Discussion Paper

Filling the Gap: Legal and Regulatory Challenges of Mobile Health (mHealth) in Europe

Work in progress.
Comments are welcome.

Please send your comments to: cybmail@itu.int by September 1st, 2014.

Table of Contents

Page

Summary iii

1 Contextual Elements 1

1.1 The recent emergence of mHealth 1

1.2 The lack of definition for mHealth 1

1.3 Expected development of mHealth in Europe 2

1.4 Legal challenges facing mHealth in Europe 3

1.5 Purpose of the present paper 5

2 mHealth and Medical Devices 6

2.1 Accessibility of the European market 6

2.2 Directive 93/42/EEC, amended 7

3 mHealth and Medical Information 11

3.1 Protection of privacy 11

3.2 European patients' rights 12

3.3 European medical information regime 12

3.4 Personal Medical Record 14

3.5 Shared health information systems 15

4 mHealth and Medical Practice 16

4.1 Legal issues surrounding the practice of medicine delivered over mobile devices (mobile telemedicine) 16

4.2 Legal recognition of mobile telemedicine 16

4.3 Legal regime governing mobile telemedicine 17

5 Conclusion 20

Legal and Regulatory Challenges Facing mHealth in Europe

Author: Prof. Lucien Rapp, Professor at the University of Toulouse1-Capitole, Associate Professor, HEC (Hautes Etudes Commerciales), Paris

Summary

This paper is intended to provide an analysis of the primary legal challenges faced by European countries (lato sensu) with the development of medical information services, and patient health care or follow-up services, accessible over mobile terminals (telephones, PDA, tablets, and dedicated equipment) (hereinafter "mHealth"). When relevant, it refers to the European Union, which started to take a few initiatives in the field of mHealth, including a Green Paper recently published (10 April 2014) and offers some useful examples of harmonized solutions.

Part 1 will discuss contextual elements useful for the topic at hand.

Then it will articulate a summary of current legal issues facing mHealth around the three notions of **medical devices** (Part 2), **medical information** (Part 3) and **medical practice** (Part 4).

Finally, in Part 5, it will offer some recommendations concerning opportunities and purpose of further in-depth measures for harmonization of national laws.

1 Contextual Elements

1.1 The recent emergence of mHealth

Developments in mobile communication in recent years[1] and its subsequent widespread penetration in many countries, primarily in Europe, has promoted the emergence of new services, accessible from mobile terminals, for medical information, monitoring and surveillance, and delivery of care, including:[2]

- dissemination of health-related information for prevention purposes;
- creation of call centres to provide medical advice or brief medical consultations;
- remote diagnosis and treatment of certain diseases;
- training of medical and paramedical personnel;
- monitoring of seasonal epidemics or pandemics;
- home care of mildly ill or chronic patients (diabetics, hypertensive) or the elderly;
- conduct of longitudinal studies using regularly updated databases.

All of these services and applications[3] describe what should now be called "mHealth".

1.2 The lack of definition for mHealth

In current national laws and regulations, there is no definition of mHealth, which might seem to hinder an in-depth analysis of these new medical practices. The World Health Organization (WHO) defines mHealth very broadly as "medical and public health practice supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants (PDAs) and other wireless devices"[4].

Generally speaking, mHealth encompasses all available services for delivering care or medical information using mobile equipment and networks.

Technically mHealth implies:

- wireless broadband electronic communications infrastructure;
- an electronic platform;
- downloadable software and specialized applications ;
- connected mobile terminal equipment whether common (telephones, tablets, PDA) or specific (implantable or non-implantable).

---

[1] "*By 2016, mobiles devices will account for about 80% of all broadband connections in the G-20 nations*". In addition, "*by 2016, there will be an estimated three billion internet users*". (source: The Digital Dimension of Healthcare, Report of the Digital Innovation in Healthcare, Working Group, 2012)

[2].WHO, *New horizons for health through mobile technologies Global Observatory for e-Health series*. Vol.3, p.6

[3] The GSMA categorizes mHealth solutions into two broad areas: solutions across the patient pathway and healthcare systems strengthening.

[4] WHO Global Observatory of eHealth series – Vol.3.

1.3 Expected development of mHealth in Europe

Progress made in the use of radiofrequency capacities with the appearance of 4G and the widespread uptake of LTE networks, the use of increasingly sophisticated intelligent terminals, today allows the development of mHealth in Europe to be predicted in the years to come[5]. It is highly probable that these will constitute, in turn, a factor in the acceleration and emergence of new health information services or medical care accessible via mobile terminals[6].

Already many industry actors are mobilized in this new market sector in which they are also expecting major developments. Electronic communications operators, particularly mobile network operators, have created internal departments dedicated to health and sometimes specifically mHealth or eHealth. They intend to operate as "trusted third parties", connecting patients and healthcare personnel, providing data and bandwidth using a system offering strict confidentiality and security. Manufacturers of medical devices (such as pacemakers) have not hidden their intention to build communicating devices, sending the collected information to call centers and central servers to be accessed by physicians and medical experts. The main actors in the microprocessor sector are currently working to develop "health hubs" that will allow very high rates of data transmission over short distances sent by sensors or even communication modules (3G variety) integrated into a medical sensor. Publishers of medical encyclopedias are also positioning themselves in the market for training or providing remotely accessible information for medical personnel who might access it over mobile terminals (smart phones, tablets, portable computers).

Pharmacists themselves and pharmaceutical laboratories also intend to take their rightful place in the development of mHealth. They are mobilizing resources to provide support in the treatment of chronic diseases and intend to act as intermediaries for the patient's correct use of these mobile tools.

This perspective has been especially welcomed by governments since:

- European Union is an integrated commercial space built around the 28 member States and the laws of the European Union, representing today, both for Europeans and non-Europeans alike, one of the largest – if not the largest – markets in the world[7];
- More generally, the countries of Europe are confronted by an ever more pronounced aging demographic, leading them to promote home health care for elderly or dependent persons as a credible alternative to hospitalization[8];

[5] It is estimated that some of 30% of smartphone users are likely to use wellness apps by 2015

[6] The number of mHealth apps that are published on the two leading platforms, iOS and Android, has more than doubled in only 2,5 years to reach more than 100.000 apps (Q1, 2014). The market revenue reached USD 2,4bn in 2013 and is projected to grow to USD 26bn by the end of 2017.

[7] By 2017, Europe will be one of the largest markets for mHealth globally, representing roughly 30% of global revenues.

[8] Taking data collected from pilots and projects in Scotland and Norway, it is estimated that mHealth could reduce overall elderly care expenditure by 25% see Ernst & Young, The State of Remote Care in Norway Enabling a sustainable welfare state (2011). More generally, see Boston Consulting Group, The Socio Economic Impact of Mobile Health, April 2012.

- The growth in health-care costs and the size of budget deficits and the resulting social security deficits has now forced all European public authorities to search for savings and greater efficiencies in public expenditures[9].

This should lead all of the concerned States to:

- create a statement of currently used services or practices and a list of the different sectors of activity concerned;
- share their respective experiences, and particularly legal challenges, that arise from the development of these new uses and any solutions found for them; and
- adopt a shared legal framework, harmonized if possible;
- reflect on shared initiatives, such as, for example, the implementation of a single control structure, specifically intended to coordinate all of the efforts led by medical or pharmaceutical practitioners, mobile electronic communication network operators, manufacturers (from medical device or mobile terminal manufacturers to software designers), content aggregators, insurers and welfare agencies, to develop mHealth.

1.4 Legal challenges facing mHealth in Europe[10]

The development of mHealth in Europe lies within a paradoxical context.

The technology is already present and used in many sectors and it is becoming increasingly common to be used to provide remote care to patients.

Mobile electronic communications networks have entered the 4G era. As with their counterparts in other countries of the world, European users hold in their hands mobile terminals containing more processing power than was necessary at the end of the 1960s for Man to walk on the moon.

Technical platforms used to provide remote care have been subject to multiple experiments that, in several cases, have been conclusive. They could be generalized and up-scaled.

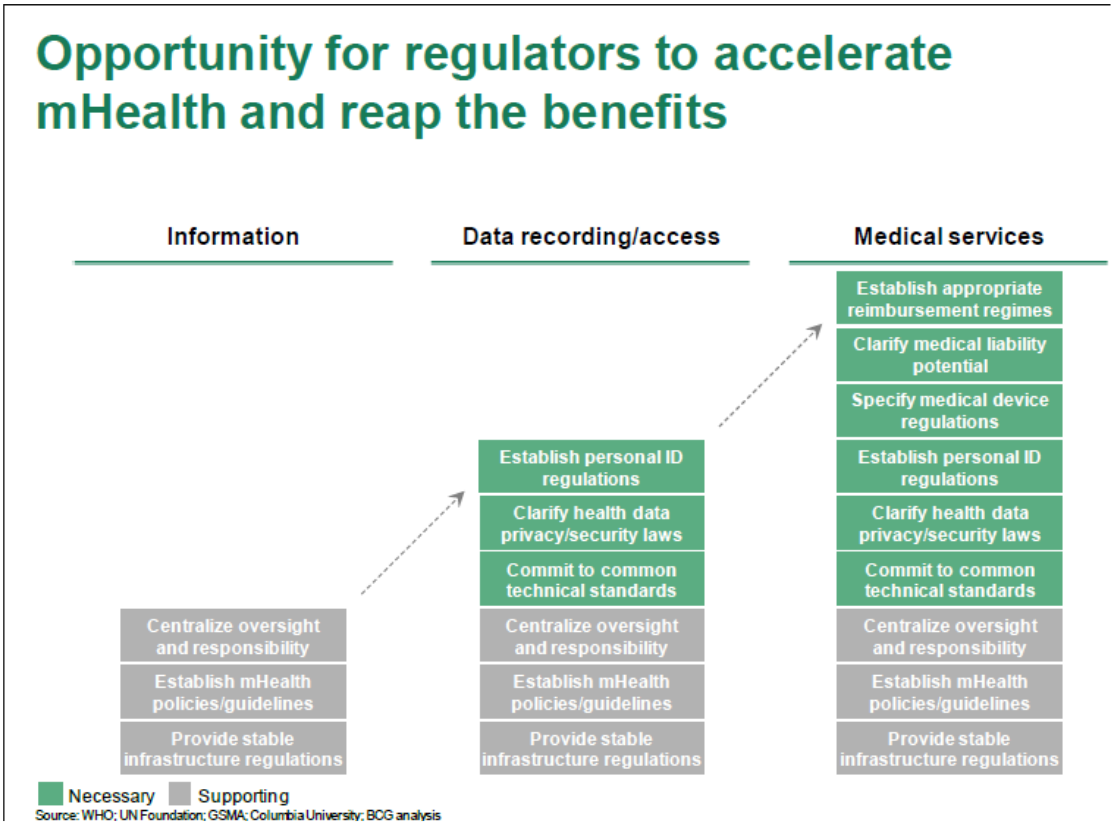
Many medical applications, which were not developed in Europe, may now be downloaded. Their uses are expanding with the number of clients of mobile network operators, of which there are now more in Europe than fixed network operators.

Added to this are the traditions of excellence in training and skills of medical personnel (physicians, nurses, caregivers), who regularly put Europe in first place among the world regions, from the point of view of quality of care provided both in a hospital or medical setting and at home. These traditions are served by a welfare system which is certainly costly as was previously noted, but which is highly valued by Europeans, to the extent that it has become the original characteristic of what may today be called the "European way of life".

[9] Trials in Nordic countries show that mHealth could generate a 50-60% reduction in hospital nights and rehospitalisation for patient with COPD, see European Commission, Report on the pubic consultation on eHealth Action Plan 2012- 2020 (2011)

[10] Please see Appendix A herenafter.

However, mHealth is insufficiently widespread and, in the end, still in a very largely experimental phase. Many reasons might explain that. European operators, those in the health and social sectors as well as those in the electronic communications sector, suggest that one of the main reasons lies in insufficient rules and an inadequate national and European legal framework, representing a "legal challenge" to overcome if the development of mHealth is to be promoted.



The current inadequacy of the legal system for mHealth in Europe involves three types of issues:

1. currently applicable rules in Europe are either nonexistent as will be seen in the discussion below, or extremely inadequate, which might mean that they do not account for or, at least do not appropriately account for, the specific requirements for the development of mHealth[11];

2. European institutional and legal landscape is too fragmented as it is largely dominated by individual State jurisdictions. Accordingly, operators are confronted by what appear essentially as national legal obligations (when they are not imposed on sub-national levels). No attempt at harmonization or consistency has yet been made in the systems – for example a system of mutual recognition for national approvals. All operators are thus quite cognizant of the need to harmonize rules on a Europe-wide, if not worldwide basis.

[11] As GSMA observes in its report on the EU Regulatory Framework for Medical Devices, "*new mHealth devices are increasingly covered by two regulatory frameworks: the Radio Equipment and Telecommunications Terminal Equipment (RTTE) and the EU Medical Devices Directives (MDD)*".

3. European regulatory framework for mHealth appears to be lagging behind that of competing regions (North America or Japan), since the development of mHealth implies a minimum level of international coordination.

The best practices in other regions of the world, namely the United States with the initiative by the FDA (Food and Drug Administration), shows, however, that any undertaking to define a legal framework adapted to the requirements of mHealth will also be fought against with allegations of untimely regulatory or legislative initiatives that risk impeding innovation and preventing the development of technologies or practices which require, at the start of their use at the very least, an adaptation phase served by a very flexible legal framework as unrestrictive as possible.

Therefore, there is a need to be quite prudent and to refrain from adopting either of two equally disputable attitudes:

- legal conservatism, which would consist in claiming that current inadequacies in the legal framework benefit the development of mHealth and that nothing needs to be done to promote the emergence and development of new infrastructure and services;
- legal activism, which, conversely, would seek to investigate and systematically propose modifications to this legal framework, more or less inspired from North American initiatives which, while certainly useful references, need to be examined with regard to their ability to be transposed into the European cultural, social, economic, and industrial context.

1.5 Purpose of the present paper

This paper offers an analysis of the primary legal issues raised by the development of mHealth in Europe and their appropriate solutions. In the discussions below, it presents a summary of these legal issues and their possible solutions with regard to the three notions of medical devices (Part 2), medical information (Part 3), and medical practice (Part 4). It offers some recommendations concerning the opportunity and purpose of measures intended to provide greater depth to the harmonization of the European institutional framework and national laws.

Because this is a discussion paper, the following discussions employ very general terms without explicit reference to any particular European nation. However, these discussions are based on an initial study, limited in scope, of several legal systems from European countries used as meaningful examples (Belgium, Spain, France, Italy, Poland and the Czech Republic). They are also based on an analysis of the European Union's legal regime, which today is the most developed. From such systems, an initial set of notions has been gathered. The discussions also draw on contributions from several informal dialogues with operators in the relevant business sectors (network or platform operators, equipment manufacturers, designers and distributors of specialized software, healthcare professionals or pharmacists, insurers or welfare agencies). When relevant, they consider legal rules from non-European countries, particularly the United States or international organizations, whether general or specialized, whose jurisdiction extends beyond the territory of Europe. They recommend a more systematic identification of the problems and solutions they enumerate. The States might conduct such activity themselves, in connection with professionals from the business sectors in question, using a questionnaire that might be submitted to them. This

questionnaire would allow for the further identification of difficulties encountered in each European State, its expectations, and to the extent that such exist, the specific legal solutions that the State has been able to implement, the efficacy of such solutions, and their potential for generalization across other European States.

2 mHealth and Medical Devices

2.1 Accessibility of the European market

To review, the medical devices considered in the following discussions fall, without differentiation, into two types of architectures as follows:

- the first represents services provided using specific software that is intended to be used for diagnostic and/or therapeutic purposes (as will be explained below) and which is downloaded by a user through a mobile network operator from any mobile Applications stores; the user thereby becomes a remote patient[12]; and
- the second involves a patient wearing – or having implanted in him – specific equipment, which uses wireless frequencies to transmit the patient's medical information so as to allow a team of physicians to monitor him remotely.

With these notions in mind, the development of mHealth in Europe implies access to the European market by medical device manufacturers or distributors. However, such access may not be complete since European States must be able to exercise their control over the quality of medical devices circulating in Europe and ensure, above and beyond their intrinsic efficacy, their safety vis-à-vis the patients using them. The difficulty arises here because each European State has – or may reasonably have – specific requirements with regard to protecting the health of its citizens. These exigencies should not, however, act as a pretext for protectionist policies, intended to defend national industries, which would be contrary to the principle of free movement of goods.

In principle, to the extent discussed below, the national administrative, regulatory, and legal provisions continue to establish conditions for medical devices to access individual European States. These provisions implement certification and control procedures intended to verify that the medical devices in question offer patients, users, and third parties, a high level of protection and that they attain the performances assigned to them by their manufacturer.

The fragmentation of national territories and the disparity in administrative, regulatory, and legal provisions applicable to medical devices, even though such disparity is currently more and more relative, explain the complaint by manufacturers or their European

[12]To determine whether an app is in fact meant for a medical purpose or simply for general health and wellness, the regulators look at the intended use of an app. Part of this determination is based on how the app is marketed, promoted, labelled, or advertised. However, both the intended use and actual use will factor into whether the app is ultimately regulated as a mobile medical app. Apps that carry a potential risk to the public if they fail to function properly are primary concern in this arena. Many if not most healthcare apps at this point are not considered mobile medical apps. See the European Commission's Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012

representatives – when such manufacturers are non-European – against the current legal system in the European territory and their hope for a continent-wide harmonized regime or, failing on that, procedures for reciprocity between national approvals.

This criticism is especially striking since the European market, despite its size, does not offer a level of consistency as high as that as the United States, a federal State. Be this as it may, over the course of the last two decades, Europeans have made a laudable effort to harmonize their national laws, - at least within the European Union - and to adopt a body of common rules (see below). This body of common rules, while still quite imperfect, today offers the beginning of a minimum legal basis that may be hoped for not only by European manufacturers, but also their non-European counterparts in the European market.

This is reinforced by the experience of procedures for mutual recognition of approvals for terminal equipment in the related mobile electronic communications sector, before such procedures were replaced by the current system of certificates of conformity to essential requirements or, at a different level, by more recent Commission initiatives intended to implement harmonized procedures, if not direct community-based procedures, to authorize use of frequency spectra.

2.2 Directive 93/42/EEC, amended

The system implemented within the European Union is actually based on Council Directive 93/42/EEC dated 14 June 1993, the Medical Devices Directive[13]. This directive does not cover all national or European rules applicable to a manufacturer or the European agent thereof who wishes to sell a medical device on the European market.

Other rules[14] may be applicable depending on whether:

- medical device is sufficiently similar to a medicine or incorporates substances that may act on the patient's body by a separate action from that of the medical device (Council Directive 65/65/EC, amended, of 26 January 1965 on the approximation of provisions laid down by Law, Regulation or Administrative Action relating to proprietary medicinal products);
- medical device raises the question of its electromagnetic compatibility (Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of the Member States relating to Electromagnetic Compatibility);

[13] Please note that on 11 April 2014, public consultations were launched by International Medical Device Regulators Forum on Medical Device Single Audit Program and the Software as a Medical Device. On 16 May 2014, the European Commission issued a communication in the framework of the implementation of the Council Directive 93/42/EC of 14 June 1993 concerning medical devices OJ C-149/3.

[14] The core legal framework consists of 3 directives: Directive 90/385/EEC, regarding active implantable medical devices, Directive 93/42/EEC regarding medical devices and Directive 98/79/EC regarding in vitro diagnostic medical devices. They aim at ensuring a high level of protection of human health and safety and the good functioning of the Single Market. These 3 main directives have been supplemented over time by several modifying and implementing directives, including the last technical revision brought about by Directive 2007/47/EC. On 26 September 2012, the European Commission adopted a Proposal for a Regulation of the European Parliament and of the Council on medical devices and a Proposal for a Regulation of the European Parliament and of the Council on in vitro diagnostic medical devices which will, once adopted by the European Parliament and by the Council, replace the existing three medical devices directives.

- medical device emits ionizing radiation (Council Directive 80/836/Euratom of 15 July 1980 amending the Directives laying down the basic standards for the protection of the health of workers and the general public against the dangers arising from ionizing radiations);
- medical device in question uses radio frequencies which have undergone harmonization or harmonized procedures.

2.3 Harmonized definition of medical devices and status of mobile medical applications (MMA)

The aforementioned Directive of 14 June 1993 concerning medical devices is based on a set of definitions, at the center of which is precisely that of a medical device. As the provisions of the directive now stand, as modified in 2007, a distinction is made between a device itself and its accessory or accessories.

A medical device is defined as being "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, intended by the manufacturer to be used for human beings for the purpose of:

- diagnosis, prevention, monitoring, treatment or alleviation of disease;
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
- investigation, replacement or modification of the anatomy or of a physiological process;
- control of conception; and
- which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means.

An accessory is defined as being "any article which whilst not being a device is intended specifically by its manufacturer to be used together with a device to enable it to be used in accordance with the use of the device intended by the manufacturer of the device.

From these definitional elements, it follows that:

- medical device is recognized, above and beyond its functions, by its intended use as defined by the manufacturer; a medical device is therefore, to a certain extent, a finished product that should be regulated by a set of rules different from those governing any adaptations or uses that might be made of it independently of the end-uses assigned to it by its manufacturer;
- these end uses concern medical practice which have nothing to do with hygiene or cosmetic products;
- similarly, equipment designed to alleviate or compensate for a handicap is not a medical device;
- software intended to be used specifically for diagnostic and/or therapeutic purposes is a medical device;

- device with multiple intended uses may be a medical device for the sole use which identifies it as such.

Accordingly, it seems difficult to label a mobile terminal used by patient as a medical device, to the extent that this terminal does not meet the intended end-uses of a medical device as defined above. However, software designed for diagnostic and/or therapeutic purposes that may be downloaded to a mobile telephone meets or may meet the preceding definitions and, consequently, may lie within the scope of the Directive of 14 June 1993.

It is meaningful to note that such a possibility garnered the attention of the United States Food and Drug Administration (FDA) which sought to clarify its analyses with regard to manufacturers of specialized software and has published the guidelines on how it intends to regulate health and wellness apps in 2013. The objective of the guidelines is to provide more clarity to developers about the types of apps that will fall under FDA regulation. The FDA will focus on two types of apps that have the potential to harm consumers if they do not function properly. The first are those apps that are intended to be used as an accessory to a regulated medical device, for example an application that allows a healthcare professional to make a diagnosis by viewing a medical image from a picture archiving and communication system (PACS) on a smartphone or a mobile tablet. The second type of app transforms a mobile platform into a regulated medical device, for example an app that turns a smartphone into an electrocardiography (ECG) machine to detect abnormal heart rhythms or determine if a patient is experiencing a heart attack. Mobile health apps that undergo FDA review will be assessed under the same standards that the agency applies to other medical devices[15].

Given its importance for the development of mHealth, it might be useful for a similar type of reflection to be undertaken in Europe.

Additionally, there is the fact that the development of these applications and their utilization — beyond the question of their legal qualification as medical devices – raises even more delicate issues given that the development and utilization of such applications occurs in a multinational (cross-border) environment in which multiple systems of law may apply or overlap. Furthermore, they involve the use of an operator, the developer, who may either creates an application on his own behalf and makes it available to an end-user, or does so on behalf of a third-party as part of a development contract or even under an employment contract.

An issue then arises, for example, as to which intellectual-property regime will cover such specialized software. It must be resolved with consideration given to the fact that a developer holds rights (property rights and moral rights) over the application he markets or over which he has created on behalf of another and the regime governing such rights must be established either by law, or by the development or employment contract. The development of open-source medical applications also raises the question of the license governing the use of such software and the conditions in which public sources are made available.

The distribution of mobile applications further implies the formation of usage licenses, even the implementation of terms and conditions for use and distribution when the software may

[15] http://www.mobileworldlive.com/fda-finally-rules-health-wellness-apps?utm_campaign=MWL-H-20130902%20%3a%20Copy&utm_medium=email&utm_source=Eloqua&elq=4222b65ae87e41ea9816601e17d4da5a&elqCampaignId=657

be downloaded over a third-party platform, which should be defined and over which the legal regime should be established.

Finally, some mobile medical applications include processing of the users' personal information, even the possibility of geolocation the persons in question, which implies legislative oversight either based on the general system for protecting personal information or on the more specific one of the rules applicable to network operators or electronic communications service providers. Users of mobile medical applications providing geolocation services should therefore be informed that their data may possibly be reused by third-party advertisers for commercial purposes and must be able to give their consent to this transfer (opt-in or opt-out).

2.4 National certification procedures and essential requirements

As defined in its scope, the Directive of 14 June 1993 lays out the contours of a harmonized system of rules, the purpose of which is to frame national laws so as to guarantee the principle of free movement throughout the territory of the European Union.

This harmonized legal framework is based on the recommendation made to the States to ensure that their national provisions pursue no other purposes other than those necessary to satisfy essential requirements when they govern a medical device's entry into the stream of commerce or initial use. These essential requirements are defined by their end purpose: which the Directive defines as being to ensure patients, users, and third parties a high level of protection and to allow the States to ascertain that the performances attributed to the medical devices in question by their manufacturers are in fact attained.

More specifically, the Directive articulates the rules governing medical devices involving four product classes with corresponding procedures for evaluating conformity with different essential requirements based on the risks that they may cause patients, users, and if applicable, other persons. These four classes involve:

- a procedure for which the manufacturer is solely liable based on the low degree of vulnerability of the medical devices in question (class I)
- required intervention by a notified body during the manufacturing stage (class II a);
- inspection of the design of the medical devices (class II b);
- explicit authorization confirming the conformity of the medical devices to national requirements, prior to their marketing (class III);

This legal system is itself doubly framed:

- by the possibility for each State to invoke a safeguard clause and appear to be more restrictive with regard to medical devices which a State might consider as being more vulnerable;
- conversely, with the right to implement a presumption of conformity to essential requirements when medical devices satisfy their national standards, which themselves were adopted in accordance with harmonized European standards.

2.5 CE marking

CE marking of medical devices released into the European stream of commerce confirms their conformity to essential requirements. This occurs by means of a rather complex procedure, the diagram of which is included in Appendix B, showing all of these elements, including consideration as to whether the medical device manufacturer is European or non-European.

It can be seen that these procedures yield different pathways depending on the type of device and it may be concluded that these different pathways are one factor in adapting legal rules to the characteristics of each medical device. But, it would, of course, be useful to study the opportunity for simplifications required by the development of mHealth in Europe.

Furthermore, one should not fail to note that the recommendations of the Directive of 14 June 1993 have, to date, been transposed in their totality in the 28 member States of the European Union and that manufacturers of medical devices already bearing the CE marking at the time it took effect, had 18 months to achieve full conformity with the requirements of its provisions.

Therefore, one might think that, they are presently all in conformity. Such that regarding the European countries which do not belong to the European Union, the aforementioned Directive of 14 June 1993 presents a solid basis, a harmonization policy for national procedures and laws may be pursued.

3 mHealth and Medical Information

3.1 Protection of privacy

The development of mHealth in Europe implies the ability to collect, retain, and transfer personal information likely to contain intimate details of patients' private lives[16]. Accordingly it is essential for the legal rules governing these operations to be strictly framed and that particular attention is to be given to the adoption and implementation of restrictive rules that are already provided for by the national laws in most European countries.

Of course, it should be noted that this touches on one of a person's fundamental rights as consecrated by Article 12 of the Universal Declaration of Human Rights, and in a more specifically European context, by the European Convention for the Protection of Human Rights; more particularly in its article 8, which itself has resulted in now established jurisprudence from the European Court on Human Rights.

In many States, protection of medical information is even one of the subsets of the law governing the protection of health or the right to health written into the Constitution.

It is therefore no wonder that all States in Europe have laws or have adopted formal rules intended to protect privacy and more precisely data of a personal nature.

Generally, these laws are backed by a system of relatively dissuasive criminal sanctions.

[16] See notably "*Legal Framework for eHealth* », World Health Organization, Global Observatory for eHealth series – Vol.5, 2012

In the more specific domain of social and health services, patients' rights over their personal health information are based on four cardinal principles, about which European states rarely compromise:

- the obligation to inform the patient and respect his freedom of decision;
- patients have a right to maximum treatment efficacy, regardless of its cost to the community, even governments have become increasingly preoccupied about this cost given scarce public resources;
- treatment safety and any reduction in risks that it may potentially provide the patient who must be fully informed thereof;
- equal access to care.

3.2 European patients' rights

Therefore, one will not be surprised to find intra-European agreements devoted to notions of respect for each patient's privacy and the necessary protection of the patient's personal health information:

- Convention for the Protection of Individuals with regard to Automatic Processing of Personal information (the convention known as Convention 108 adopted on the basis of the aforementioned article 8 of the European Convention for the Protection of Human Rights);
- Recommendation from the Council of Europe on the Protection of Medical information (Recommendation No. R (97) 5, adopted in 1997);
- A declaration on the promotion of patients' rights in Europe, adopted in 1994 under the aegis of the World Health Organization;

These documents (international conventions or treaties) frame the efforts by the States who have all, at least in Europe, established national rules taking direct inspiration from them.

3.3 European medical information regime

In Europe, the effort at harmonizing these national laws has been the most advanced, primarily on the basis of 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 information and on the free movement of such data[17]. An e-Privacy Directive 2002/58/EC of 12 July concerning the processing of personal data and the protection of privacy in the electronic communications sector as modified by Directive 2009/136/EC[18] sets a specific standard to any entity worldwide that wishes to store or access information stored in devices of users located in the European Economic Area. Its main provision is relating to cookies or similar tracking technologies which require each user's specific consent, provided that a clear and comprehensive information have been furnished about the purposes of the processing (art.5 (3°) of the e-Privacy Directive)[19].

[17] A proposed EU Privacy Regulation intends to replace the 95/46 Data Protection Directive.
[18] OJ L337, 18 December 2009, p.11
[19] Other e-patient's rights include the rights enshrined in Consumers' rights Directive 2011/83/EC, in e-Commerce Directive 2000/31/EC and in Unfair Commercial Practices Directive 2005/29/EC

With regard to data that is collected and processed for purposes of preventive medicine, medical diagnostics, administration of care and treatments or even management of healthcare services, the provisions of the Directive are based on two simple principles:

- medical information is definitely sensitive data which, in principle, may not be processed, as is noted in article 8.1 of the Directive;
- but when such processing is performed for the previously mentioned purposes (preventive medicine, medical diagnostics, administration of health care or treatment, management of healthcare services), the processing of medical information – sensitive data – may be authorized under national laws, provided that such processing is performed by a healthcare practitioner subject to an obligation of professional confidentiality under national law (laws, regulations, decisions from regulatory bodies or professional orders).

This explains the concern found in all national laws to promote respect for the confidentiality of health data, a principal guaranteed on penalty of criminal sanction. From this too follows the importance of the emphasis placed on collecting the patient's consent, which is, without a doubt, the best guarantee for respect of this confidentiality.

Above and beyond this first set of considerations, processing of medical information lies within the more general system of rules governing personal information which in Europe it is certainly one of the most protective, if not the most protective, systems in the world. This particularly means that:

- medical information may only be collected after the interested parties have been informed;
- processing applied must comply with definite, explicit, and legitimate purposes;
- data processing must be loyal and legitimate;
- files created must be accurate, updated, and stored in conditions of guaranteed security, for a duration not to exceed that which is necessary to conduct the purposes for which said data has been collected.

It was on these legal bases in many European countries that exceptions were made and granted to the previously stated principle concerning the prohibition against the collection and processing of personal information,

- for data processing by physicians or biologists for purposes of preventive medicine, medical diagnostics, or administration of care or treatment;
- for the purpose of conducting epidemiological studies or biomedical research;
- for medical research purposes, since the legislatures have, in many countries, strengthened the control procedures over these files, regardless of the legal status of the body in question;
- in the setting of procedures for evaluating care delivered by healthcare professionals, hospitals, or care-giving organizations (welfare funds, insurance companies, mutual benefit associations).

In many states, work done in pursuit of the public interest also justifies the collection and processing of personal health information.

In parallel, patients have an acknowledged right to access medical information which concerns all information in the possession of professionals or healthcare establishments; this right of access is exercised either directly, or more often in Europe, through a physician.

Finally, national laws have placed an obligation on the parties responsible for data processing to ensure the security of recorded data and to prevent their misuse. These protective and security measures are applied through user authentication mechanisms, a connection management (connection logging) policy, even specific obligations incumbent on the host, since data hosting can take place only with the express consent of the concerned person.

3.4 Personal Medical Record

The arrival of personal medical records (PMR) in many European States has justified the adoption of specific provisions intended to guarantee confidentiality of data when such data is to be shared, particularly in the context of healthcare networks.

From the last point of view, it is quite interesting to note that in Europe, the record is often considered as belonging to the patient, meaning that only with the patient's authorization may health professionals access the record and make entries in it concerning the patient.

These precautions lie more generally within the framework of government policies - or those of regulatory bodies for the sector, when such are present - which require that any data processing implemented for purposes of coordinating care and which, consequently, necessitate data sharing, are in the public interest.

It appears important to signal an adaptation in the regime of express consent given by the party concerned; unlike the common law governing personal information, this consent, except where expressly provided, is not sufficient to ensure protection of the patient; the law has established the personal information scheme in question, prohibiting or regulating the methods for processing medical information under relatively restrictive conditions.

Among the obligations incumbent on the concerned operators, are found, in general, the following obligations:

- the obligation to mask certain data;
- the obligation to designate by name each of the health professionals whom the patient wishes to provide with rights to read or write information;
- the obligation to implement technical mechanisms that will allow the patient to directly access his medical record from his computer terminal.

However, given the state of national regulations in Europe, these obligations are not always accompanied by efficient sanctions, thereby in many States posing the question as to the guarantee offered by protections for personal health information.

In particular, the requirements established in the national laws and regulations, particularly with regard to the healthcare provider's card, or the implementation of equivalent mechanisms, does not appear adapted to the reality of information systems which are built over time, without communication-based interoperability criteria. This situation is even more regrettable since any person who is cared for by a professional or an institution, a

healthcare network, or any other body participating in healthcare and prevention clearly is entitled to respect for his or her privacy and confidentiality with regard to his/her personal information.

3.5 Shared health information systems

Several European states have created specific regulatory bodies such as the *French Agence des Systèmes d'Informations Partagées de Santé* (Agency for Shared Health Information Systems) which should be welcomed with interest. Among the numerous responsibilities entrusted to this body, besides defining the means necessary to protect health information, such as data security and confidentiality, but also:

- implementation of a national framework for health information system interoperability,
- definition of the standards used when sharing or exchanging health data between information systems, and
- implementation of these standards through particular specifications.

This is an experience that could be generalized provided that all lessons are learned and any deficiencies are corrected. They might, for example, have the means to make state financing for mHealth projects in the territory subject to compliance with standards for interoperability and security that they would publish.

One might also engage in widespread implementation of procedures for approving personal health information hosts as has been successfully done by several European states, seeking to authorize only those hosts that guarantee a high level of security and confidentiality and who commit to comply with the principle of protecting personal health information.

Special attention may even be given to the concept of regional health information organizations (RHIO) that can be found in several European states. These organizations provide decentralized electronic services and are designed to work institutionally with regional health agencies, regional health agencies, and are controlled by a regional project manager. In this manner, data protection is decentralized and utilized more effectively.

Although it is not specific to the healthcare sector, the question of the legal status of cloud computing must be asked in specific terms when personal health information is at issue. Even greater attention must be paid since the use of cloud computing techniques allows cross-border transfers of personal health information.

The aforementioned Directive of 24 October 1995, and even the recommendations from the working group on Article 29, enforces the reflection which should be actively pursued in the patients' interest.

4 mHealth and Medical Practice

4.1 Legal issues surrounding the practice of medicine delivered over mobile devices (mobile telemedicine)

Medical practice is at the center of the legal regime governing any health care system. For example, this is what conditions mechanisms for reimbursement[20] or assumption of the cost for healthcare or monitoring. It is even the basis for rules governing liability of practitioners, technicians, and other participants in the health care delivery chain.

mHealth singularly modifies its contours, particularly by complicating it with the intervention of intermediaries (operators or technicians). It renews the legal issues to the extent to which medicine is no longer delivered in a hospital or medical setting. It implies the patient's active participation for it to occur which suggests the need for a significant effort at medical instruction and education[21], even though the use of information technologies is quite widespread today. It may contribute to or indeed raise on its own the question of equal access for each patient to medical care produced using mobile networks.

This risk of disparity invites an examination, in the first place, of the right of any person, given his state of health and the urgency of the interventions that this state of health requires, to receive the most appropriate care and benefit from therapies with known efficacy and which guarantee the best health safety with regard to demonstrate medical knowledge. This should apply regardless of whether these methods use medical devices, medical platforms, or even mobile communication infrastructures.

It should also be recalled that whatever the method – particularly if it is provided using mobile devices – any act of prevention, investigation, or care must not, given the current state of medical knowledge, cause the patient to incur disproportionate risks with regard to the expected benefit and must not be pursued with unreasonable obstinacy.

Finally, there is a need to emphasize the counterpart of this right, which is the obligation for any healthcare professional to use all of the means at his disposal to provide each person with care that relieves pain and provides a dignified life until death. Medical monitoring of a patient or the delivery of care remotely using mobile devices cannot circumvent the scope of this fundamental obligation or be modified in such a way as to reduce said scope.

These elements are preconditions to any definition of a more appropriate European system.

4.2 Legal recognition of mobile telemedicine

This being so, progress made in mHealth calls for an explicit recognition of this new form of medical practice.

In the countries of Europe that have not yet explicitly recognized that, a consideration for such laws to be adapted should be taken into account.

---

[20] Reimbursement is currently viewed by the GSMA as a key regulatory issue.

[21] Particularly, the problem most often posed concerns the danger that a remotely cared for or monitored patient using mobile devices may too frequently consult the measurements that he is conducting himself, adding a potentially complicating sentiment of anxiety to his treatment difficulties.

A text having binding legal force (in law for example) must establish that this practice permits

- a diagnosis to be determined,
- a patient to be provided with preventive or post-therapeutic monitoring,
- a specialized opinion to be sought,
- a therapeutic decision to be prepared,
- drugs to be prescribed,
- services or interventions to be prescribed or performed, or even
- monitoring to be performed.

As needed, enacting legislations (regulations) should enumerate what medical practice may be provided remotely using mobile devices:

- teleconsultation;
- tele-expertise;
- remote medical monitoring;
- remote medical assistance;
- medical response.

As several European laws have noted, an emphasis should be placed on the need for the patient's free and fully informed consent to mHealth and to establish the principle by which professionals participating in the practice of medicine delivered over mobile devices may, unless opposed by the duly informed person, exchange information about this person, namely over networks or specialized platforms.

4.3 Legal regime governing mobile telemedicine

The development of medical practice or delivery of care provided over mobile devices must involve, as is already emphasized by most current laws and regulations in European countries, compliance with conditions guaranteeing:

- authentication of health professionals delivering the intervention;
- patient identification;
- healthcare professional access to the patient's medical information necessary to provide medical practice; and
- as required by the patient's condition, any patient training and preparation for use of the medical device necessary for the care that shall be delivered to him or the monitoring and surveillance of his health.

The content of patient's file maintained by each medical professional participating in care delivered to the patient remains yet to be precisely defined:

- report of the performance of the intervention;
- acts and drug prescriptions provided as part of the delivery of medical care;

- identity of the health professionals participating in the delivery of medical care;
- date and time of the care delivered;
- where appropriate, any technical incidents occurring during the delivery of care.

mHealth must become part of everyday medical practice. And to do this, it must be treated by two types of complementary regulatory or legislative provisions:

- a review of coverage in the current conditions within the territory of each European State by national health insurance agencies or individual insurance mechanisms of the practice of medicine delivered over mobile devices or networks; this coverage is evidently one of the essential conditions for the development of mHealth in Europe; it implies very close cooperation between the national welfare bodies or insurance companies in the definition of a national policy concerning its development;
- the framing of this activity might take inspiration from some currently enacted laws in Europe; such laws are notably based on (i) the definition of national programs ordered by the ministers in charge of health, the elderly, or handicapped persons, or in charge of health insurance, (ii), the registration of these programs in both a year contracts with objectives or resources formulated with participation by health professionals or hospital care institutions, even eldercare establishments, or even (iii) the conclusion of individual contracts with independent health professionals.

These programs and contracts state the conditions in which mobile telemedicine will be delivered taking into consideration the specificity of the offered care in question. These also further ensure that the professionals and psychologists participating in the delivery of care have the required training and skills necessary for the use of the corresponding devices. This ensures that the technology used complies with the provisions established with regard to hosting procedures for personal health information.

Specific public or private financing may be used to ensure the development of mHealth, such that the releasing of funds may be subordinated to compliance with the preceding conditions.

4.4 Authorization and procedures for qualifying mobile devices assisting in health care delivery

The definition of a set of rules governing medical practice must finally involve the implementation of approval systems or procedures for qualifying technical devices used to provide care with mobile equipment or networks.

It should be recalled that interventional tools or vital function sensors are not truly what is most at issue, as these are highly regulated by the rules governing medical devices, as was reviewed previously (see supra No. 2). What is primarily at issue here are the devices that are indispensable for the specificities of mobile telemedicine: the computer connection, multifunction servers, cameras and even screens.

It would be logical for the service providers who are providing tools and participating in the delivery of care within the mHealth framework to be if not officially approved or labeled, at the very least regulated using a set of appropriate standards.

This legal framework should not be considered as a constraint by the providers of the related services, who are, in reality, third parties to the relationship between the patient and the health professionals (ie. those who are practicing medicine strictly speaking). More logically, it aids in their legal protection. It is the absence of such which may be a source of danger for the professionals in question, as telemedicine delivered using devices, networks, or mobile communications platforms is actually a source of potential liability.

Hence, it would be natural that in addition to the healthcare professionals who incur liability through mobile telemedicine, that national laws or even European laws define the conditions for creating specific liability of technical third parties who intervene in remotely delivered care provided using mobile networks. In the absence of such provisions, these technical third parties may incur liability on the basis of a general principle of liability, which clearly is not acceptable. Their liability must therefore be defined so that it is neither general, nor overly limited.

It is important that not only health information hosts are to be covered by specific provisions requiring them to have prior authorization before being able to engage in their business or to create an obligation for interoperability and security in the their information systems, but also that technical third parties whose service plays a part in telemedicine are to be provided by an appropriate liability scheme.

4.5 Impact on liability law resulting from mobile telemedicine

The term of “Liability” in this paragraph refers to the state of being legally accountable for an act or omission. Patients using an mHealth device to treat a disease or illness could suffer from injuries from that same device. This could run into legal problems, featuring a product liability.

Product liability claims resulting from defective medical devices are usually based on one of the following:

- defectively manufactured medical devices
- medical devices with a defective design (even though properly manufactured), or
- defectively marketed medical devices.

Potential defendants could be among others manufacturer, testing laboratory, medical sales representative, doctor, hospital or clinic, retail supplier.

In such a context, as in many other technical sectors, , it appears essential to require a collection of all technical incidents that have occurred within the framework of mHealth practices. In fact, it is known that a series of incidents which may not be in and of themselves important may lead to more significant incidents, even accidents jeopardizing the life of the patient or the health care professional.

The mechanism for systematic and anonymous incident reports implemented in the air transport sector could inspire a separate mechanism for medical practice within the mHealth framework.

These last remarks are particularly striking in the light of a certain number of recent affairs that have moved public opinion and have been discussed within legal circles.

One might particularly think of the 450 patients who received radiation overdoses at the Epinal Hospital in France, at least seven of whom died. Despite the fact that this accident is not related to any mHealth practices, it is quite meaningful, however, with regard to the impact that accidents as such might have on the liability systems based on mobile telemedicine.

At the origin of the problem was incorrect software setting which resulted in overexposure of up to 20% of harmful nuclear radiation, resulting in irreparable consequences to the state of health of certain patients.

Beyond the liability of the three healthcare professionals, who may have been negligent by not following security protocols, the question arose as to the status of third party service providers, radiation physicists or computer scientists.

A national oversight committee to monitor radiation therapy interventions was created in France following this affair.

It is perhaps useful to examine this affair and, once again, ask the question whether there should be – at the European level or for each European State – a committee, an agency, or even a specialized body overseeing all mHealth activities. Such a body might have, counted among its missions, oversight of the correct functioning of devices, platforms, and systems based on incidents and reports that may have been generated thereof.

This is assuredly the price to be paid if mHealth in Europe is to gain the necessary confidence, without which it will not take off and have buy-in from all, beginning with the patients concerned.

5 Conclusion

In light of aforementioned, it seems necessary to promote an approach bringing existing laws in Europe closer together and recommending, when necessary, their adaptation to mHealth.

This is particularly the case with the rules governing access to the European market for medical devices which must be unified with the implementation of mechanisms for mutual recognition of national approvals since such approvals are given based on European standards or references or even better, the implementation of genuine harmonized European procedures. The same also applies for the protection of health information collected and processed using medical monitoring or care delivery systems over mobile networks and for medical practice itself delivered using these systems.

This work at harmonization must clearly be based on a more in-depth analysis of the specialized laws and regulations in force in Europe.

This harmonization effort, which appears to be widely felt in Europe, should be supported by three principles:

- First principle consists of the regulations that strengthen confidence in mHealth and maximize its beneficial effects for patients. mHealth with regard to this last point of

view presents specific characteristics to which any normative enterprise must pay special attention:

- it adds an additional layer of complication to the care delivery chain by involving new intermediaries and equipment which are not necessarily part of the healthcare domain;
- it involves a greater contribution by the patient in the caregiving act;
- it is based on the transfer of personal information, its storage, and sharing under circumstances and following procedures that expose practitioners to the risk of breaking their obligation for confidentiality and secrecy.

European States appear to be ever more geographically unified, forged by a shared history and connected by an attachment to legal principles constituting the basis of a single civilization. It should not be very difficult to find points of conversion between the national laws and regulations in order to reach the goals of harmonization of existing laws in Europe discussed above.

- Second principle is an active cooperation among the States which remains a fundamental principle within the European Union and which it may be possible to extend to the entire continent.
  No legislative effort may be undertaken without sincere cooperation by the States (to use the community vocabulary), in the same manner that no legislation may be effectively implemented if each of them does not provide its own contribution to this implementation and sanction for its respect.
  European countries have been engaging in this cooperation for a good many years. They find and defend shared positions in international organizations. Within the European Union they even have the procedure for mandating the Commission to represent them.
  The Court of Justice of the European Union has stated, on multiple occasions[22], the bases and mechanisms for a genuine foreign-policy for the Union. These bases and mechanisms are very supporting factors for progress in harmonization of current laws and regulations.

- The third principle is the principle of reciprocity that the European States, at least those that are members of the European Union, have applied in the domain of protecting personal information. This has led them not to allow exchanges or transfers of information with non-EU countries[23] if the countries towards which such personal information is transferred or with which it is exchanged do not offer an equivalent level of protection to that offered on European soil.
  As the rules for protecting personal information in Europe are surely one of the most perfected, by this means, European countries have forced all other countries in the world to significantly improve their national laws and regulations or to form agreements with them which guarantee Europeans adequate levels of protection. This mechanism has contributed to be quite tangible improvement in the level of protection for exchanges of personal information worldwide.

[22] As an example, see CJCE, 5 november2002, aff. C-466/98, C-467/98, C-468/98, C-469/98, C-471/98, C-472/98, C-475/98 et C-476/98, Commission c/ Royaume-Uni, Danemark, Suède, Finlande, Belgique, Luxembourg, Autriche et Allemagne

[23] More particularly under the framework of article 29 of the Data Protection Directive. On 27 February 2013, the Article 29 working Party published an opinion 02/2013 on “apps on smart devices”

This movement must be strengthened by extending it to the entire legal system governing mHealth for which Europe still appears to be lagging far behind compared to other areas of the world, notably initiatives made by the Food and Drug Administration in the United States.
Nothing justifies this delay especially since the proposed rules are compatible both with the freedom of commerce and with the development of innovation in all of its technical, economic, financial, commercial, and even legal or institutional dimensions.

For the mechanism surrounding such initiatives, Europeans would do well to be inspired by solutions achieved in other sectors, notably the aviation sector.

The Joint Aviation Requirements (JAR) and Joint Airworthiness Authority (JAA) the purpose of which is to minimize problems rose by standard certifications and to facilitate the movement of aeronautical products. These are European-inspired original and effective institutions, whose mechanism could be repeated and extended to the mHealth industries, more particularly to improve both the standardization process in the medical device domain and the interoperability of the various medical platforms conceived and manufactured according to different legal or regulatory requirements.

The experience of European agencies, particularly with regard to air traffic control or security, might lead Europeans to consider the creation of an office specialized in mHealth, as is today offered by the FDA whose policy is often provided as an example, notably with regard to the legal system governing mobile medical applications (MMA). A European Agency could unlock the full potential of mHealth, encourage innovation in healthcare in Europe and stimulate new deployment on the market.

This would provide better visibility with regard to the efficacy of medical devices in circulation and would contribute to improving technology, thereby reinforcing patient and physician trust in mHealth.

Given the coexistence of activities or interests as diverse as those found in mHealth, it would be a good to bring together one or more associations (The close association between an international organization, the International Civil Aviation Organization and an international association whose members are professionals in the sector, the IATA), joining industrialists, practitioners, and patients to define regulatory policies for implementation.

There are, therefore, more than one lesson to be drawn from these legal or institutional innovations which could easily be transposed to the mHealth sector and thereby actively contribute to its development in Europe and perhaps, beyond the borders of Europe.

References

Bajarin, T., Is Mobile the Future of Healthcare ?, PC Mag Sept.9, 2013

Balboni P. and Lafelice B., Mobile Cloud for Enabling the EU eHealth Sector, Regulatory Issues and Opportunities for Telecoms World, (ITU WT), 2011, Technical Symposium at ITU, Geneva, 51 - 56.

Bloomrosen M., Presentation to FDA Public Workshop – Mobile Medical Applications Draft Guidance, September 12-13, 2011

Bossi J., Comment organiser aujourd'hui en France la « protection » des données de santé, Revue de droit sanitaire et social 2010, p.208

Business Wire, Airstrip Technologies reçoit la marque CE pour ses solutions mobiles de surveillance du patient, 3 janvier 2012

Cerrato, P., What's Holding Back the Mobile Health Revolution ?, Information Week, Oct.2, 2013

Clapaud A., L'informatique en nuage simplifie les traitements de l'imagerie médicale, 01 net Entreprises, 7 septembre 2012

CNIL, Editeurs d'applications mobiles, quelles sont vos obligations au regard de la loi informatique et libertés ? (available : http//www.cnil.fr)

Congdon K., 4G m-Health : Possibilities and Pipe Dreams, Health Technology on Line, June 23, 2011

Conrad K., Making telehealth a viable component of our national health care system, Professional Psychology : Research and Practice 1998, 29 :525-526

Contis, M. (2010), La télémédecine : nouveaux enjeux, nouvelles perspectives juridiques, Revue de droit sanitaire et sociale, n°2, mars-avril 2010, p. 235.

Deleporte, B. et Sfez, B., Applications mobiles : du développement à la distribution, les droits et obligations du développeur, 27 septembre 2011, (avail. : www.dwavocat.com)

D., Chr., Apple et le contrôle des applications mobiles, EFF, 11 mars 2010

Eastwood, B. Healthcare IT Struggles to Keep Up With Mobile Health Demand, CIO, Aug, 27, 2013

Emord, J., FDA Rains on Mobile Medical App Parade, November 14, 2011 (avail. : http://newswithviews.com)

Ernst & Young, mHealth : Mobile Technology Poised to Enable a New Era in Health Care, Report Jan.2013

European Commission, Proposal for a Regulation of the European Parliament and Council on Establishing a Health Growth Programme, Com (2011) 709 final

Evans, J., How the Mobile Revolution Will Transform Healthcare Around the World?, Citeworld, Aug.22, 2013

Faure, H., Télémédecine: définitions et moyens techniques in Malek K. (2001), pp.1-5

FDA Regulation of Mobile health, Mobihealth News, Report, 2010

Felten, Ed. W., Nuts and Bolts of Network Neutrality, paper in process, Centre for Information Technology, Department of Computer Science and Woodrow Wilson School of Public and International Affairs, Princeton University

Gouvernement du Canada, Les accords/arrangements de reconnaissance mutuelle (ARM), 8 octobre 2012

GSMA mHealth, mHealth and the EU Regulatory Frame work for Medical Devices, 2013

GSMA mHealth, Understanding Medical Services Regulation for mHealth – A Guide to Mobile Operators, Feb.2012

GSMA mHealth and PA Consulting Group, Policy and Regulation for Innovation in Mobile Health, 2012

Gutman, R. How Mobile Tech Can Transform Health Care?, Tech Fortune, Sept.23, 2013

Holzinger and al, Chances of Increasing Your Health Awareness Through Mobile Wellness Applications, 2011

Hyman W., FDA Addresses Mobile Medical Apps, Standard and Regulatory, Medical Connectivity, July 20, 2011

Krupinski E.A., Chair Commentary: FDA Guidance on MMA, August 16, 2011, (avail.: http://siimshare.org)

Labordes P., La télésanté : un nouvel atout au service de notre bien-être – Un plan quinquennal éco-responsable pour le déploiement de la télésanté en France, Rapport au Ministère de la Santé et des Sports, Paris 2009.

Läkemedelverket, The Medical Products Agency's Working Group on Medical information Systems, Proposal for Guideline regarding Classification of Software based on Information Systems used in Health Care, 2 June 2009

Ledieu M-A, Interopérabilité des réseaux de communication, Communication Commerce Electronique, n°4, avril 2006, alerte 83

Liu P.R., Meng M.Q-H., Liu P.X., Tong F.F.L., Chen X.J., A telemedicine system for remote health and activity monitoring for the elderly, Telemedicine and e-Health, 2006, vol.12, n°6.

Mair F.S., Haycox A., May C., Williams T., A review of telemedicine cost-effectiveness studies, Journal of Telemedicine and Telecare, 2000, 6(Suppl.1):S1:38-40.

Malek K. (2001), Du bon usage de la télémédecine, Flammarion Médecine Science, Paris

Mamou Y., La télémédecine attise l'intérêt des industriels du high tech et de la santé, Le Monde, 13 novembre 2010.

Marghiset T., Les enjeux industriels de la télémédecine in Malek K. (2001), pp.6-8.

M-Health, le rendez-vous des telecoms et de la santé, 15-16 novembre 2011

Michael, m-Health : FDA Gives Okay Sign to GE Healthcare's Groundbreaking Mobile X-Ray Platform, Mobile Marketing Watch, June 27, 2011

Poitevin B. et Gelles V., Les applications mobiles et le respect de la loi « Informatique et Libertés », Les Echos, 9 octobre 2012

Rapp L., Does a Legal Principle regarding Net Neutrality Exist? The Journal of Regulation, 2011, I.2.6

Roine R., Ohinmaa A., Hailey D., Assessing telemedicine: a systematic review of the literature, Canadian Medical Association Journal, 165 (6), 18 sept 2001, pp.765-71

Ruskin P.E., Silver-Aylaian M., Kling M.A., Reed S.A., Bradham D.D., Hebel J.R., Barrett D., Knowles F., Hauser P. (2004), "Treatment outcomes in depression: comparison of remote treatment through telepsychiatry to in-person treatment", American Journal of Psychiatry, 161:8

Saltonstall P. L, FDA Safety and Innovation Act: A Step Forward for Patients with Rare Disease, (available : http://www.biotech-now.org)

Sanni Yaya H., Raffelini C., Des souris et des médecins, Publibook 2007, Paris

Simon P., Acker D., La place de la télémédecine dans l'organisation des soins, Direction de l'Hospitalisation et de l'Organisation des Soins, Rapport Mission Thématique 2008, n°7/PS/DA

Slobodkin G., Legislation to Call for Creation of FDA Office of Mobile Health, Fierce Mobile Healthcare, September 28, 2012

Sood S., Mbarika V., Jugoo S., Dookhy R., Doarn C. R., Prakash N., Merrel R. C., What is telemedicine? A collection of 104 peer-reviewed perspectives and theoretical underpinnings, Telemedicine and e-health 2007 vol.13, n°5, pp.573–59

Sordet, E. et Milchior R., Le Cloud Computing, un objet juridique non identifié? Communications Commerce Electronique, n°11, Novembre 2011, Etude 20

Thompson, M., Frictionless Health : The Top 5 Reasons the Future of Healthcare Will be Mobile, Huffington Post, Oct.15, 2013

Touré, H. I., Speech by the ITU Secretary General, mHealth Summit, 6 December 2011

Vejvelka, J., European Mobile Health Initiative – Background document, September 2012

Vollebregt, E., eHealth Applications and Websites developed by Clinicians: There are Rules for That! Eucomed, 7 June 2011

Vollebregt, E., European Union: FDA Draft Guidance on Mobile Medical Applications, 27 July 2011 (available: http://www.mondaq.com)

Wicklund E., FDA Mobile Medical App. Guidelines on the Way, Healthcare Finance News, July 12, 2012

Wicklund E., America Well Make a Play for Mobile Healthcare, mHealth News, Oct.11, 2013

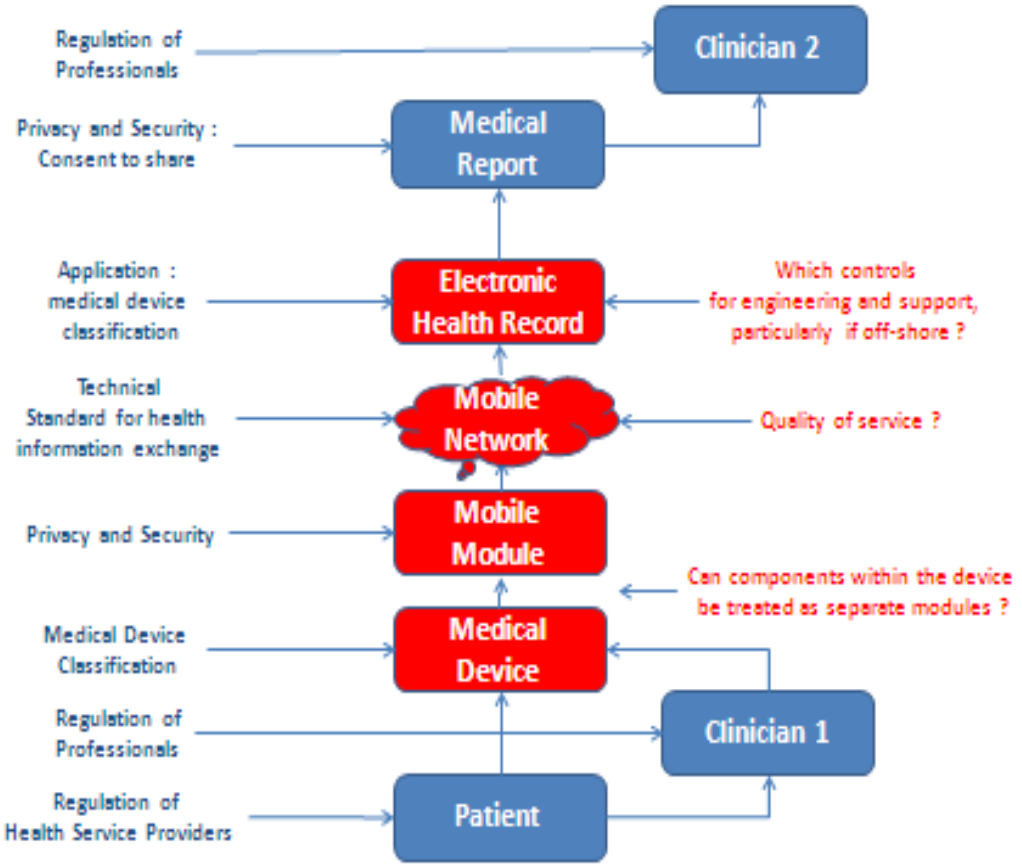
Workman, B., The Explosion in Health Apps, And How They're Disrupting the Gigantic, Lethargic Health Care Industry, Business Insider, Sept. 13, 2013

World Health Organization, Legal Framework for e-Health, Global Observatory for e-Health series, Vol.5, 2012

The Digital Dimension of Healthcare, Report of the Digital Innovation in Healthcare, Working Group, 2012

APPENDIX A

Key Legal Challenges
(Adapted from GSMA mHealth and the EU Regulatory Framework for Medical Devices, Report 2012)



APPENDIX B

CE Marking