Chapter 12
Are mHealth Apps Safe? The Intended Purpose Rule, Its Shortcomings and the Regulatory Options Under the EU Medical Device Framework

Eugenio Mantovani and Pedro Cristobal Bocos

Abstract This chapter discusses the legality of operating commercially available applications or 'apps' for medical purposes in Europe. The meticulous certification process established in the Medical Device Directive (MDD) is seldom applied to mHealth apps. This is due to the application of the concept of "intended purpose", which allows app developers to create apps that are analogous to medical devices (i.e. having similar functions) but, because they have not been intended by their manufacturers to attain a medical purpose, they do not need to satisfy the stringent safety checks foreseen in the MDD. The chapter highlights two vulnerabilities of this regulatory framework, concerning the reliability of the apps and the traceability of "bad apps". In response to these concerns, the EU has taken a mixed approach-combining top down regulation with stakeholders' participation and "self-assessment". A comparison with the regulation of borderline apps in the United States allows the authors to make a recommendation for future research and policies concerning mHealth apps in Europe.

This chapter discusses the legality of operating commercially available applications or "apps" for medical purposes. This chapter observes how the meticulous certification process established in the Medical Device Directive (MDD) is seldom applied to mHealth apps. This is the result of the application of the concept of "intended purpose". This concept allows app developers to create apps that analogous to medical devices (i.e. having similar functions), but, because they have not been intended by their manufacturers to attain a medical purpose, they do not need to satisfy the stringent safety checks foreseen in the MDD. With the aid of concrete examples, this chapter highlights two gaps in the regulation of mHealth apps, concerning the

E. Mantovani (✉) • P.C. Bocos
LSTS – VUB, Brussels, Belgium
e-mail: emantova@vub.ac.be

© Springer International Publishing AG 2017

H.R. Marston et al. (eds.), *Mobile e-Health*, Human–Computer Interaction Series,
DOI 10.1007/978-3-319-60672-9_12

reliability of the apps and the traceability of "bad apps". In response to these concerns, the EU has taken a mixed approach combining top-down regulation with stakeholders' participation and "self-assessment". A comparison with the regulation of borderline apps in the USA allows the authors to make a recommendation for future research and policies concerning mHealth apps.

12.1 Introduction

Mobile health technologies (MHTs or mHealth) are extending beyond the precincts of hospitals and health-care services into a growing market of applications (apps) for well-being or lifestyle. There are today over 100,000 mHealth apps available on the market that work in combination with smartphones, tablets, and wearables (European Commission 2016a).

As with any technological development, mHealth is laden with uncertainties, ambiguities, and interpretative flexibility in terms of meanings, values, and cognitive frames associated with artefacts (Bijker 2010, p. 68). Regulation, which we take as "the intentional activity of attempting to control, order or influence the behaviour of others" (Black 2002, p. 1), is one of the elements influencing this interpretative flexibility. This holds particularly true for safety regulations, which put constraints on developers of mHealth apps.

In Europe, the centrepiece legislation with regard to the safety of medical devices is the Medical Device Directive (MDD). This directive, part of the medical device framework (MDF), amended in 2007, and currently undergoing a general revision, explicitly includes in its scope software that works in combination with mobile devices, known as "applications" or "apps".

Increasingly many mHealth apps that are presently commercially available are, in fact, not considered as medical devices (Medical Device and Diagnosis Industry 2015), but are introduced into the market as simple software. As such, the safety of several mHealth apps available in the EU today is gaged against the general requirements for information society services, and not against the more stringent, as we will see, requirements for medical devices. This chapter puts into question this state of affairs.

Section one provides a definition of mHealth and, with the aid of a scenario, highlights the importance of guaranteeing the safety of mHealth apps. Section two describes the legislative framework, pausing on the definition of medical device, the "intended purpose" rule, the essential requirements that app developers need fulfil, and the control and supervisory mechanisms that are in place. Recognising that many mHealth apps enter the market without going through the safety checks of the MDD, section three discusses two problems: the reliability of apps and the traceability of "bad" apps. Section four pauses on the EU regulatory initiatives adopted to address the vulnerabilities of the so-called borderline apps. Eventually, section five looks at relevant aspects of the US system that departs from the EU.

12.1.1 Navigating Daily Life with Safe mHealth Apps

The International Telecommunication Union (ITU) defines mHealth as "all available services for delivering care or medical information using mobile equipment and networks" (International Telecommunications Union 2014). For the European Commission, the term refers to "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices"(European Commission 2014a, p. 3).

From a technical point of view, mHealth "apps" are software programs that run on mobile devices (hardware) such as smartphones, tablets, smartwatches (Huckvale et al. 2015). These pieces of software process data collected by sensors, such as accelerometers, gyroscopes, ambient light sensors, GPS, cameras, and multitouch screen, which are embedded in the (hardware) mobile devices. The flexibility offered by a smart device allows applications (software) to collect and process information for an astonishing range of purposes (Article 29 Data Protection Working Party 2013, p. 2).

A non-exhaustive list of mHealth apps include apps for patient and carer decision aids, such as the "Chronic Obstructive Pulmonary Disease (COPD) – NHS Decision Aid" app that helps people make a decision about treatment choices (Google Play 2013); apps for self-management, such as the "Self-help for Anxiety Management" app, which offers a range of self-help methods to manage anxiety (Itunes 2015); apps for treatment recommendation, such as the "Micromedex" app, which delivers proper drug dosage and medicine recommendations (DigitalTrends 2016); apps for monitoring, accessing, and editing electronic health records such as the "MyChart" app, which provides access to medical records "through the phone at any time" (DigitalTrends 2016); communication apps such as "Telemed", which enable patients to send images of their skin, eyes, or body (Google Play 2016); the "UpToDate" app, which "tracks medical advancements and news" (DigitalTrends 2016), and so on and so forth.

The uptake of mHealth has been dramatic in the last years. In the USA, a third of physicians say they have recommended an app to a patient (IHS Report 2013); 7 in 10 U.S. adults admit to routinely using one or more health tracking apps (Pew Research 2013). In Europe, the European Commission estimates that over 100,000 mHealth apps are currently available on the market (European Commission 2016a). Of these, approximately 70% target the wellness and fitness sectors, and 30% of apps are specifically designed for health professionals (Deloitte 2012).

It is not only the quantity of mHealth apps that has attracted attention. Mobile health, it has been said, has captured our collective imagination (Cortez 2014). Observers argue that mobile health technologies will "revolutionise" the way we deliver, consume, measure, and pay for health care (Prainsack 2014; Hanlon and Thiel 2016; Cortez 2014). In literature, while some authors discuss the impact on health-care services and systems, others focus on how technology meddles with ordinary, routine life.

In the first chapter of her recent book, legal scholar Mireille Hildebrandt depicts in a scenario the life of a young mother, rampant professional, Diana, and of her frail old father, Jacob. Both navigate their day accompanied by a personal digital assistant (PDAs) (Hildebrandt 2015). The mobile device of old, frail Jacob (in the book the PDA is embodied in a robot) is programmed to:

> Exchange information with similar devices from the same service provider, and with a number of healthcare service providers […]: Jacob's family doctor, the medical specialists who treat his various conditions, the insurance that covers the cost, the pharmacies that supply his medications, and the local nursing centre that provides him with hands-on medical care. (Hildebrandt 2015, p. 6)

Jacob's PDA is able to detect a serious harm from a mild symptom that is, statistically speaking, to be expected. The application that runs on Jacob's device has been designed to set off an alarm only in case a certain condition threshold is crossed. Interestingly, Hildebrandt imagines that the decision of the PDA as to whether or not to send out an alert depends on the input that is provided by another app running on the PDA. This other app has been designed to learn about old Jacob's vision of the world, values, and, given his advanced age, his attitudes towards end of life decisions. In the scenario, the PDA detects an anomaly in Jacob's biometric parameters but, based on previous preferences, decides not to alert him or anyone else. Three days later Jacob dies of a stroke.

As Hildebrandt points out, the scenario is not farfetched. Mobile technologies are already allowed to make invisible inferences of risks and preferences (e.g. playing the right tune for the morning jog, suggesting what to eat, and when to train) or make choices on our behalf (e.g. respecting our values and don't disturb me decisions). The story of Jacob suggests several ethical, societal, and legal questions that are emerging around mHealth: the impact on patients' autonomy, the boundaries of private life and family life, the responsibility of carers, the confidentiality of medical records, the right to be and not to be informed, etc. (Prainsack 2014).

This contribution departs from the sobering recognition that the scenario portrayed above may never see the light, mHealth apps stop being downloaded and sold, if the technology is not safe enough (European Commission 2014b). Take Jacob's mobile device: Will the app send an alarm off when the agreed threshold is reached? Is the software assessing Jacob's value accurately? What happens in the case of conflict between two opposed courses of action, e.g. alert the relatives or not? In the EU, the decision as to whether apps for mobile phones are safe to be used and marketed depends on a certification system regulated by the EU medical device framework. Given that Jacob's and most mHealth scenarios are likely to employ medical software, this framework is of cardinal importance.

12.1.2 Safety of mHealth Apps in the EU Medical Device Legal Framework

12.1.2.1 Introduction

In Europe, the organisation of health care is firmly in the hands of the Member States. After the Maastricht Treaty of 1992, however, the EU introduced a medical device framework (MDF) laying down common rules for the safety of medical devices produced and commercialised in the internal market. The 2009 Treaty of the Functioning of the EU (TFEU) recognises this EU's exclusive competence, sanctioning it in competence to legislate in "high standards of quality and safety for medicinal products and devices for medical use" (European Union 2012, p. 122).

The MDF, which is currently undergoing a process of reform (European Commission 2012a), consists of three directives: the Medical Devices Directive (MDD) 93/42/EEC (European Communities 1993), amended in 2007 by Directive 2007/47/EC (European Union 2007), the Active Implantable Medical Devices Directive (AIMD) 90/385/EEC (European Communities 1990), and the In Vitro Diagnostic Medical Devices Directive (IVDMD) 98/79/EEC (European Communities 1998).

While the AIMD and the IVDMD apply to specific technologies, the MDD is applicable to most medical devices, including software (Callens 2010). Because of the main theme of this chapter, only the MDD is considered. In this chapter, the expressions "MDF" and "MDD" are used exchangeably to refer to the framework described below.

12.1.2.2 The Legislative Framework

Directive 93/42/EEC, the Medical Device Directive (MDD), harmonises national provisions for the safety and health protection of patients, users, and other persons with regard to the use of medical devices. The MDD covers medical devices, from simple bandages, sticking plasters to sophisticated equipment and information technology tools. The legislative regime introduces a classification schemes geared on the risks that a device poses to the human body. The directive puts developers under the obligation to respect a series of essential requirements and documentary procedures. National bodies verify this process.

Importantly for mHealth, a series of guidelines complement the MDD clarifying some of the obscurities of the directive and its implementation. The European Commission's MEDDEV guidelines (medical devices guidance documents) (last amendment 2016b) and the guidelines on assessment of the reliability of mobile health applications (2016c) are of particular relevance for the regulation of mHealth apps and will be broached below.

12.1.2.3 Definition of Medical Device

The basic idea behind the MDD is that all computer programs that meet the definition of a medical device must comply with the MDD (Callens 2010). According to article 1, point 2, letter a, of Directive 93/42/EEC a medical device is:

> 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 its manufacturer.

for a number of defined purposes, including "diagnosis, prevention, monitoring, treatment or alleviation of disease" (European Communities 1993, p. 5). As clarified in recital 6 of Directive 2007/47/EC, which amends Directive 93/42/EEC, such a definition includes software:

> 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. (European Union 2007, p. 1)

12.1.2.4 Essential Requirements

Before being allowed to circulate freely in the EU internal market, article 3 of the MDD states, "all devices must meet a series of 'Essential Requirements'" (European Communities 1993, p. 9). These requirements are found in Annex I of the directive. They range from general prescriptions, such as "eliminate or reduce risks as far as possible" (European Communities 1993, p. 25), to more specific, technical, organisational, informational, ergonomic, and requirements. The following list is a non-exhaustive list but purposefully offered to give an idea of the multifaceted safety issues that (may) appear on the medical device developers' list. They include the choice of materials; issues of flammability; design, manufacture, and packaging; risks connected with environmental conditions such as magnetic fields, pressure, temperature or variations in pressure; interference with other devices; obsolescence of materials; loss of accuracy of any measuring or control mechanism; physical resistance, stability and moving parts, vibrations, noise, heat from accessible parts of the device; sufficient levels of accuracy and stability; device's accuracy as stated by the manufacturer; measurement, monitoring, and display scales; and the respect of ergonomic principles taking account of the device's intended use, etc.

Importantly, these requirements are said "essential" because they apply to all medical devices, although the assessment of the conformity may differ, depending on the risk class apps belong to (European Communities 1993, pp. 25–32).

12.1.2.5 Classification

Article 9 of the directive introduces a classification system based on an estimation of the risk posed by a device to the human body and health (European Communities 1993, p. 12). There are four risk classes: Low – I, IIa, IIb, III – and High. A set of criteria, which are listed in Annex IX of Directive 93/42/EEC, determines to which class devices belong. These criteria, for example, "duration of contact with the body" or "degree of invasiveness", enable manufacturers to anticipate the risk class to which their device belongs, and therefore the type of conformity assessment that is required (European Communities 1993, pp. 52–56).

Any mHealth app, which relies on an external energy source in order to function, is considered as "active medical devices". Active medical devices can pertain to different risk classes. For example, devices intended to allow direct diagnosis or monitoring of vital physiological processes pertain to Class IIa; devices intended for monitoring vital physiological parameters, but "where the nature of variations is such that it could result in immediate danger to the patient" (European Communities 1993, p. 55), say, devices measuring variations in cardiac performance, pertain to Class IIb.

In practice, however, it is not always easy to clarify when a given product is a medical device, in the first place. Secondly, it is not easy to determine the class. The expression "borderline technologies" (European Commission 2011, p. 5) has been coined to refer precisely to cases where it is unclear whether a product falls within the definition of a medical device and to which class of risk. The aforementioned "guidelines" provide practical advice to manufacturers, organisations, public authorities, and users to determine when a software falls under the definition of a medical device.

12.1.2.6 Conformity Assessment

As mentioned earlier, essential requirements apply to all medical devices; however, not all devices are "treated" in the same way. As it is stated in article 11 of the MDD, the risk class determines the type of conformity assessment a device must be subjected to (European Communities 1993, pp. 7–8). This means, in clear, a graduated system of control, which corresponds to the level of potential hazard inherent in the type of device concerned. Once again, the following lines are provided to illustrate the detailed assessment a medical app should undergo, if it were considered medical device.

For example, manufacturers of low-risk Class I devices are only obliged to write a statement to declare that the medical device complies with the requirements in the MDD. Manufacturers then need to apply to a notified body to approve and certify the parts of the manufacturing process that include a function (European Communities 1993, p. 8). Manufacturers of high-risk Class III devices must carry out either an annex II audit of the full quality assurance system, including a design dossier examination or an annex III type examination plus one examination and testing

of each product or homogenous batch of products (Annex IV of the MDD), or one audit of the production quality assurance system (Annex V of the MDD) or an audit of final inspection and testing (Annex VI of the MDD) (European Communities 1993, p. 7). Once the conformity assessment is completed, medical devices can be CE marked (see below) and put into free circulation. Conformity assessment can be a long and costly process.

12.1.2.7 The "CE" Marking

The letters "CE" (from the French "Conformité Européene", meaning "European Conformity") is a declaration informing users that the product bearing it complies with the essential requirements of the relevant European legislation. In line with article 17 of Directive 93/42, devices considered to meet the essential requirements referred to in article 3, mentioned above, must bear the CE marking of conformity when they are placed on the market. The CE marking must appear in visible, legible, and indelible form on the device, on the instructions for use, and, where applicable, on the sales packaging. The CE marking must display the identification number of the notified bodies, introduced below, responsible for its quality assurance. It is prohibited to affix marks or inscriptions that mislead third parties or hide the CE marking (European Communities 1993, pp. 20–21).

12.1.2.8 Notified Bodies, Vigilance System, and the European Database on Medical Devices (EUDAMED)

The first placing on the market of a medical device must involve notification to the competent national authority of the place of residence of the manufacturer. A notified body (NB), established in every Member State (Article 16 of the MDD), carries out the conformity assessment mentioned earlier (European Communities 1993, pp. 19–20). Where a notified body finds that pertinent requirements have not been met or are no longer met by the manufacturer or where a certificate should not have been issued, it will suspend or withdraw the certificate or place restrictions. These bodies are under the obligation to inform the Competent National Authority (CNA), such as the "Federal Agency for Medicines and Health Products" in Belgium, of all certificates issued, modified, supplemented, suspended, withdrawn, or refused.

In addition, the MDD envisages a Medical Device Vigilance System. The aim of this system is to reduce the likelihood of reoccurrence of incidents related to the use of a medical device. Adverse incidents are evaluated and information about them disseminated, where appropriate (European Commission 2016a). This serves to prevent repetition of incidents, such as the Poly Implant Prothèse (PIP) breast implant case, reported below, and improve coordination between notified bodies, for instance, via monthly vigilance teleconferences (European Commission 2014b).

The MDD also requires that data about certified "CE" medical devices is stored in a standardised format in a database called the EUDAMED, a central repository

(European Communities 1993, pp. 17–18). EUDAMED contains information about manufacturers and devices, certificates issued or renewed, modified, supplemented, suspended, withdrawn or refused, as well as data obtained in accordance with the vigilance procedure and data on clinical investigations (European Commission 2010). Its purpose is to provide national competent authorities with fast access to relevant information (European Commission 2012b).

12.1.2.9 The Applicability of Medical Device Law to mHealth Apps: The Intended Purpose Rule

Most mHealth apps engage the literal definition of medical device, provided above. Despite this, they are not considered as medical devices. Therefore the essential requirements and the conformity assessment procedures outlined above do not apply to them. The 2016 Commission guidelines' document, discussed below, states: "those apps that are on the *borderline* and could fall under the medical device definition *could be aligned* with the medical devices requirements as far as possible" (European Commission 2016b, p. 7, our emphasis).

The reason why most mHealth apps escape the purview of the MDD is that the manufacturer, or developer, developed them without an intended medical purpose. In clear, only if the intended purpose of the app is medical, the Medical Device Directive applies. "Intended purpose" indicates 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" (European Communities 1993, p. 7). The European Court of Justice has confirmed the centrality of the intended purpose rule in a case concerning a computer program recording brain activity, called "ActiveTwo" by BioSemi VOF (European Court of Justice 2012).

The case originated when a competitor of BioSemi VOF, Brain Products, argued that "ActiveTwo" could not be allowed to circulate freely, as it was not marketed as a medical device. The Court disagreed, explaining that a medical device must satisfy the essential requirements of the directive and bear the CE marking, only if its manufacturer expressly intends to market it for medical purposes. In contrast, a device that de facto performs an activity that squarely falls within the letter of the definition – such as, in the case at hand, recording brain activity – but is not intended to be used for medical purposes by its manufacturer is not a medical device. Accordingly, the safety certification as a medical device cannot be required (European Court of Justice 2012).

The Court decision clarified that, in order to determine whether a software is a medical device or not, the main criterion is the intended purpose. This criterion is more important than the risk that the device per se can pose to human health, which characterise the US approach and upon which we will return in the conclusion. The initial, basic idea behind the MDD evoked earlier, namely, that all computer programs that meet the definition of a medical device must comply with the MDF's requirements, appears, in fact, as "all computer programs intended by its manufacturers to be medical devices must comply with the MDD". The foregoing means

that mHealth apps may not be "as safe". As will be noted below, this situation is unsatisfactory because "people are actually using this stuff and thinking it's real" (Wired, 2014).

12.1.3 Two Gaps of the MDD in Relation to mHealth Apps

12.1.3.1 Reliability of Apps

In 2015, the European Commission organised a series of stakeholders' meetings about the safety risks posed by mHealth apps. The gatherings identified three areas of risk and needs:

1. The need to ensure that mobile health applications function based on sound clinical evidence
2. The need to provide users with reliable and transparent information about the purpose and functionalities of the apps
3. The need for testing the performance of the apps with different devices (European Commission 2016c)

12.1.3.2 Clinical Evidence

Clinical evidence refers to the scientific credibility of an application, which is generated through validation "by […] specialized professionals, health organization and scientific society" (European Commission 2016c, p. 12). Scientific evidence includes information regarding studies and researches that have been used to withstand it, including clinical evidence, information about the authors and of any conflicts of interest (European Commission 2016c, p. 12). An example of an mHealth app lacking clinical evidence is the "Instant Blood Pressure" app, reported by technological magazine Wired (Wired 2014). The app claimed to be working on strong clinical evidence as its manufacturers claimed that the app "use[d] a patent-pending process developed by a team from the Johns Hopkins University—a world leader in health innovation" (Ibid. 2014). In fact, any clinical evidence supported the app, and the John Hopkins University had not participated in its development (Ibid. 2014).

12.1.3.3 Claims on the Purpose and Functions of mHealth Apps

Clarity and transparency about the purposes and functionalities of apps are essential to enable users, doctors, and patients alike to purchase the "right" app. What an app does can be communicated in the logo, in the instructions, in the labelling, or in any form of communication designed to promote directly or indirectly its services (European Commission 2016c, p. 13).

Several cases, such as the one shown below, suggest there is a lack of transparency on the part of developers when they explain the capabilities of their products. The latter is justified on the ground that an app with an advertised pseudo-medical purpose attracts consumers more than normal apps. For this reason, the indication that the app is not intended to serve a medical purpose is not advertised clearly but specified only in the instructions, which consumers seldom read before purchasing an app. For example, the Instant Blood Pressure app claimed it could take a "blood pressure reading in under a minute using only your iPhone—no cuff required" (Wired 2014). It is only by scrolling down in the app store description that one could find a warning stating that this technology was for "recreational use".

Reportedly (Wired 2014), this notice arguably did not discourage users. The reviews left at the bottom of the app store web page clearly indicate that some users downloaded and used the app believing that they were getting accurate blood pressure measurements from it. In 2013 a group of researchers from the University of Pittsburgh Medical Center screened the catalogue of the default app stores of IOS and Android, searching for apps that claimed to be able to detect skin cancer or to assist users in detecting malignant skin lesions (Wolf et al. 2013). In four cases, apps were described in the instructions as intended for educational purposes and not cancer diagnosis. Despite the obvious medical relevance, the instructions merely warned users not to use them to replace standard medical care (Wolf et al. 2013). As mentioned earlier, "people are using this stuff and thinking it's real" (Wired 2014).

12.1.3.4 Test and Validation of Performance

The performance of a device relates to the accuracy of technology features and components, such as buttons, menus, resistance over time, after prolonged use, etc. (European Commission 2016b, p. 43).

There are general and specific problems related to the testing and validation of apps. A general problem is that apps, like any software, are "impossible to guarantee [being] error-free" (Forsström 1997, p. 143). In this regard, the best way to minimise errors is to conduct tests with users. However, in the low-cost business model of the apps industry, cost-constrained software development validation means that software often undergoes "minimal testing" (Lurie 2003). This is the case, for example, of the "Instant Blood Pressure" app, presented above. Put to the test after being released on the market, the app first measured a heart rate of 55 beats per minute. Reactivated after two misfires, the app measured a heartbeat of 74 per minute (Wired 2014).

The specific problem relates to the fact that mHealth apps, unlike conventional medical software, are designed to work with a potentially enormous range of generic devices. The MDD requires that the testing of a medical device be performed with all the accessories with which it is to be used (European Communities 1993, p. 6). In other words, the essential requirements must be met by the app, working in combination with the accessory (the mobile device) (European Commission 1994). This

includes software, called "stand-alone software", which is not incorporated into a device at the time of its placing on the market (European Commission 2016d). To come into line with the directive, apps should be tested on every mobile device that can run it. In addition, given the versatility of operating systems such as Android, such apps may well be capable of being run on phones that did not even exist when the app in question was created. This apparent impossibility to test the medical device with all available accessories poses unknown safety issues (Quinn 2013).

12.1.3.5 Traceability of mHealth Apps

The other safety issue highlighted in EU-sponsored stakeholders' meetings concerns the possibility of retrieving defective apps from users. In general, the recall of products is exercised when a device is defective, poses a risk to health, or both, for example, a critical bug in a software. Launching a recall procedure can be a legal obligation. It is found in community legislation on medicinal products (European Union 2001, p. 72; European Union 2003, p. 25). Under these directives, manufacturers must implement a system for recording and reviewing complaints, together with an effective system for recalling promptly and at any time (investigational) medicinal products, which have already entered the distribution network.

Recall is also foreseen under the MDD. In Annex IV, the MDD obliges manufacturers to implement "any necessary corrective action", including the recall of devices (European Communities 1993, pp. 40–41). Annex VII of the same piece of legislation requires manufacturers to notify the competent authorities of "any technical or medical reason […] leading to systematic recall of devices of the same type by the manufacturer" (European Communities 1993, pp. 48–49).

A case in which medical devices had to be recalled occurred in 2009, after some French surgeons began reporting an abnormally high rupture rate of breast implants produced by a company called Poly Implant Prothèse (PIP). Some months later the French medical safety agency (AFSSAPS) issued a recall of PIP implants when it found out that company was substituting unapproved silicone in place of approved medical-grade silicone (Keogh 2012). The French government later recommended the removal of PIP implants and announced that the 30,000 French women who received PIP implants were entitled to have them removed at no cost (Chrisafis 2011).

The PIP case concerns a traditional, material, medical device. In the specific context of mobile health apps, however, it may not be easy to implement a recall procedure. The reason for this is that it is difficult to trace the different channels through which an app without a CE mark can be distributed. An app that is not a medical device can be downloaded from app stores or directly from the Internet. A manufacturer may contact the app stores to retrace those who downloaded the app and contact them (Article 29 Data Protection Working Party 2013, pp. 20–21). But in case a defective app has not been downloaded from official channels, for instance, from a privately owned website, tracing the user concerned is more difficult. This

holds true in particular for apps that, once they are downloaded, work autonomously, i.e. without the need to stay connected to the Internet. In this case, it is only the owner of the mobile device that can uninstall the defective app. To do so, he or she must be told, as the example below shows.

In April 2011, the multinational pharmaceutical company Pfizer Inc. released a "Rheumatology Calculator" app. This app was not a CE-marked medical device and, once downloaded, could work offline. The app was a calculator, as its functionality was to help physicians to "measure the disease activity of patients with various inflammatory diseases, in particular that of patients with rheumatoid arthritis" (Pfizer 2011). The Pfizer app, more specifically, used an algorithm to measure specific markers of disease activities of patients based on data provided by their doctors.

In October 2011, the app disappeared from the app stores, and Pfizer informed the British and the Swiss competent authorities that it had found a bug in the software. Pfizer also sent a letter to many doctors based in the UK informing them that:

> "a bug in the app […] gives wrong results", and that "if you have downloaded the "Pfizer Rheumatology Calculator" application to your mobile device, the application should not be used any longer and should be deleted from the device". (Ibid, 2011)

It is not clear how many doctors Pfizer tried to contact. It is not equally clear why the company decided to send the letter only to British doctors (Ibid, 2011). More worryingly, it is unknown whether there are doctors out there who, not having being informed, are still using the calculator in their daily work.

12.1.3.6 Regulatory Initiatives to Address the Safety Needs of mHealth Apps

European authorities have been hesitant to impose the requirements of the MDD on apps (Quinn 2013). The reason for this is that stricter enforcement of the MDD may stifle an area of ongoing innovation and potential growth (European Commission 2012a). Given the costs involved with MDD compliance, a more rigorous application of the MDD would likely mean an increase in the cost of such applications beyond a level which may be feasible for a low-cost business model.

However, recently, the EU has grown aware that the safety concern is a barrier to the very uptake of mHealth. In 2016, the European Commission launched a guidelines document to ensure "a consistently high level of health and safety protection for EU citizens using mHealth apps" in which the reliability and transparency needs discussed earlier are cautiously addressed (European Commission 2016c). In response to the specific problem of traceability, no specific initiative has been adopted. However, the newly proposed Medical Device Regulation (European Commission 2012a) introduces a unique device identifier (UDI) system that may be used to mitigate that problem (see below page 12).

12.1.3.7 The EU Guidelines on the Assessment of the Reliability of Mobile Health Applications

In 2016, the European Commission adopted the first draft of the "EU guidelines on assessment of the reliability of mobile health applications". The EU guidelines, which are not legally binding, deal with the grey zone of "borderline" mHealth apps (European Commission 2016c, p. 4). Drafted by a private consultancy contracted by the Commission, the "EU guidelines" contain an assessment procedure that takes the form of a series of precise questions.

The EU guidelines document is structured in three sections, one for each of the three stages of the assessment process. Each step consists of a series of questions addressed to app developers, citizens, health professionals, and health providers alike.

The first step is concerned with the identification of the app, to discover if it exists, if it is appropriate for the evaluation, whether it is downloadable (Ibid., pp. 8–9), its name, the supplier and the developer (in the case that they are not the same), and the intended use declared by the manufacturer. In the case that the app is "CE" marked, there is no need to carry out an assessment (Ibid., p. 8). If not, mHealth apps must undergo a simple testing, which consists of installing and uninstalling the app on available platforms and verifying whether the app is easy to understand, easy to navigate, and if it works as stated (Ibid, p. 9).

In the second step, "risk assessment", the information gathered about the app is used to rank the clinical and technological risk. Depending on its specificities, each app will be ranked differently; this ranking, in turn, determines the level of "scrutiny" the app should be submitted to (see below third phase "scrutiny"). This stage, in other words, helps stakeholders to clarify the appropriate level of conformity assessment that the app they have in mind "may" undergo.

In the third phase, called "scrutiny", a series of questions about the technological and the medical aspects of the app are asked (Ibid., pp. 11–15). As far as the problem of clinical evidence is concerned, the guidelines dedicate seven questions to assess the credibility of the app. These questions include: "Does the app provide references to the scientific evidence used to ensure content quality?" "Is there appropriate information provided about the authors of the app content to generate credibility and provide quality assurance?" "Does it indicate how often the app's content is reviewed/updated?" "Does it indicate the last review date?" "Does it notify changes/modifications made at the last update?" (Ibid., p. 12).

As far as the transparency about the claims of the app, the EU guidelines recommend, as first step, to give a face to the app, that is, who are those developing and introducing the app in the market. Moreover, the guidelines urge more clarity about the intended purpose of the app. Users should be able to understand right away what the app can do and what it cannot do. The detailed questions asked by the guidelines complement the transparency obligations that already exist under community law. The eCommerce Directive 2000/31/EC and Directive 2011/83/EC, the Directive on Consumer Rights, impose on manufacturers a series of obligations intended to ensure that consumers who purchase an app "at the distance" are informed in

transparent and clear fashion (European Union 2000; European Union 2011). Furthermore, Directive 2005/29/EC on Unfair Commercial Practices sanctions unfair commercial practices. On the account of the directive, a commercial practice is unfair if it does not comply with the principle of professional diligence, if it is likely to distort the economic behaviour of the average consumer, and if it is misleading or aggressive (European Union 2005, p. 28).

As per the problem of testing the performance of the app with the different devices, the guidelines propose to involve and, more specifically, to encourage users to test the apps "in every platform" (European Commission 2016b, p. 11).

12.1.3.8 The Unique Device Identifier

In 2013 the Commission acknowledged in a recommendation that the "traceability of medical devices throughout the whole supply chain contributes to patient safety by facilitating vigilance, market surveillance and transparency in this sector" (European Commission 2013, p. 1). In that same text, the Commission advocated for a unique device identification system of medical devices in the EU (Ibid., p. 1). The proposed reform of the MDF, the draft Medical Device Regulation (MDR), introduces a unique device identification (UDI) mechanism.

The Unique Device Identification (UDI) is a unique numeric or alphanumeric code that pertains to any medical device. Such a unique numeric or alphanumeric is composed of two parts, a device identifier and a production identifier. By combining these identifiers, the UDI is expected to improve the traceability of devices and allow for easier recall of devices, as well as for combatting counterfeiting. The UDI will not replace but add to the existing labelling requirements of the Medical Device Directive (European Commission 2016a).

In the intention of the Commission, Eudamed is expected to take a more important role under the new regulation, improving the capacity of medical authorities to trace devices through the supply chain and to facilitate the prompt and efficient recall of "bad", unsafe, devices from the market and from consumers' hands.

12.1.3.9 A Brief Look into the US Legislative Framework for "Borderline" mHealth Apps

The US approach to regulating mHealth apps display similarities and some differences from the European Union's. This section presents the US legal framework on medical devices, focusing on what interests this chapter, the regulation of "borderline" mHealth apps.

The centrepiece legislation for the safety for medical devices in the USA is the Federal Food, Drug, and Cosmetic Act (FD&C Act) of 1938 (United States Congress 1938). The Medical Device Amendment of 1976 introduced in the FD&C criteria and norms for the classification and regulation of medical devices. The same amendment entrusted to a federal authority, the Food and Drugs Administration (FDA), the

role of ensuring that a "reasonable assurance of safety and effectiveness" is provided before medical devices are marketed and, importantly, the power to investigate and discontinue the commercialisation of apps that are deemed to pose a serious risk to the health and safety of users/patients (United States Congress 1976).

In the last few years, like in the European Union, the FDA has issued guidelines to clarify the application of medical device law to mHealth apps. As in Europe, these "guidance documents" do not establish legally enforceable responsibilities but contain non-binding recommendations. The most relevant instruments, for our purposes, include:

(a) The *Mobile Medical Applications Guidance* of 2013, subsequently amended in 2015, which seeks to provide clarity and predictability for manufacturers of mobile medical apps (US Food and Drugs Administration 2013a; US Food and Drugs Administration 2015a)
(b) The *Medical Device Data Systems*, *Medical Image Storage Devices*, *and Medical Image Communications Devices* of 2015, which covers devices used to collect and store data from other medical devices (US Food and Drugs Administration 2015b)
(c) The *Medical Device Accessories*: *Defining Accessories and Classification Pathway for New Accessory Types Guidance* of 2016, which deals with accessories to medical devices (US Food and Drugs Administration 2016a)
(d) The *General Wellness*: *Policy for Low-Risk Devices Draft Guidance of 2016*, which deals with low-risk products that promote healthy lifestyle or general wellness products, such as fitness trackers, calorie trackers, or lifestyle trackers (US Food and Drugs Administration 2016b)

The definition of medical device introduced in the FD&C Act is similar to the one adopted in the EU. Section 201(h) of FD&C Act considers a medical device "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory" (United States Congress 1938, p. 5). In contrast to the European MDD, in order to determine whether a device is a medical one, the US legislator appeals to the "intended use" criterion. A device is medical if it is:

> Intended for use in the diagnosis of disease or other conditions, or […]; or intended to affect the structure or any function of the body of man or other animals […]. (United States Congress 1938, p. 5)

The intended use may be shown by oral or written statements (by manufacturers or their representatives) or by labelling claims or by advertising materials (United States Congress 1938, pp. 322–329). As discussed earlier, in the EU MDD, the criterion is the "purpose", "intended by the manufacturer" (European Communities 1993, p. 5); in the USA such a specification does not exist. This means that while in Europe a company can avoid compliance with the medical device legislation by disavowing an app's medical purpose, in the USA "when it is clear that the app serves as a medical device, such disavowals are ineffective" (McFarlane 2014, p. 3).

The case of 23andME, discussed below, illustrates the practical implications of this provision.

The similarities and differences between the USA and the EU do not stop here. Similar to the European MDD, the US FD&C Act organises medical devices into classes (United States Congress 1938, pp. 191–200). While in Europe there are four classes, US legislation provides for three classes: "low-risk" Class I devices, which are subject only to general controls, such as registering their name and products with the FDA; medium-risk Class II devices, which are expected to meet performance standards and undergo specific controls; and high-risk Class III devices, which must be subjected to a review process, including clinical trials, before they are allowed to be marketed (Kramer et al. 2012). Notwithstanding the difference in the number of classes, the logic behind the classification remains the same, based on prior evaluation of the risks that type of device poses to the health and safety of the patient.

Both the EU and US regulators face the similar challenge of ensuring that borderline apps that are sold in the market are safe (Sorenson and Drummond 2016, pp. 145–150). As discussed earlier, the EU legislator asks manufacturers of borderline apps to abide by "as close as possible" to the requirements of the MDD. In contrast, the US FDA refrains from the attempt of bringing borderline apps under the umbrella of the FD&C Act (*US Food and Drugs Administration* 2015c). The FDA reserves to itself the power to intervene if a borderline app is procuring a high risk. In its website, the FDA offers a list of examples of mobile apps that "may be regulated" (*US Food and Drugs Administration* 2016c): apps that transform a mobile platform into a regulated medical device using sensors or by including functionalities similar to those used in other regulated devices, apps that are used for patient monitoring or that analyse data from a connected device, etc. (*US Food and Drugs Administration* 2016c).

Both the EU and the US legislator have put in place vigilance systems. Also in the USA, manufactures of marketed devices are, for instance, under the obligation to report adverse events and to continue monitoring the device's safety and effectiveness (Kramer et al. 2012). The FDA also supports a number of the so-called surveillance data networks, the Medical Device Epidemiology Network Initiative (MDEpiNET) and the Medical Device Surveillance Network (MedSun). These networks conduct systematic collection, collation, and analysis of data to identify safety problems and advance epidemiological research (Fiedler 2016, p. 56). Since 2013, a Unique Device Identification (UDI) system and a central database of medical devices (GUDID) have been in place (*US Food and Drugs Administration* 2013c). The system and the database share similarities with the tasks performed by European notified bodies, for what concerns the post market surveillance, and by EUDAMED, the central database of medical devices, for what concerns surveillance data.

The case of the company "23andMe" offers an example of what we have briefly discussed so far concerning the regulation of borderline apps in the USA. 23andMe is a private company that provides consumers with information about their genetic

heritage, using a sample of their saliva, and against the payment of a price ($99) (23andme 2013).

In 2011, when it started operating, the purpose of 23andMe was to offer a genetic testing service, which provided clients with information about their ancestors. Shortly thereafter, the company launched another service: clients could now obtain genetic information revealing their predisposition to develop certain pathologies or their responsiveness to certain drugs (Brandon 2013). The new service proved extremely successful and profitable. The popularity of the service, however, attracted the attention of the federal authority, the FDA. Few months after, the FDA ordered 23andMe to discontinue the marketing of its genetic diseases predictive services, while it could keep the genealogical services in place. For the FDA, the genetic testing kit posed a serious risk to individuals because (1) it did not provide sufficient information about the reliability of the "predisposition" diagnoses, (2) it did not give advice to consumers about how to navigate the information extracted from the kit, and (3) it provided misleading information, suggesting to users that the test could replace traditional medical diagnosis (*US Food and Drugs Administration* 2013b). Today, 23andMe has obtained the certification of the FDA also for its predictive genetic testing services. However, a warning appears in its website making clear that the tests:

> Are not intended to diagnose a disease, or tell you anything about your risk for developing a disease in the future" and they are "not intended to tell you anything about the health of your fetus, or your newborn child's risk of developing a particular disease later in life. (23andme 2016)

In conclusion, there are not substantial differences between the EU and US approach to borderline medical apps, which are both lenient in imposing the application of the respective medical device frameworks. Under both jurisdictions, regulators have been hesitant to take action that they fear may stifle an area of ongoing innovation. The difference between the EU and the USA is perhaps mostly related to the regulation technique. The European framework tends to be overarching and participative. It seeks to cover all apps, including borderline apps, and promotes stakeholders' self-regulation through self-assessment of their products. In the USA, the legislator is less interested in extending the medical devices rules to borderline apps or in involving stakeholders. Developers are warned that a US federal authority retains the power to intervene at any moment should a borderline app pose serious risks to health.

12.2 Conclusion

This chapter has raised the question of the use of commercially available mHealth apps for medical purposes. To answer the main research question, "are mHealth apps safe?", it has mobilised the EU's Medical Device Framework. This detailed legal system of administrative rules, checks and testing, documentary procedures,

and requirements, amended over the years, does not clearly apply to most mHealth apps. "Borderline" apps that are not intended by their manufacturers to be used for medical purposes do not have to comply with it. This also holds true if they technically meet the definition of a medical device and/or they perform acts on subjects that doctors would consider pertaining to the medical field. The non-applicability of the MDF to borderline mHealth apps implies a general "market clearance" given to de facto medical-connected devices that potentially affect individuals' health, without medical justification.

This situation creates safety problems that, as discussed in this contribution, concern primarily the "reliability" and the "traceability" of "bad" apps. Clinical evidence, claims on the purpose and functions of mHealth apps, procedures for testing and validating of performance, and the traceability of mHealth apps are the issues of major concern. The recent EU guidelines offer general and specific questions to address them by guiding "stakeholders" in the self-assessment of the credibility, the solidity, etc. of the apps and their functionalities. The guidelines closely reflect the MDD. Indeed, after reading the questions, one comes under the impression of being spoon-fed medical device law for non-experts. This is done in the attempt to bring the mHealth apps market "as close as possible" to the medical device framework, as recommended by the EU.

This apparently positive effort can be put into question. In particular, one may raise doubts about the rationale behind the decision of addressing the guidelines not only to manufacturers or developers but to all stakeholders. The point should be emphasised that stakeholders in mHealth carry different points of view (Bijker 2010): they have specific interests and concerns and also constraints that limit what they can actually do. Manufactures will read the guidelines because they need to know whether they have to comply, and with which parts, of the complex medical device framework. Other stakeholders, such as doctors and patients, may very well read the guidelines, but they cannot really make a difference. Their concern is to decide whether or not to use an app, which has already been produced. A more useful guidance is, for example, the Medical App Checker of the Royal Dutch Medical Association (KNMG 2016).

What is worrisome is the proclivity of the EU to include "all stakeholders". This choice is seemingly premised on the assumption if the rules are well explained, "all stakeholders" will be able to self-assess the risks of apps that are about to develop, recommend, purchase, use, etc. In our view, this "pedagogic" approach may create unnecessary confusion; it may, most importantly, dilute the responsibilities of those primarily concerned with the development of safe apps, app developers, or manufacturers.

In an earlier publication (Mantovani et al. 2013, p. 66), one of the authors suggested that we were approaching a fork in the road. In that article, one route led towards a future where mHealth apps are regulated according to the same principles as conventional medical devices; the other route was to continue with the current situation whereby mHealth apps are allowed to avoid the need of complying with medical device regulation. Looking at the most recent legislative initiatives, it seems that mHealth is threading the second route. In this connection, and to mitigate the

risk of diluting the responsibilities of the developers, just evoked, the EU could benefit from two lessons learnt from the regulation of borderline mHealth apps in the USA.

First, while the EU's technique to regulate borderline mHealth apps appears overarching and participative/pedagogical, in the USA the "activity of attempting to control, order or influence" (Black 2002, p. 1, mentioned in the Introduction) the development of mHealth apps could be said "sector specific" and "adversary". It is sector specific because the regulatory frameworks, including the guidelines, address developers of mHealth apps only; it is adversary because a federal authority, the FDA, retains a discretionary power of intervention. Although it exercises its power only in a restricted number of cases, this system boils down to a warning for manufactures that if the use of a device or app poses serious risks to health, the FDA will intervene, forcing the application under the medical device framework, regardless of the intended use that the developer attributed to it (as in the 23andMe case).

In our view, the EU regulation of mHealth apps may consider an expansion of the domain of activity of public authorities in the mHealth safety domain. The EU has a long tradition of creating networks of supervisory bodies, for instance, the data protection authorities (DPAs) under Directive 95/46/EU. To guarantee a high level of health safety in a world of connected devices, the existing independent authorities, at national and/or European level, could be able to receive complaints or notifications by stakeholders concerned with the safety of apps. Legislative change may be required to make rights enforceable, and it may be necessary to adopt an approach similar to that found in the distant selling and consumer directives, i.e. whereby consumers are able to ask questions and obtain genuine information from app developers.

Second, the US authorities accept the situation where one does not know if certain lifestyle and well-being apps pose a risk to citizens' health and to what extent, until they are reported, investigated, and/or accidents occur. It is hard to deny that this statement candidly reflects the reality of uptake of mHealth today, not only in the USA but also in Europe. What is noteworthy is that the formal recognition of this situation in the USA means that if an app poses a risk to health, it will not be enough for an app developer to disavow the medical or pseudo-medical purpose of use. Regardless of the purpose intended by its manufacturer, if an app poses a risk to health, it is stopped and must undergo the medical device standard procedure before being marketed again.

In our view, the EU regulation of mHealth apps could also consider risk assessment, in addition to the "intended purpose" rule, to distinguish between medical and non-medical mHealth apps. Embracing risk assessment would mean opening the doors to independent scientific advice on all aspects relating to safety, communication, and dialogue with consumers, as well as networking with national agencies and scientific bodies. This process may be costly and difficult to realise across different Member States. It may be worth trying. Unchecked medical technology developments have the potential not only to harm the health of individual; they can also engender fears and mistrust in the public, to the detriment of any medical technological innovation.

Acknowledgements The authors acknowledge the support of the IRIS project – Interoperable platform for Remote monitoring and Integrated e-Solutions (Grant agreement Nr. BRGEOZ234), funded by INNOVIRIS, the Brussels Institute for Research & Innovation.

References

Article 29 Data Protection Working Party (2013) Opinion 02/2013 on apps on smart devices. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf. Accessed 21 Dec 2016

Bijker WE (2010) How is technology made?—that is the question! Camb J Econ 34:63–76

Black J (2002) Critical reflections on regulation 27 Australian Journal of Legal Philosophy 1

Brandon R (2013) Body blow: how 23andMe brought down the FDA's wrath. http://www.theverge.com/2013/11/25/5144928/how-23andme-brought-down-fda-wrath-personal-genetics-wojcicki. Accessed 21 Dec 2016

Callens S (2010) The EU legal framework on E-health. In: Mossailos E, Permanand G, Baeten R, Hervey T (eds) Health systems governance in Europe. Cambridge University Press, Cambridge

Chrisafis A (2011) French government "to order women to remove defective breast implants". https://www.theguardian.com/world/2011/dec/20/french-remove-breast-implants-silicone. Accessed 21 Dec 2016

Cortez N (2014) The mobile health revolution? http://lawreview.law.ucdavis.edu/issues/47/4/articles/47-4_cortez.pdf. Accessed 2 Jan 2017

Danzis SD, Pruitt C (2013) Rethinking the FDA's regulation of mobile medical apps. https://www.cov.com/~/media/files/corporate/publications/2013/02/rethinking_the_fdas_regulation_of_mobile_medical_apps.pdf. Accessed 1 Jan 2017

Deloitte (2012) mHealth in an mWorld. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lhsc-mhealth-in-an-mworld-103014.pdf. Accessed 25 Nov 2016

DigitalTrends (2016) Maintain your health and mind with these 15 medical apps. http://www.digitaltrends.com/mobile/best-medical-apps/. Accessed 5 Dec 2016

European Commission (1994) MEDDEV 2.1/2 guidelines rrelating to the application of: the council directive 90/385/EEC on active medical devices and the council directive 93/42 on medical devices. http://ec.europa.eu/consumers/sectors/medical-devices/files/meddev/2_1-2___04-1994_en.pdf. Accessed 21 Dec 2016

European Commission (2010) 2010/227/: Commission Decision of 19 April 2010 on the European Databank on Medical Devices (Eudamed) (notified under document C (2010) 2363) (Text with EEA relevance) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0227&from=en. Accessed 11 Dec 2016

European Commission (2011) Manual on borderline and classification in the community regulatory framework for medical devices. http://ec.europa.eu/consumers/sectors/medical-devices/files/wg_minutes_member_lists/version1_9_borderline_manual_en.pdf. Accessed 21 Dec 2016

European Commission (2012a) 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. http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf. Accessed 15 Oct 2016

European Commission (2012b) Evaluation of the "European databank on medical devices". http://ec.europa.eu/DocsRoom/documents/12981/attachments/1/translations/en/renditions/native. Accessed 21 Dec 2016

European Commission (2013) Commission recommendation on a common framework for a unique device identification system of medical devices in the union text with EEA relevance. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013H0172&from=EN. Accessed 17 Dec 2016

European Commission (2014a) Green paper on mobile health. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147. Accessed 21 Dec 2016

European Commission (2014b) EU consultation on mHealth. https://ec.europa.eu/digital-single-market/en/public-consultation-green-paper-mobile-health. Accessed 5 Dec 2016

European Commission (2016a) Market surveillance and vigilance. Available at: https://ec.europa.eu/growth/sectors/medical-devices/market-surveillance_en. Accessed 1 Nov 2016

European Commission (2016b) MEDDEV 2.1/6 guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices. http://www.twobirds.com/~/media/pdfs/news/articles/2016/firstdraftguidelinesandannexes.pdf?la=en. Accessed 13 Dec 2016

European Commission (2016c) EU guidelines on assessment of the reliability of mobile health applications. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16090. Accessed 13 Dec 2016

European Commission (2016d) Code of conduct on privacy in mHealth. http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125. Accessed 13 Dec 2016

European Communities (1990) Directive 90/385 on the approximation of the laws of the member states relating to active implantable medical devices. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31990L0385&from=EN. Accessed 10 Oct 2016

European Communities (1993) Directive 93/42 concerning medical devices. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:EN:PDF. Accessed 21 Dec 2016

European Communities (1998) Directive 98/79/EC of the European parliament and of the council of 27 October 1998 on in vitro diagnostic medical devices. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31998L0079. Accessed 13 Nov 2016

European Court of Justice (2012) C129/11 Brain Products GmbH v. BioSemi VOF. http://curia.europa.eu/juris/document/document.jsf?docid=130247&doclang=en. Accessed 12 Oct 2016

European Union (2000) Directive 2000/31/EC of the European parliament and of the council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce'). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML. Accessed 16 Nov 2016

European Union (2001) Directive 2001/83/EC of the European parliament and of the council of 6 November 2001 on the community code relating to medicinal products for human use. http://ec.europa.eu/health//sites/health/files/files/eudralex/vol-1/dir_2001_83_consol_2012/dir_2001_83_cons_2012_en.pdf. Accessed 16 Nov 2016

European Union (2003) Commission directive 2003/94/ECof 8 October 2003 laying down the principles and guidelines of good manufacturing practice in respect of medicinal products for human use and investigational medicinal products for human use. http://ec.europa.eu/health//sites/health/files/files/eudralex/vol-1/dir_2003_94/dir_2003_94_en.pdf. Accessed 16 Nov 2016

European Union (2005) Directive 2005/29/EC of the European parliament and of the Council of 11 May 2005concerning unfair business-to-consumer commercial practices in the internal market and amending council directive 84/450/EEC, directives 97/7/EC, 98/27/EC and 2002/65/EC of the European parliament and of the council and regulation (EC) No 2006/2004 of the European parliament and of the council('Unfair Commercial Practices Directive'). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005L0029&from=en. Accessed 16 Nov 2016

European Union (2007) Directive 2007/47/EC of the European parliament and of the council of 5 September 2007 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. http://ec.europa.eu/consumers/sectors/medical-devices/files/revision_docs/2007-47-en_en.pdf. Accessed 17 Nov 2016

European Union (2011) Directive 2011/83/EU of the European parliament and of the council of 25 October 2011on consumer rights, amending council directive 93/13/EEC and Directive 1999/44/EC of the European parliament and of the council and repealing council directive 85/577/EEC and directive 97/7/EC of the European parliament and of the council. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0083&rid=1. Accessed 15 Nov 2016

European Union (2012) Treaty on the functioning of the European union. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN. Accessed 3 Aug 2016

Fiedler BA (2016) Managing medical devices within a regulatory framework. Elsevier, Cambridge, MA

Forsström J (1997) Why certification of medical software would be useful? Int J Med Inform 47(3):143–151

Google Play (2013) COPD – NHS decision aid. https://play.google.com/store/apps/details?id=uk.co.activata.TotallyHealth.condition119. Accessed 5 Dec 2016

Google Play (2016) Telemed. https://play.google.com/store/apps/details?id=com.telemed.ae&hl=es. Accessed 5 Dec 2016

Hanlon B, Thiel S (2016) The mobile health application revolution: tapping its potential. http://www.covance.com/content/dam/covance/assetLibrary/whitepapers/Mobile-Health-Applications-WPCVD002-0816.pdf. Accessed 3 Jan 2017

Hildebrandt M (2015) Smart technologies and the end(s) of law: novel entanglements of law and technology. Edward Elgar Publishing, Cheltenham

Huckvale P, Tilney B, Car (2015) Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Med 13:214

IHS report (2013) The world market for sports & fitness monitors—2013 Edition

International Telecommunications Union (2014) Filling the gap: legal and regulatory challenges of mobile health (mHealth) in Europe. https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/ITU%20mHealth%20Regulatory%20gaps%20Discussion%20Paper%20June2014.pdf. Accessed 21 Dec 2016

Itunes (2015) Self-help for anxiety management. https://itunes.apple.com/us/app/self-help-for-anxiety-management/id666767947?mt=8. Accessed 20 Dec 2016

Keogh B (2012) Poly implant Protheses(PIP) breast implants: interim report of the expert group. http://www.nhs.uk/news/2012/01January/Documents/pip-report.pdf. Accessed 22 Dec 2016

KNMG (2016) Medical app checker: a guide to assessing mobile medical apps http://www.knmg.nl/Over-KNMG/About-KNMG/News-English/152830/Medical-App-Checker-a-Guide-to-assessing-Mobile-Medical-Apps.htm

Kramer DB, Xu S, Kesselheim AS (2012) Regulation of medical devices in the United States and European Union. N Engl J M 366(9):848–855

Lurie J (2003) Error-free software is in reach, but is anyone reaching?. http://www.devx.com/enterprise/Article/16687. Accessed 1 Aug 2016

Mantovani E, Guihen Barry B, Quinn P, Habbig A-K, De Hert P (2013) eHealth to mHealth. A journey precariously dependent upon apps? Eur J ePractice 21:48–66

McFarlane B (2014) FDA regulation ofmobile medical apps. https://www.namsa.com/wp-content/uploads/2015/10/WP-FDA-Regulation-of-Mobile-Medical-Apps-7-7-2014.pdf. Accessed 21 Dec 2016

Medical Device and Diagnosis Industry (2015) Consumer mHealth app or regulated medical device? http://www.mddionline.com/blog/devicetalk/consumer-mhealth-app-or-regulated-medical-device-03-04-15. Accessed on 14 Nov 2016

Pew Research (2013) Tracking for health. Available at http://www.pewinternet.org/2013/01/28/tracking-for-health-2/. Accessed 2 Sept 2017

Pfizer UK (2011) Dear doctor letter: “Pfizer rheumatology calculator” iPhone/android application — important information. Available at: http://www.pharma-mkting.com/images/Pfizer_Rheum_BugLetter.pdf. Accessed 20 July 2016

Prainsack B (2014) The powers of participatory medicine. PLoS Biol 12(4):e1001837

Quinn P (2013) Medical apps and accountability – where can the patient/consumer find protection? European Journal of Health Law. Fourth Conference on European Health Law, Book of Abstracts

Rübsamen K, Sakellariou S (2015) Mobile health apps: are they a regulated medical device?. http://www.whitecase.com/publications/article/mobile-health-apps-are-they-regulated-medical-device. Accessed 1 Jan 2017

Sorenson C, Drummond M (2016) Improving medical device regulation: the United States and Europe in perspective. Milbank Q 92(1):145–150

United States Congress (1938) Federal Food, Drug, and Cosmetic Act. https://www.epw.senate.gov/FDA_001.pdf. Accessed 8 Aug 2016

United States Congress (1976) Medical device amendment. https://www.congress.gov/bill/94th-congress/house-bill/11124. Accessed 8 Aug 2016

US Food and Drugs Administration (2013a) Mobile medical Applications. http://www.gpo.gov/fdsys/pkg/FR-2013-09-25/pdf/2013-23293.pdf. Accessed 6 Dec 2016

US Food and Drugs Administration (2013b) 23andMe, Inc. 11/22/13. Available at: http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2013/ucm376296.htm. Accessed 6 Dec 2016

US Food and Drugs Administration (2013c) Unique device identification system-final rule. http://www.fda.gov/downloads/aboutfd/ucm368961.pdf. Accessed 6 Dec 2016

US Food and Drugs Administration (2015a) Mobile medical applications. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf. Accessed 6 Dec 2016

US Food and Drugs Administration (2015b) Medical device data systems, medical image storage devices, and medical image communications devices. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM401996.pdf. Accessed 6 Dec 2016

US Food and Drugs Administration (2015c) Draft guidance for industry and food and drug administration staff. http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429672.pdf. Accessed 6 Dec 2016.

US Food and Drugs Administration (2016a) Examples of mobile apps for which the fda will exercise enforcement discretion. Available at: http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/ucm368744.htm. Accessed 9 Dec 2016

US Food and Drugs Administration (2016b) Medical device accessories–describing accessories and classification pathway for new accessory types. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429672.pdf. Accessed 6 Dec 2016

US Food and Drugs Administration (2016c) General wellness: policy for low risk devices. Available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery. Accessed 6 Dec 2016

Wired (2014) These medical apps have doctors and the FDA worried. http://www.wired.com/2014/07/medical_apps/. Accessed 8 Aug 2016

Wolf J, Moreau J, Akilov O et al (2013) Diagnostic inaccuracy of Smartphone applications for melanoma detection. JAMA Dermatol 149(4):422–426

23andMe (2013) A look At 23andMe’s DNA revolution. https://blog.23andme.com/news/a-look-at-23andmes-99-dna-revolution/. Accessed 8 Aug 2016

23andMe (2016) Order. https://store.23andme.com/en-int/cart/. Accessed 8 Aug 2016

Eugenio Mantovani is research fellow at the interdisciplinary research on Law, Science, Technology and Society (LSTS) at the Vrije Universiteit Brussel (VUB). Eugenio's research interests include the law on data protection and privacy, with particular focus on the area of health care delivery. He is interested in the evolving use of technologies for ageing societies and has published a number of articles on these issues. His doctoral thesis delves on the relationships between ageing and technology, which he broaches from the point of view of the law. Eugenio has been active in a number of European research projects with a focus on these themes.

Pedro Cristobal Bocos is a researcher at the VUB, where he focuses on the relation between new technologies and fundamental rights from a European Union regulatory perspective. He is currently working at the Interoperable platform for Remote monitoring and Integrated e-Solutions (IRIS) project for the development of an open-source and secure ICT platform for interoperable collection and communication of wireless 3G/4G audio-video data, point-of-care device data and patient medical history data, across hospitals, emergency vehicles and patient portals at home. He is assuring that the IRIS platform will comply with the legislation on privacy and data protection, medical device regulations and liability legislation as well as technological regulations. He studied political science at the Universidad Carlos III de Madrid (2009–2012, including a stay at Maastricht University), European law at the Universidad Nacional de Educación a Distancia (2012–2013) and European Union studies at Maastricht University (2012–2013). He has experience working in institutions based in Spain and Belgium, including the International Automobile Federation, European Digital Rights and the European Centre for International Political Economy.