie voor de Gezondheidszorg) ensures that the manufacturers and suppliers of medical devices observe all relevant legislation, and takes action in the event of a breach of the regulations. The Inspectorate evaluates all incoming reports about malfunctions or quality issues relating to medical devices. It also oversees the activities of DEKRA Certification, the Notified Body for the Netherlands (http://www.dekra-certification.nl/nl/managementsysteem-certificering). Recently, in response to the sharp growth in the mobile health app market, the Inspectorate announced **intensified enforcement of CE-mark medical device certification** in 2014 (Ekker & Van Rest, 2013).

Norway

Patient rights

Patient rights for Norwegian citizens are laid down in the Patients' Rights Act (1999). The Act contains provisions about access to essential health care, assessment by a specialist within 30 days, choice of hospital, the right of access to and the right to correct patient records, client participation, information, the special rights of children, consent to health care and individual plans for people who require several different types of services. The supervision authorities are the Norwegian Board of Health Supervision (the central office), and the Offices of the County Governors. The Norwegian Board of Health Supervision, part of the Ministry of Health and Care Services (HOD) is the superior, national supervision authority. At the level of the counties, supervision is carried out by the Offices of the County Governors.

Protection of personal health data is regulated by the Personal Health Data Filing System Act (2001). The purpose of this Act is to contribute towards providing public health services and the public health administration with information and knowledge without violating the right to privacy. The Act ensures that personal health data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and respect for private life and ensure that personal health data are of adequate quality.

Quality of care

Safety for patients and quality within the health service as well as trust in both health personnel and the health service are defined in the *Health Personnel Act* (1999). The *Norwegian Registration Authority for Health Personnel* (Norwegian: Statens

autorisasjonskontor for helsepersonell, SAK (until 2012 SAFH)) is the authority that licenses health care personnel who fulfill requirements laid down in the Health Personnel Act.

Healthcare security standards

The Norwegian "*Code of Conduct for information security in the healthcare, care, and social services sector*" ("Normen", 2010) is a holistic approach to an information security policy. Nytrø, Sørby & Seland (2012) describe this code as follows:

> "The Code itself covers all aspects of information security as regulated by Norwegian law. In some instances, the Code of Conduct defines more stringent rules than the law itself. The Code ensures a secure interoperability for all organizations that comply with the regulations set forth in the Code. The Code of Conduct has been developed by representatives from the sector, and comprises the sector's view of how to ensure information security. In addition to developing the Code of Conduct, the sector has produced a set of short practical guidelines on how to meet the individual requirements in the Code. Note: Version 2 of the Code of Conduct was published in September 2010. New versions of other Code of Conduct documents in English were published in February 2011.
>
> An increasing amount of communication in the health sector, both internally, i.e. within a health service provider entity, and between such providers, is taking place electronically. The fact that the information is collected, stored and spread electronically, in an extent hardly imaginable only a few years back, evoked a need for mechanisms safeguarding that all aspects of information security in the sector are handled adequately. Consequently, in 2003, the Directorate for Health and Social Affairs invited affected organizations and authorities to establish project group, whose objective was to compose a holistic set of information security rules for the sector. A prerequisite was that the group's recommendations were to be in accordance with the data protection and information security principles laid down in EU Directive 95/46/EC (the Data Protection Directive). As a result, on August 7th 2006, the *Code of conduct for information security in the health sector* ("the Code") was launched, ready to be used by small, medium-sized and large health service providers alike, and by the collaborating partners of these bodies, as a means to establish satisfactory information security.
>
> The Code is supposedly the first of its kind in Europe; no other overall standards on information security in the health sector are yet developed in any of the EU/EEA countries. Norsk Helsenett SF ("Norwegian Health Network") is the provider of a national infrastructure for electronic communication in the health sector, helsenettet ("the health network"). In order to be linked to, and actually utilize, this network, the health service provider must enter into an "affiliation agreement" with the company. By force of this agreement, the entity admitted to the infrastructure, is obliged to comply with the Code. By this mechanism, the health service providers ensure that the receivers of health-related data – i.e. collaborating partners of many kinds – within the network, all meet the standards of the Code, and thus of the legal provisions. Failing to meet the information security standards of the Code, may lead to the exclusion of the contract-breaching entity."

4 Good clinical practice

4.1 EU

Guiding principles in healthcare research are provided by two international standards. The first is the *Declaration of Helsinki* (DOH; World Medical Association; 1964-2008), which is a set of ethical principles regarding human experimentation developed for the medical community by the World Medical Association. Since its inception, the Declaration has witnessed six revisions. DOH is not a legally binding instrument in international law, but instead draws its authority from the degree to which it has been codified in, or influenced, national or regional legislation and regulations. The Declaration is **morally binding** on health researchers, and that obligation overrides any national or local laws or regulations, if the Declaration provides for a higher standard of protection of humans than the latter. Investigators still have to abide by local legislation but will be held to the higher standard.

The fundamental principle is respect for the individual (Article 8), the right to self determination and the right to make informed decisions (Articles 20, 21 and 22) regarding participation in research, both initially and during the course of the research. The investigator's duty is solely to the patient (Articles 2, 3 and 10) or volunteer (Articles 16, 18), and while there is always a need for research (Article 6), the subject's welfare must always take precedence over the interests of science and society (Article 5), and ethical considerations must always take precedence over laws and regulations (Article 9).
The recognition of the increased vulnerability of individuals and groups calls for special vigilance (Article 8). It is recognised that when the research participant is incompetent, physically or mentally incapable of giving consent, or is a minor (Articles 23, 24), then allowance should be considered for surrogate consent by an individual acting in the subjects best interest. In that case consent should still be obtained if possible (Article 25).

According to DOH, research should be based on a thorough knowledge of the scientific background (Article 11), a careful assessment of risks and benefits (Articles 16, 17), have a reasonable likelihood of benefit to the population studied (Article 19) and be conducted by suitably trained investigators (Article 15) using approved protocols, subject to independent ethical review and oversight by a properly convened committee (Article 13). The protocol should address the ethical issues and indicate that it is in compliance with the Declaration (Article 14). Studies should be discontinued if the available information indicates that the original considerations are no longer satisfied (Article 17). Information regarding the study should be publicly available (Article 16). Ethical publications extend to publication of the results and consideration of any potential conflict of interest (Article 27). Experimental investigations should always be compared against the best methods, but under certain circumstances a placebo or no treatment group may be utilised (Article 29). The interests of the subject after the study is completed should be part of the overall ethical assessment, including assuring their access to the best proven care (Article 30). Wherever possible unproven methods should be tested in the context of research where there is reasonable belief of possible benefit (Article 32).

A second set of international quality standards are provided by the International Conference on Harmonisation (ICH) under the general name *Good Clinical Practice (GCP;* http://ichgcp.net/*)*. ICH is an international body that defines standards, which governments can transpose into regulations for clinical trials involving human subjects. ICH-GCP guidelines include protection of human rights as a subject in clinical trial, assurance of the safety and efficacy of the newly developed compounds, standards on how clinical trials should be conducted, and define the roles and responsibilities of clinical trial sponsors, research investigators, and monitors.

Requirements for the conduct of clinical trials in the EU are provided in *Directive 2001/20/EC* (the Clinical Trials Directive) of the European Parliament and of the Council of 4 April 2001 (http://ec.europa.eu/health/human-use/clinical-trials/) and Good Clinical Practice Directive 2005/28/EC. The Directives seek to simplify and harmonize the administrative provisions governing clinical trials in the European Community by

establishing explicit procedures for trial documentation and registration and provide general guidance for the conduct of clinical research. Although the directives relate to clinical medicinal research, in some countries, the whole regime has been applied to all research involving patients (Van Veen, 2009).

4.2 National Perspective

The eCH system will be pilot-tested only in the Netherlands (by VUA and GGZInGeest). Hence, this report will only review regulations regarding clinical research from the Dutch perspective.

In the Netherlands, principles of good clinical practice (and specifically EU's Clinical Trial Directive) are implemented in *the Medical Research involving Human Subjects Act* (WMO: Wet Medisch-wetenschappelijk Onderzoek met Mensen). Research covered by WMO must be submitted to an accredited Medical Research Ethics Committee (MREC) for approval before it is carried out. The research committee reviews research protocols in accordance with the rules laid down in the WMO. Research subject to the WMO cannot be carried out without a positive judgement. Starting a study subject to the WMO without a positive judgement is a legal offense which may result in six months imprisonment or a € 19.500 fine (maximum; see: Wet Medisch-wetenschappelijk Onderzoek met mensen, Artikel 33 Strafbepalingen)

The central body (CA; 'competent authority') responsible for implementing WMO is the Central Committee on Research Involving Human Subjects (CCMO; Commissie mensgebonden onderzoek; http://www.ccmo-online.nl). CCMO accredits Medical Research Ethics Committees (METC), reviews protocols (along with the accredited committees), registers research protocols of clinical trials in a public database (https://www.toetsingonline.nl/), handles appeals and objections and provides general information to the field regarding WMO. The Dutch Health Inspectorate (IGZ) is the monitoring authority.

Practically, researchers have to follow a four-step procedure to obtain ethical review of their studies:

1. In step 1, it is determined whether WMO applies. Studies are subject to the WMO if 1) it is medical/scientific research, and if 2) people are subjected to procedures or are required to follow rules of behaviour. Scientific research is research in which data is collected and studied in a systematic way in order to answer the question that the research is carried out to address, and to produce generally valid statements and new conclusions. Research involving human subjects only falls within the remit of the Act if it involves any form of invasion of the study participant's integrity. Boundaries are not clear-cut. Often an initial review of the study by the review board is necessary.
2. In step 2, it is determined whether the review will be conducted by an accredited METC and/or by CCMO.
3. In step 3, the researchers prepare a set of standard documents (research files), which are eventually submitted to the review committee. This set includes the research protocol providing a highly structured and detailed description of the study, but also informed consent texts, patient information leaflets, etc. etc. In addition, the study is registered in the central trial repository (https://www.toetsingonline.nl/). A study review can take up to 60 days.
4. If the study review is positive, the study can start. The reviewers (METC/CCMO) must then be informed of the starting date of the study, any amendments to the protocol, unexpected and undesirable effects or premature termination (if applicable), annual progress, and – eventually - of the final results.

5 Summary

In this report, the landscape of mental healthcare regulations was sketched. General requirements towards security, privacy and patient rights in mental health practice and research were discussed. Europe's standards towards these issues were identified, including standards towards documentation, data gathering, storage and access control. In addition, national regulations were considered. In consort with the other tasks in WP1 (needs assessment, requirement specification and system architecture specification), this will inform further development of the envisioned eCH platform.

The overview shows that mental healthcare is highly regulated, both on the EU and on the national level. EU directives are most explicit with regard to personal data protection and clinical research, and least explicit about patient rights. However, this is more than made up for by detailed national healthcare regulations and professional standards.

What can be said about legal and regulatory issues that are *critical* to the development and subsequent deployment of the eCH platform?

A first observation is that existing regulations constrain mental healthcare and the eCH platform. E-health = health. When ICT is used to implement healthcare processes, the ICT application should comply with current healthcare regulations and standards. Current regulations are set up to protect our patients, to raise the quality of care and to ensure free flow of innovations across EU member states. In that sense, awareness and application of the regulative framework are critical to the success of the ECH project.

Second, it should be noted that current regulations and standards provide limited detailed guidance how to implement and safeguard their core principles in user-friendly e-health applications in every-day practice. Consider for example, personal data protection, which, in practice, rests on unambiguous user identification. Within the digital realm, a variety of user authentication solutions exist and the most secure technological solution is not applied the most, presumably because it is also more demanding and technically complex (Fernández-Alemán, Señor, Lozoya & Toval, 2013). The eCh-project would benefit from an accompanying overview of best ICT-*practices* in the implementation of current mental health regulations, which was beyond the scope of this report.

Third, it is important to stress that boundaries defined by most regulations are not clear-cut and that compliance with current dominant practices in mental health is not perfect. Most regulations and standards leave considerable room for interpretation and implementation, especially when translated into the digital realm. Moreover, regulative bodies appear to tolerate certain violations of regulations. For instance, in mental healthcare today, mental health professionals are known to use standard (unencrypted) e-mail in the communication with their clients. This presents a clear threat to the principles of confidentiality and personal data protection, since it cannot be ruled out that the communication can be intercepted by third parties.

Fourth, eCH may benefit from the adoption of an overarching generic privacy framework. Privacy and personal data protection are crucial to quality mental healthcare. Privacy is a basic right, one of the cornerstones of the therapeutic relationship and a key element of properly conducted clinical trials. Given this multi-layeredness, there is considerable overlap in the privacy principles defined in the regulations. Avancha, Baxi & Kotz (2012) analyzed several international frameworks privacy frameworks (including the EU Data Protection Directive) and used this to compile a list of ten basic privacy requirements for m(obile)Health applications.

5-1 The mHealth privacy Framework of Avancha, Baxi and Kotz (2012)

1	**Openness and Transparency**	Users should be able to know what information has been collected about them, the purpose of its use, who can access and use it, and where it resides. They should also be informed about how they may obtain access to information collected about them and how they may control who has access to it. The system should be open about the policies and technologies in use.
2	**Purpose Specification**	The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes, or others that are specified on each occasion of change of purpose
3	**Collection Limitation and Data Minimization**	Personal health information should only be collected for specified purposes and should be obtained by lawful and fair means. The collection and storage of personal health data should be limited to that information necessary to carry out the specified purpose. Where possible, consumers should have the knowledge of or provide consent for collection of their personal health information
4	**Use Limitation (Transitive).**	Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified. The information policies and practices should follow the data through chain of trust agreements that require business partners to adhere to the applicable policies and practices.
5	**Individual Participation and Control**	Users should be able to control access to their personal information. They should know who is storing what information on them, and how that information is being used. They should also be able to review the way their information is being used or stored. Users should be able to make informed choices about what data is collected, how it is used, and to whom it is disclosed. Patients can designate proxies to act on their behalf.
6	**Data Quality and Integrity**	All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and up-to-date. Users should be able to correct mistakes in their records.
7	**Security Safeguards and Controls**	Reasonable safeguards should protect personal data against such risks as loss or unauthorized access, use, destruction, modification, or disclosure.
8	**Accountability and Remedies**	Entities in control of personal health information must be held accountable for implementing these principles. Remedies must exist to address security breaches or privacy violations.
9	**Access to Data**	Users should have an easy method to obtain their PHI in a readable electronic format. Users should be able to annotate the records submitted by others, as well as to enter their own information, with entered data marked as such.
10	**Anonymity of Presence**	The presence of medical sensing devices, or the nature of sensor-data collection, should not be observable by nearby parties (this privacy threat is unique to mHealth).

A fifth observation is that the Medical Device Directives demand attention. It is likely that eCH components will be classified as a medical device and that, consequently, these components will have to be considered for CE-certification. More strict enforcement of MDD has been announced and recent experiences with VU METC indicate that failures to comply with MDD may result in significant delays in research projects. Critically, it is forbidden to use or distribute medical devices that fall under MDD without proper CE-marking, although research is allowed, as long as the research efforts are directed toward CE-certification. Three actions are recommended: 1) Determine the class and type of the medical device according to the MDD of each proposed eCH component (Class I, II), 2) set up a road map for Risk Management (e.g., as described in Ossebaard, De Bruijn, Van Gemert-Pijnen & Geertsma, 2013), and 3) identify and comply with relevant quality standards (to which this report provides a first guidance).

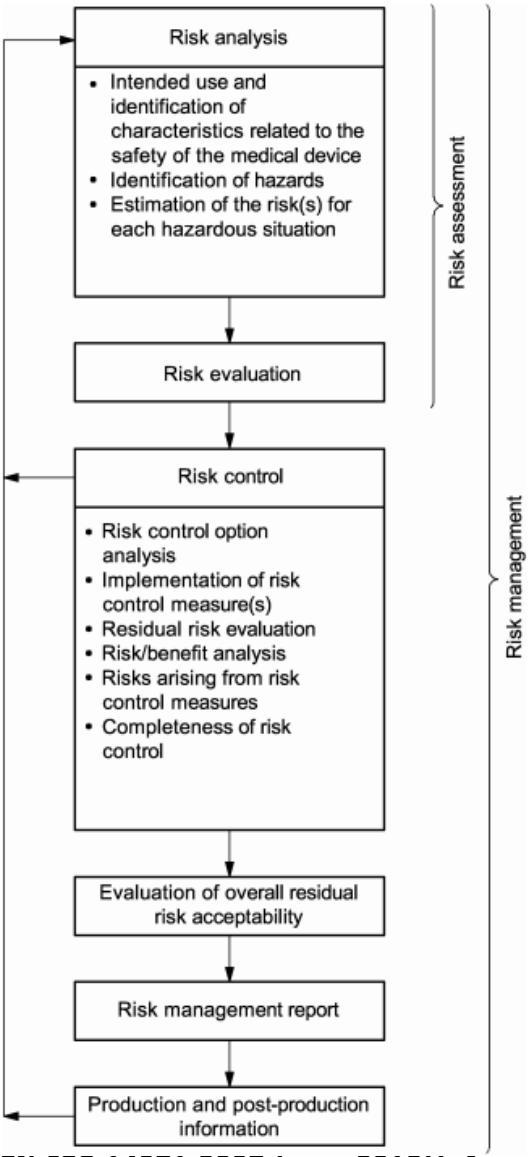

Figure 5-1 ement process (NEN-EN-ISO 14971:2007 (corr. 2012)). [reproduced in Ossebaard et al, 2013; copyright remains with NEN www.nen.nl]

6 Recommendations

1. Prepare for CE-marking certification of the eCH "Medical Device"

- **Classify the eCH system** according to the MDD directives based on final eCH requirements as documented in the functional needs assessment documents of WP1 of the eCH project (D1.1 User demands, D1.2 Design and Specification of the userPad, customisation apps, informal care portal, formal care portal and the care centre and D1.3 Specification of the IT environment). Based on current drafts of these reports, eCH most likely will be classified as a Class 1 medical device (since eCH has a therapeutic purpose, contains monitoring and possibly automated feedback options so that safety concerns apply). In that case, self-certification will suffice. However, given the envisioned monitoring/feedback functions, eCH may also fall under Class II, since current regulations are not explicit about the status of measurement of mental health parameters (see also the third bullet below). The more general recommendation is to aim for Class 1 and to update product requirements where possible to avoid Class II classification.
- **Assess documentation procedures** and/or certification of quality processes, quality control, risk and hazard assessment, testing and analysis of both the development process and the intended use of the eCH system. In practice, this means that the manufacturer should (start to) adopt a quality system such as ISO 9000/EN46000/EN 724/EN 50103.
- **Submit the study protocol of the pilot tests early,** to provide ample time for discussion with the Institutional Ethics Review board of VUA. While CE-markings are required for medical devices, pilot studies can probably be run even if the CE-marking certification process has not been completed. However, the pilot trial must then focus on the assessment of a) patient safety and b) clinical effectiveness and CE-marking certification efforts from the manufacturers side must be reported in the application to the review board (e.g., what quality systems are in place?).

2. Adopt a generic privacy framework
Match the abstracted privacy requirements of the mHealth privacy Framework of Avancha, Baxi and Kotz (2012) with the characteristics of the eCH system. Provide a detailed description of the way in which the eCH system implements these high-level requirements of this framework. This would ensure at least basic adherence to many of the privacy regulations listed in this document.

3. Aim for EuroRec Seal Level 1 certification. The main objective of the EuroRec Seal (http://www.eurorec.org) is to initiate a process of harmonisation between Electronic Healt Record systems, favouring cross-border interoperability of those systems. The EuroRec seal has two levels. Level 1 defines a minimal set (N = 20) of quality criteria for EHR systems and focuses on trustworthiness of the clinical data (see Appendix 2 for a detailed list of the criteria). Adopting these requirements would ensure adherence to basic requirements of quality EHR systems. This would provide a useful first step towards the implementation of more extensive EHR and security requirements frameworks, such as the Norwegian Code of Conduct (e.g., see Nytrø, Sørby & Seland 2012), and the Dutch Mental Health EHR requirements reference document .

4. Avoid storage of personal data on US servers
Given the US Patriot Act, personal health data of EU-citizens should not be stored on the servers of American organizations, since stakeholders may hold the position that confidentiality can not be ensured under that Act. In view of this, the eCH project should best opt for an implementation solution in which data is stored on servers that are located in the country of residence (ideally) or, at a minimum, at servers managed by EU parties and located in EU countries in which EU privacy regulations apply. On an architecture level, it would be useful if the database would make a clear distinction between personal data and health data. The latter are generally considered more sensitive. When the system allows for

split storaging of these two types of data, it is likely that the eCH system is accepted more easily on local sites.

7 Sources

Athena Privacy LLC (2010) *Privacy for the Pharmaceutical and Medical Device Industry: An Introduction*. Available online.

Avancha, S., Baxi, A. & Kotz, D. (2012). Privacy in mobile technology for personal healthcare. *ACM Computing Surveys (CSUR), 45(1)*.

Buijsen MAJM (2006). Kwaliteitsregulering in de gezondheidszorg [Quality regulation within health care]. In: Hermans HEGM, Buijsen MAJM, eds. *Recht en gezondheidszorg. [Law and health care]*. Maarssen, Elsevier Gezondheidszorg:107–130.

Callens, S. (2010) The EU legal framework on e-health. In: *Health Systems Governance in Europe. The Role of European Union Law and Policy*. Cambridge: Cambridge University Press. Available online.

GSM Association (2012) *mHealth and the regulatory framework for medical devices*. London: GSMA. Available online.

Ekker, A., Burghouts, A., Hutink, H. Uitendaal, P. Golyardi, S. & Veereschild, S. (2013). *Wet- en regelgeving in de zorg [Law and regulations in healthcare]*. Den Haag: NICTIZ. Available online.

Ekker, A. & Van Rest, B. (2013) *Medische apps, is certificering nodig? In 7 stappen naar een CE-markering voor uw app [Medical apps, is certification required?]*. Den Haag: NICTIZ. Available online.

El-Wakeel, H. & Taylor, G, & Tate, J. J. T. (2006). What do patients really want to know in an informed consent procedure? A questionnaire-based survey of patients in the Bath area, UK. *J Med Ethics 2006; 32*:612–616

European Commission (1995). *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Available online

European Union (2013*) National Patient Rights Legislation : The Netherlands*. Available online

Fernández-Alemán, J.L., Señor, I. C., Lozoya, P. Á. O. & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of Biomedical Informatics, 46 (2013) 541–562.

LinkLaters (2013). A global report on the status of data protection laws in 2013. London, LinkLaters LLP. Available online

NICTIZ (2007). *Kwalificatieschema voor een ZorgServiceProvider*. Den Haag: NICTIZ.

Nytrø, Øystein, Sørby, I.D. & Seland, G. (2012) *D1.3: Security and privacy, reliability analysis – Norwegian perspective*. From WP1 of the EU / AAL InclusionSocietyproject.

Ossebaard HC, De Bruijn ACP, Van Gemert-Pijnen JEWC & Geertsma RE (2013) Risks related to the use of eHealth technologies - an exploratory study. [RIVM Report 360127001/2012]. Bilthoven: RIVM [National Institute for Public Health and the Environment].

Schäfer W, Kroneman M, Boerma W, van den Berg M, Westert G, Devillé W & van Ginneken, E. The Netherlands: Health system review. *Health Systems in Transition, 2010*, 12(1):1–229.

Stroetmann, K., Artmann, J., Stroetmann, V,N. with Protti, D., Dumortier, J., Giest, S., Walossek, U. & Whitehouse, D. (2011). *European Countries on their Journey towards national ehalth infrastructures: Final European Progress Report*. Brussels: European Commission. Available online.

Van Veen, (2009). The Implementation of Directive 2001/20/EC in Europe. Tijdschrift voor Gezondheidsrecht, 33, 6 Available online.

Wolters, M. et al. (2012) Monitoring People with Depression in the Community: Regulatory Aspects. In: *Proceedings of BCS HCI 2012 Workshops: People, Computers & Psychotherapy*.

World Medical Association (1964). *Declaration of Helsinki. Ethical Principles for Medical Research Involving Human Subjects*. Available online.

8 Appendix I: Identified Regulations & Standards

Theme	Scope	ShortName	Full name	Year	Summary
Privacy	EU	ECHR	The European Convention on Human Rights	1950	Defines privacy as a basic right.
Privacy	EU	CFREU	The Charter of Fundamental Rights of the European Union	2000/2010	Defines privacy as a basic right.
Privacy	NL	Dutch Constitution	Constitution of the Netherlands	1815-2008	Defines privacy as a basic right.
Privacy	NO	Norwegian Constitution	The Constitution of the Kingdom of Norwa	1814	Defines privacy as a basic right (indirectly).
Privacy	UK	HRA	The Human Rights Act	1998	Defines privacy as a basic right.
Personal Data protection	EU	The Data Protection Directive (DPD)	EU Directive 95/46/EC; amendment 2003	1995/2003	Regulates the processing and free movement of personal data.
Personal Data protection	EU	E-Privacy Directive	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	2002	Regulates data protection and privacy in the digital realm.
Personal Data protection	EU	EU Cookie Directive	Directive 2009/136/EC	2009	Regulates data protection and privacy in the digital realm (amends the E-Privacy Directive)
Personal Data protection	EU	EGDPR	European General Data Protection Regulation	2012 (draft)	Proposed update of EU DPD.
Personal Data protection	NL	WBP (DDPA)	Wet Bescherming Persoonsgegevens (Dutch Data Protection Act)	1994/1998/2000	Dutch DPD; governs processing of personally identifiable information.
Personal Data protection	NO	PDA	Personal Data Protection (Personopplysningsloven)	2000	Norwegian DPD; governs processing of personally identifiable information.

Theme	Scope	ShortName	Full name	Year	Summary
Personal Data protection	NO	PDR	Personal Data Regulations (*"Personopplysningsforskriften*)	2000-2009	Norwegian DPD; governs processing of personally identifiable information.
Personal Data protection	NO	IKT-forskrifte	The Regulations on the use of Information and Communication Technology (IKT-forskrifte)	2003	Defines personal data protection in the digital realm.
Personal Data Protection	UK	UK DPA	Data Protection Act	1998	UK DPD; governs processing of personally identifiable information.
Personal Data Protection	UK	UK DPA	Privacy and Electronic Communication Regulations	2003-2011	Defines personal data protection in the digital realm.
Personal Data Protection	UK	Information Act	Freedom of Information Act	2000	Defines a right to acces information held by public authorities.
Patient rights	EU	CFREU	The Charter of Fundamental Rights of the European Union.	2000/2010	Defines access to preventive health care and medical treatment as a basic right.
Patient rights	EU	ECHRB	European Convention on Human Rights and Biomedicine	1997	Provides a common framework for patient rights.
Medical Devices	EU	The Medical Device Directives (MDD)	Council Directive 93/42/EEC concerning medical devices	1993/2007	Defines rules pertaining to the safety, administrative requirements, and free circulation of medical devices in the EU.
Liability	EU	Product Liability Directive	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 1985 No. L210/29.	1985	Regulates liability for damages caused by defective products.
Risk Management	International	ISO 14971	NEN-EN-ISO 14971 Medical devices -- Application of risk management to medical devices	2000 - 2007	Specifies a process for a manufacturer to identify the hazards associated with medical devices.
Patient rights	NL	WGBO	Dutch Medical Treatment Agreement Act (Wet op de Geneeskundige Behandelingsovereenkomst)	1994 / 2007	Stipulates the rights and obligations that apply to care providers and patients.
Patient rights	NL	Wcz	Wet cliëntenrechten zorg (Patient Rights Healthcare Act)	Proposed	Clarifies and strengthens the legal position of patients.

Theme	Scope	ShortName	Full name	Year	Summary
Patient rights	NL	Wbsn-z	Wet gebruik burgerservicenummer in de zorg (Law on the use of the Civilian's service number in healthcare)	2008	In cross-enterprise communication of patient data, the Civilian's service number must be used as the distinguishing ID property.
Patient rights	NO	PRA	Patients' Rights Act		
Quality of care	NL	KZi	*Kwaliteitswet zorginstellingen (Quality of Health Facilities Act)*	1996	Broadly defineds quality requirements applicable to all health care institutions.
Quality of Care	NL	BIG	*Wet op de beroepen in de individuele gezondheidszorg) (Individual Health Care Professions Act)*	1993	Safeguards the quality of the practice of professions and protects from incompetent healthcare practitioners.
Quality of Care	NO	HPA	Health Personnel Act	1999	Defines safety for patients and quality within the health service as well as trust in both health personnel and the health service
Security Standard	International	ISO 27001	ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements	2005	Formal set of specifications against which organizations may seek independent certification of their information security management system.
Security Standard	International	IEC 27002	ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management	2005	Defines good practice for information security.
Security Standard	NL	NEN7510	Netherlands Norm for information security in the health care sector.	2004-2011	Related to IEC 27002. Provides a practical reference security framework for the healthcare sector.
Security Standards	NO	Normen	Code of Conduct for information security in the healthcare, care, and social services sector	2010	Provides a practical reference security framework for the healthcare sector.
Good clinical practice	International	DOH	The Declaration of Helsinki	1964-2008	Defines ethical principles regarding human experimentation.
Good clinical practice	International	ICH-GCP	ICH	1996	International quality standards for clinical trials.

Theme	Scope	ShortName	Full name	Year	Summary
Good clinical practice	EU	The Clinical Trials Directive	Directive 2001/20/EC of the European Parliament and the Council relating to implementation of good clinical practice in the conduct of clinical trials on medicinal aid for human use	2001/2003/2004	Regulates medical research involving humans.
Good clinical practice	EU	GCPD	The Good Clinical Practice Directive 2005/28/EC	2005	Regulates medical research involving humans.
Good clinical practice	NL	WMO	Wet Medisch-wetenschappelijk onderzoek met Mensen (Medical Research involving Human Subjects Act)	2012	Regulates research involving humans.
User interface	International	ISO 14915	Software ergonomics for multimedia user interfaces	2002	Establishes design principles for multimedia user interfaces and provides a framework for handling the different considerations involved in their design.
User interface	International	ISO/IEC 18021	Information technology -- User interfaces for mobile tools for management of database communications in a client-server model	2007	Defines user interface functions for management of database communication of an MBT client capable of interchanging data with an MBT server.
Health informatics	International	ISO IEEE 11073	CEN ISO/IEEE 11073 Health informatics - Medical / health device communication standards	2004	Defines standards for medical device connectivity.

9 Appendix 2: Eurorec Seal Level 1 Criteria

#	Criterium
1	Each version of a health item has a date and time of registration.
2	Each version of a health item has a user responsible for the effective data entry identified.
3	Each update of a health item results in a new version of that health item.
4	Each version of a health item has a status of activity, e.g. active or current, inactive, history or past, completed, discontinued, archived.
5	Deletion of a health item results in a new version of that health item with a status "deleted".
6	Each version of a health item has a person responsible for the content of that version. The person responsible for the content can be a user or a third party.
7	A complete history of the versions of a health item can be presented.
8	Each version of a health item has a date of validity.
9	The system enables the user to designate individual health items as confidential.
10	The system makes confidential information only accessible by appropriately authorised users.
11	Each health item is uniquely and persistently associated with an identified patient.
12	The system enables to assign different access rights to a health item (read, write,...) considering the degree of confidentiality.
13	All patient data can be accessed directly from the patient record.
14	Each patient and its EHR is uniquely and persistently identified within the system.
15	The system takes the access rights into account when granting access to health items, considering the role of the care provider towards the patient.
16	The system offers to all the users nationally approved coding lists to assist the structured and coded registration of health items.
17	Data entry is only done once. Entered health items are available everywhere required.
18	The pick lists and reference tables offered by the system are the same for all the users of the same application.
19	The system does not display deleted health items, audit logs excepted.
20	The system does not include deleted health items in clinical documentation or export, for audit purposes excepted.