Healthcare Meets Smart Wireless – and the Law?

Michael Isler

Biographical Information

Title: Dr

Name: Michael Isler

Position or Title: Senior Associate

Firm or Place of Business:

WENGER PLATTNER Attorneys-at-Law

Address: Goldbach-Center, Seestrasse 39, CH-8700 Küsnacht-Zürich, Switzerland

Phone: +41 43 222 38 00

Fax: +41 43 222 38 01

E-Mail: michael.isler@wenger-plattner.ch

Primary Areas of Practice: ICT, IP, Life Sciences

Education: University of Zurich

Recognition: Who'sWhoLegal Switzerland 2013 (Technology, Media and Telecommunications)

Membership in Associations, Committees, etc.: ITechLaw, Institut für Gewerblichen Rechtsschutz (INGRES)

Introduction[1]

"The average [physician] appointment lasts seven minutes in the US. And usually the patient is waiting for an hour. So it's a very inefficient system. With digital tools, if you're seeing someone who has high blood pressure and blood-sugar problems, a lot of the data that's relevant could be sent through the Web before or during the visit. That's different from today, when you and your doctor don't have data available during the visit."[2]

As is apparent from the above quote, mobile health is about to revolutionize medical practice. Service providers', physicians' and patients' reliance on mobile medical applications (apps) to transfer important patient information is steadily increasing.[3] It is not only the new gadgets that are shifting

[1] Special thanks go to David Hoffmeister of Wilson Sonsini Goodrich & Rosati (Palo Alto) for his valuable comments and expert advice on US regulatory aspects, and to Axel Ernst of the University Hospital of Basel for the insights provided into the Hospital's enterprise mobile management.

[2] Dr Eric Topol, *in:* Wall Street Journal, 16 April 2012, The Wireless Revolution Hits Medicine.

[3] FRANKO / TIRRELL: Smartphone App Use Among Medical Providers in ACGME training programs, J Med System 2012, 3135–3139 (stating that over 50% of all physicians surveyed reported using a medical app in their practice); D4 RESEARCH: Regulation of Health Apps: A Practical Guide, February 2012, p. 11 (stating that 30% of the UK doctors run work related software/apps on their smart mobile devices); WORLD HEALTH ORGANIZATION: mHealth, New Horizons for Health Through Mobile Technologies, Global Observatory for eHealth Series, Vol. 3, 2011. Besides, hospitals start deploying enterprise app stores listing recommended mobile medical apps within an overall mobile access environment to electronic health records.

paradigms, but it is the ubiquity and mobility of medical data by means of wireless connectivity. Instead of collecting and processing patient information during specific and scheduled doctor appointments, medical data are collectable over the continuum of time and may be processed and stored in technology-neutral (cloud-based) platforms, where they are potentially made available to a variety of healthcare professionals and patients alike, be it for purposes of diagnostics, treatment, monitoring, teaching and research, or administration.[4]

Many app developers and platform providers are not well versed in the regulatory environment that significantly impacts the medical device industry, and quite a few of these developers are completely unfamiliar with the bounty of regulatory requirements that are piercing the healthcare sector. The present paper provides an overview and analysis on the regulations and privacy requirements relevant to medical device mobile app manufacturers. It will also shed a light on liability risks in the event said requirements are not complied with.

[4] See by example WILTZ: Qualcomm Life and WebMD Partner to Bring mHealth Data to Consumers, DeviceTalk, 5 March 2013 (http://www.mddionline.com/blog/devicetalk/qualcomm-life-and-webmd-partner-bring-mhealth-data-consumers).

1. The Advent of Mobile Medical Apps

One of the first mobile medical applications to receive clearance from the US Food and Drug Administration (FDA) as a medical device in 1997 was likely a telephone electrocardiographic (ECG) system that transmitted received and recorded ECG data to a personal digital assistant.[5] 15 years later, the predominant part of the mobile medical applications for which FDA clearance is sought are traditional medical device systems consisting of a sensor applied to a patient for a specific medical purpose and wireless connectivity to a dedicated mobile platform enabling further analysis of the patient data or controlling of the sensor.

However, the real boom of mobile medical applications started with the increasing penetration of smartphones and tablets (smart mobile devices) together with the vast deployment of wireless broadband access. Today, almost 15'000 mhealth apps are available on the iTunes® app store, which is about 4% of the total app population.[6] Only very few of them enjoy FDA clearance[7] or have been examined for conformity with

[5] 75 FDA Regulated Mobile Medical Apps, mobihealthnews 2012 Report, p. 5 referring to (510(k)) K971650, 4 December 1997, http://www.accessdata.fda.gov/cdrh_docs/pdf/K971650.pdf.

[6] RRESEARCH2GUIDANCE: Global mHealth Market Report 2011–2015.

[7] See overview in 75 FDA Regulated Mobile Medical Apps, mobihealthnews 2012 Report, p. 16–37; MCNAIR: FDA Facing Huge Task in Regulating Mobile Medical Apps, 9 August 2011,

essential requirements under European medical device regulations.

The "app economy" created new and generally low-threshold market opportunities for the IT industry in the healthcare sector. A typical and widespread example of an easy-to-develop and easy-to-use mobile medical app is a medication dosage calculator for pediatrics, where the input of the patient's weight and age delivers the drug dosage to be dispensed.[8] Yet the health implications of a miscalculated drug dosage can be serious. In October 2011, a "Rheumatology Calculator" app was withdrawn from the market because it gave incorrect values for the calculation of a drug dose used to treat rheumatoid arthritis patients.[9]

Smart mobile device features now include embedded sensors for recording pictures or sounds and for tracking speed and direction of movements (gyroscope, digital compass, and accelerometer), as well as geo-positioning systems, which are all capable of being applied for medical purposes. This tech-

http://www.cerner.com/blog/fda_facing_huge_task_in_regulating_mobile_medical_apps/.

[8] BANKER: PediCalc medical app, customizable pediatric drug dosing at the touch of a button, *in:* iMedicalApps, 9 February 2012, http://www.imedicalapps.com/2012/02/pedicalc-medical-app-pediatric-drug-dosing/.

[9] See e.g. publication of 7 November 2011 in the recall list database of medical devices of the Swiss Agency for Therapeutic Products, http://www.swissmedic.ch/rueckrufe_medizinprodukte/archiv/index.html?lang=en&RlArchiv=2011-07&RlArchiv=2011-07.

nological evolution renders the app ecosystem even more attractive, but also more hazardous, for healthcare. In this respect, a recent survey reporting diagnostic inaccuracy of smartphone apps for automated melanoma detection received significant media attention.[10]

Connecting external patient sensors that interface with software downloaded onto smart mobile devices enhances the latter's potential in health service delivery even more by virtue of the processing power of the smart mobile device, and the instant access to the mobile network.[11] With these possibilities, a great variety of mainly diagnostic and monitoring applications are capable of converging into one single interfacing mobile platform. An example of such use is a heart monitor that snaps onto a smart mobile device and records, displays, stores and transfers patient ECG rhythms through an app installed on the device.[12] Glucose meters working with an app installed on a smartphone are another popular use case.[13]

[10] WOLF / MOREAU / AKILOV / PATTON /ENGLISH / HO / FERRIS: Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection, *in:* JAMA Dermatology 2013.

[11] GSMA: Understanding Medical Device Regulation for mHealth: A Guide for Mobile Operators (February 2012), p. 6.

[12] See e.g. AliveCor® Heart Monitor for iPhone® (www.alivecor.com).

[13] See e.g. iBGStar® Glucose Meter and Diabetes Manager App (www.ibgstar.com).

2. The Players and their Roles

Development, distribution and operation of mobile medical apps involve many stakeholders. It is important to keep in mind this fragmented landscape when assessing regulatory requirements, privacy and liability schemes:

- The main focus lies on the app manufacturer. The *app manufacturer* or app owner is responsible for the design, development, testing, regulatory clearance and marketing of the programs and may also maintain a cloud-based data base or health data processing platform interfacing with the app within a client-server architecture.
- The *app distributor* makes the app available on a download platform.
- The *device and OS manufacturer* delivers the smart mobile device and the operating system on which the app is installed and running. Examples include Apple® (makers of the iPhone, iPad, iPod touch devices) or Google® (makers of the Android operating system).
- The *app service platform provider* may either be identical or under the control of the app owner, or it may offer an independent service by way of collecting, aggregating and making available medical data collected from various mobile sources.

- The *network operator* eventually assumes the task of transmitting the data to the platform where the recipients can access them, i.e. usually the *patient* or the *healthcare provider*, unless there is isolated processing of data solely within the app installed on the smart mobile device itself.

3. The Medical Device Regulation

a) The Legal Definition of Medical Device

The main regulatory issue facing many mobile medical apps is whether these software programs are or can be regulated as medical devices by regulatory authorities, such as the U.S. Food and Drug Administration (FDA) in the relevant markets.

The starting point of the analysis is the definition of a medical device under pertinent legislation and statutory authority. Under US federal law, a medical device is deemed a product that meets the definition of "device" in Section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&D Act).[14] In the European Union, the national medical devices regulations are harmonized by virtue of several directives, including the

[14] 21 U.S.C. 321(h).

Medical Device Directive (MDD),[15] where Article 1.2 (a) provides for a Community wide definition of "medical device".

Pursuant to said provisions, a medical device is practically any kind of product, appliance or contrivance, including (stand-alone) software,[16] which is *inter alia* intended by the manufacturer to be used for the purpose of diagnosis, prevention, monitoring, treatment or alleviation of disease or other human condition.

The regulatory framework also applies to accessories of medical devices. These are articles that fall under the jurisdiction of regulatory authorities when used or intended to be used in conjunction with a medical device. The notion of accessories is particularly relevant to software which has not stand-alone functionality as a medical device, but in combination with a medical device. Under the EU regime, the definition of accessories is rather narrow, comprising elements that are specifically intended by the manufacturer to be used together with a medical device to render the intended use of such device at all possible.[17] The definition applied by the FDA is

[15] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJ L 169, 12 July 1993, p. 1, as amended.

[16] See Article 2.1 (a).of the Directive 2007/47/EC of the European Parliament and the Council of 5 September 2007, OJ L 247, 21 September 2007, p. 21, amending *inter alia* the definition of medical device in the MDD accordingly by explicitly introducing software.

[17] Article 2.1 (b) MDD.

broader: an intention that the accessorial element be attached to or used in conjunction with a medical device suffices. An example of an accessory falling under both approaches may be a mobile medical app intended to control a blood pressure cuff.

Looking at the pertinent definitions, it becomes apparent that the *intended use* of a mobile app is pivotal in determining whether it meets the definition of a medical device under the different regulatory regimes. Pursuant to Article 1.2 (g) MDD, intended purpose means the use for which the device is intended according to the data supplied by the manufacturer on the labeling, in the instructions and/or in promotional materials. The intended use of an app can be determined from explicit or implied promotional and advertising claims and the objective intent of the manufacturer.[18]

All this being said the regulation of mobile medical apps is nothing new. From the perspective of the lawmakers and regulators, there is no difference if the intended purpose is pursued by a software application installed on a smart mobile or on a more traditional dedicated medical device.

[18] GARVIN: The Legal Perspective of mHealth in the United States, in: Journal of Mobile Technology in Medicine 2012, pp. 42–45, p. 43.

b) *The FDA Draft Guidance for Mobile Medical Applications*

In an attempt to bring about more clarity to the app industry, the FDA in July 2011 issued its Draft Guidance for Mobile Medical Applications (MMA Draft Guidance).[19] The purpose of the MMA Draft Guidance is to inform app manufacturers and distributors about how the FDA intends to apply its regulatory oversight on mobile medical apps.

On general terms, pursuant to the MMA Draft Guidance the FDA will apply regulatory oversight to mobile apps that are either used as an accessory to a regulated medical device or if they transform a smart mobile device into a regulated medical device.[20] Beyond this commonplace, the MMA Draft Guidance makes a great achievement in analyzing the various purposes of mobile medical apps and provides numerous instructive examples. However, the document is not very well structured and therefore difficult to navigate through.

The first main category encompasses medical device accessories, which is then divided into three sub-categories: (i) mobile medical apps that are connected to an existing medical device for the purposes of controlling such device, (ii) medical device data systems (MDDS) which display, store,

[19] Http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263280.htm.

[20] MMA Draft Guidance, p. 7, 10.

analyze or transmit patient-specific data retrieved from a medical device in its original format, and (iii) mobile medical apps that analyze or interpret such medical data by creating alarms or recommendations. An example of the first sub-category is an app that controls inflation and deflation of a blood pressure cuff. An example of a mobile MDDS is an app that displays data from bedside monitors on the screen of a smart mobile device (like an iPad). An example of the third sub-category is an app analyzing blood glucose readings to help manage diabetes.[21] The distinction between these sub-categories is important, because MDDS are subject to the risk class with the lowest control level, whilst the apps controlling another medical device or processing medical device data typically follow the regulatory classification of the parent device.

The second category of regulated mobile medical apps comprises those apps transforming the smart mobile device itself into a medical device, either by (i) using an embedded or externally connected sensor for medical purposes, or (ii) by way of analyzing or interpreting manually entered patient data for the purposes of providing a patient-specific result, diagnosis or treatment recommendation. Examples of those

[21] All examples taken from MDA Draft Guidance, p. 13 *et seq*.

sub-categories are the ECG app and the drug dosage calculator referred to above.[22]

The MMA Draft Guidance also provides examples of apps that are not regulated as medical devices, which help in drawing the demarcation line between regulated mobile medical apps and apps with a general health connotation that are not subject to regulatory oversight. For example, functional features that do not meet the threshold of a regulated mobile medical app include provision of mere medical information (in other words, a library function) or training aids, general health and fitness apps, administrative tools, archiving systems, or generic aids without medical claim.[23] Moreover, component manufacturers such as the smart mobile device and OS manufacturers (like Apple® or Google®) are exempt from medical device regulation,[24] at least as long as these smart mobile devices are not being marketed, promoted or advertised by the manufacturers as pursuing a medical purpose.

[22] See footnotes 8 and 12.

[23] MMA Draft Guidance, p. 10 *et seq*.

[24] MMA Draft Guidance, p. 10.

c) *The MEDDEV Guidance Document on Stand Alone Software*

The FDA guidance is not perfect, but so far is the only sophisticated official guidance document covering specifically the topic of mobile medical apps. The national regulatory authorities in Europe have remained fragmented, inconsistent and remarkably passive in the area, even though the European Commission's DG Health and Consumer passed the final version of the non-binding Medical Devices Stand Alone Software Guideline in January 2012.[25] The scope of application of MEDDEV 2.1/6 embraces any kind of stand-alone software and may as such serve as a compass in regulating mobile medical apps within Europe. MEDDEV 2.1/6 distinguishes in the same way as the MMA Draft Guidance between software serving as an accessory to a regulated medical device or transforming the platform on which it is stored into a medical device itself.[26] In this respect, it is remarkable that the narrow definition of accessory set forth in Article 2.1 (b) of the MDD is considerably broadened, possibly inspired by the concept adopted by the FDA. It can therefore be safely

[25] Medical Devices Guidance Document on the Qualification and Classification of Stand Alone Software Used in Healthcare (MEDDEV 2.1/6), http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf.

[26] See decision-tree in MEDDEV 2.1/6, p. 9.

argued that the threshold criteria are practically identical on both sides of the Atlantic.[27]

d) Who Bears Regulatory Responsibility for Commercializing an App?

Both under US and EU harmonized medical device law and regulations, the responsibility for securing commercial clearance and compliance of the medical device with regulatory requirements lies with the manufacturer. A manufacturer is the person controlling the functionality and labeling and intended use of the device before it is placed on the market under its own name, or any company marketing OEM devices by attaching its own brand thereon.[28] On the other hand, component manufacturers such as mobile device and OS manufacturers[29] and mobile network operators[30] are in principle exempt from medical device regulation.

With respect to app distributors, the situation in the USA and Europe is slightly different. The FDA does not consider app distributors to be manufacturers.[31] The FDA looks to distrib-

[27] THOMPSON / VOLLEBREGT: Mobile Medical Apps Guidance: What's Good for the US is Good for the EU, Scrip Regulatory Affairs, October 2011, p. 10–11.

[28] Article 1.2 (f) MDD; MMA Draft Guidance, p. 9 and 10.

[29] MMA Draft Guidance, p. 10.

[30] MEDDEV 2.1/6, p. 23.

[31] MMA Draft Guidance, p. 8 and 9.

utors to cooperate with app manufacturers in post-market duties, such as performing corrections and removal actions.[32] Under the EU regime, the manufacturer without establishment in the Community must appoint an authorized representative within the EU, who assumes the manufacturer's responsibilities.[33] Failure in so doing entails that the app distributor as importer of the app into the Community may be deemed manufacturer.[34] Further, distributors are obliged to co-operate in market surveillance measures along the supply chain.[35]

From a practical perspective, it is recommended that the app manufacturer makes the taking into use of the app dependent upon registration of the users on a web-based app service platform, in order to establish a direct link for possible warnings or product updates.

[32] MMA Draft Guidance, p. 16.

[33] Article 1.2 (j) MDD.

[34] See e.g. § 5 of the German Act on Medical Devices (*Medizinproduktegesetz*), BGBl. I p. 2192, as amended.

[35] Article 19.1 of Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93, OJ L 218, 30 August 2008, p. 30.

e) Conclusions

The qualification of a mobile app as a medical device entails a set of pre- and post-market duties that may impose heavy and unexpected burdens on app developers/manufacturers. First, it entails adherence to sector specific manufacturing and programming standards, miles away from any kind of "agile" styles. Second, the way to market is generally paved with a preapproval application to the FDA or a conformity examination under the EU regime. Last, post-market surveillance duties, including robust quality assurance management, complaint handling, adverse event reporting (covigilance), and product recall procedures, apply. It is therefore paramount to unambiguously assign the manufacturer's role in the app development contractual framework. It may be worth considering for app developers to look for a role as a subcontractor and leave the control over design and functionality to a more experienced partner.

Enforcement of the regulatory requirements pertaining to medical devices in the mobile app landscape seems to be an almost impossible task to accomplish in view of the rapid evolution of the mobile medical app landscape. The amount of adulterated mobile medical apps by far outweighs the few that are compliant. An exclusion of low-risk mobile medical apps from regulatory oversight is likely the only way to mitigate the apparent enforcement dilemma.

4. Data Privacy and Data Security

a) The Relevance of Data Privacy and Data Security in the App Operating Environment

The complex app operating landscape is particularly hazardous when it comes to the protection of personal health data. The close interlocking of mobile medical apps between the smart mobile devices hardware and OS on the one side and the internet on the other side allows such apps to collect users' health data through a variety of sensors embedded or attached to the smart mobile device. The typical data flow generated by a non-trivial mobile medical app involves numerous actors. Isolated data protection measures are thereby easily frustrated if the chain of multiple actors includes just one weak link.

b) Overview on Recent Activities

Whilst the FDA is the undisputed pacemaker in mobile medical app regulation, personal data processing by mobile apps has become subject to enhanced scrutiny in Europe and USA likewise. Recent activities include the adoption by the Article 29 Data Protection Working Party[36] of Opinion 02/2013 on Apps on Smart Devices on 27 February 2013 and the issuance by the Federal Trade Commission (FTC) of its Report on Mobile Privacy Disclosures in February 2013.[37] Simultaneously, Appthority in a test of the 100 most popular free apps concluded that the majority of the apps are associated with substantial security risks and privacy issues.[38] More specifically on mobile medical apps, a review of eight randomly selected apps conducted in Germany in autumn 2012 revealed a high degree of nontransparent data processing and unencrypted sensitive health data disclosures.[39]

[36] The Article 29 Working Party (WP29) was set up under Article 29 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive), OJ L 281, 23 November 1995, p. 31, as amended. It is composed of a representative of the supervisory authorities designated by each Member State and of a representative of the authorities established for the Community institutions and bodies, and of a representative of the Commission, and is supposed to act independently. Opinion 02/2013 is available on http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

[37] The Federal Trade Commission is endowed with enforcement authority to take law enforcement action to make sure that companies live up their privacy promises pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, as amended, since violation of privacy notices may constitute a deceptive trade practice. The Mobile Privacy Disclosures Report is available on http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

[38] Appthority App Reputation Report – February 2013, https://www.appthority.com/appreport.pdf.

[39] ALBRECHT / PRAMANN / NOLL / JUNGNICKEL / VON JAN: *Datensicherheit von Medical Apps – eine Stichprobe*, 10 October 2012,

c) The European Data Protection Framework

Under the regime of European data protection directives as transposed into the national laws of the Member States, two features of mobile medical apps are pivotal to the present analysis.

First, the smart device is terminal equipment within the meaning of the ePrivacy Directive.[40] Pursuant to Article 5.3 of the ePrivacy Directive, widely known as the "cookie rule", the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing. Storage or access is solely exempted from the consent requirement if inevitable either for the purpose of carrying out the transmission of communication over an electronic communications network, or in order for the provider to offer a technical service functionality explicitly requested by the subscriber or user. No such implied consent would apply for the storing of or the

http://plrimedapplab.weebly.com/uploads/7/4/0/7/7407163/stichprobe_datensicherheit_von_medical_apps_v17.pdf.

[40] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31 July 2002, p. 37, as amended.

gaining of access to health data (e.g. health data collected by an external sensor) already stored on the device. However, mere transit of health data by virtue of the app installed on the device directly to an external service platform without involving any storage on the device itself would not be subject to the consent requirement.

Whilst many provisions of the ePrivacy Directive apply only to providers of publicly available electronic communications services or networks, the requirements enshrined in Article 5.3 must be heeded by every entity that places on or reads information from smart mobile devices, including mobile app manufacturers.[41] Further, the consent requirement is not limited to personal data; information can be any type of data stored on the device.[42] Hence, whenever the mobile app allows collection of data stored on the device through an interface, such as location, identity of the data subject or identity of the phone, the consent requirement applies.

Second, personal health data is considered sensitive personal data the processing of which is prohibited by virtue of Article 8.1 of the Data Protection Directive, unless – among other exceptions – (i) the data subject has given his or her explicit consent, or (ii) the data processing is required for medical purposes, provided that such data are processed by a health

[41] WP29 Opinion 02/2013, p. 7.

professional subject to an obligation of professional secrecy.[43] Consent must be free, informed and specific:

- *free* means that the user has the option of accepting or refusing processing of personal data;

- *informed* means that the user be aware of the categories of data and processing purposes before rendering consent;

- *specific* means that the expression of consent must relate to the processing of a particular data item or a limited category of data processing. In other words, consent should be given in a granular, not global, manner.[44]

With respect to other data protection requirements relevant to mobile medical apps, general principles apply. These include adherence to the principles of purpose limitation,[45] proportionality[46] and transparency[47] as well as the safeguarding of data confidentiality and security, e.g. by way of implementing sophisticated authentication procedures and encrypted transport of data.[48] In the event that data is processed by a third party on behalf of the data controller, which is the case

[42] WP29 Opinion 02/2013, p. 7.

[43] Article 8.2 (a) and 8.3 of the Data Protection Directive.

[44] WP29 Opinion 02/2013, p. 15.

[45] Article 6.1 (b) of the Data Protection Directive.

[46] Article 6.1 (c) of the Data Protection Directive.

[47] Articles 10 and 11 of the Data Protection Directive.

[48] Articles 16 and 17 of the Data Protection Directive.

when the mobile app is embedded in a client-server architecture hosted by a third-party provider, the data controller must ensure by virtue of an agreement that the data processor acts in accordance with his or her instructions and provides sufficient guarantees in respect of security and organizational measures governing the processing to be carried-out.[49] Last, transfer of data to third countries without adequate level of data protection is only permissible if an adequate level of data protection exists at the place of destination.[50] Particularly from the viewpoint of the EU, the United States do not avail of an adequate level of data protection. Hence, cross-border data transfer are solely permitted if the US-based data processor is certified under the EU-US safe-harbor framework,[51] the data subject has given his or her explicit consent[52] or an adequate level of protection is assured by means of contractual guarantees.[53]

The requirements of the Data Protection Directive must be heeded by the data controller, i.e. the person who alone or jointly with others determines the purposes and means of the processing of personal data.[54]

[49] Article 17.2 and 17.3 of the Data Protection Directive.

[50] Article 25 of the Data Protection Directive.

[51] See http://export.gov/safeharbor/.

[52] Article 26.1 (a) of the Data Protection Directive.

[53] Article 26.2 of the Data Protection Directive.

[54] Article 2 (d) of the Data Protection Directive.

According to Article 4.1 (a) of the Data Protection Directive, if the processing of personal data is carried out in the context of an establishment of the data controller on EU territory, the data protection law of the Member State of such establishment applies. However, in case the controller is not established in the Community and makes use of equipment situated on the territory of an EU Member State, the national law of such Member State applies. Since the smart mobile device is instrumental in the processing of personal data from and about the user, the Article 29 Working Party considers this criterion usually fulfilled.[55] This would entail that the offshore app manufacturer needs to comply with the data protection laws of each and any Member State where the app is being made available, whilst an establishment of the manufacturer within the EU reduces the level of compliance to the jurisdiction of one single Member State only.

According to the fairly questionable view of the Article 29 Working Party the app manufacturer qualifies *per se* as data controller.[56] However, this is only the case where patient's data are actually being made available to the app manufacturer or a person under its control, but irrelevant where all data processing operations are carried-out locally on the device without further influence or control by the app manufac-

[55] WP29 Opinion 02/2013, p. 7.

[56] WP29 Opinion 02/2013, p. 9.

turer.[57] If third-parties such as the device and OS manufacturer or the app distributor are capable of retrieving personal data processed on the app through APIs, these would become data controllers with respect to such data, but not the app manufacturer itself. Currently, there is no enforceable privacy by design obligation enshrined in European data protection legislation with respect to the programming of software.[58] However, if the app is designed to store or access data on the smart mobile device, Article 5.3 of the ePrivacy Directive comes into play irrespective of whether the app manufacturer actually gains control over such data. Hence, Article 5.3 of the ePrivacy Directive may be regarded as the nucleus of a privacy by design requirement.

If the mobile medical app is being used by a healthcare provider, this person will also qualify as a data controller. In this respect, healthcare providers should be aware that any disclosure of personal health data to a third-party may entail a breach of professional secrecy obligations and constitute a criminal offence. Medical practitioners should therefore abstain from using mobile medical apps when it is unclear if patients' identifiable data is processed in an insecure way be-

[57] According to WP29 Opinion 02/2013, p. 10, the responsibilities of the app manufacturer in such case will be "considerably limited".

[58] With respect to the construction of terminal equipment, the Member States may adopt measures to ensure compatibility with prevailing data protection requirements (Article 14.3 of ePrivacy Directive).

yond the smart mobile device. Healthcare providers such as hospitals that recommend medical apps on their enterprise app store should consider this aspect as part of their selection criteria.

d) The Privacy and Security Rules Under HIPAA and HITECH Act

In the United States, privacy and data security requirements in the healthcare sector are usually discussed in the context of the Health Insurance Portability and Accountability Act (HIPAA),[59] as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH Act).[60] HIPAA contains privacy, security and breach notification rules to be heeded in the first place by so-called covered entities, which are health plans, health care clearinghouses, and health care providers (physicians) who transmit personal health information in electronic form.

A business associate is an entity that is provided access to or handles protected health information on a covered entity's behalf. The distinction between covered entity and business associate reminds somehow of the dichotomy between data controller and data processor under EU data protection law.

[59] 42 U.S.C. § 300gg, 29 U.S.C § 1181 *et seq*.

[60] 42 U.S.C. 1320d *et seq*.

The app manufacturer may qualify as a business associate in case the medical app's connected server environment is used by healthcare providers to process protected health information. Importantly, and in contrast to the EU legal framework focusing on controller's responsibility, business associates are now bound to comply with the Privacy, Security and Breach Notification Rules by virtue of the HITECH Act.

On the other hand, a mobile app that is intended to be used by a patient without provision of patient health information from a health care practitioner is not governed by HIPAA, because there is no covered entity involved. This is even the case if the patient's health information is transmitted to a physician by means of a web interface.[61]

5. The Liabilities

In case of-non-compliance with medical device regulations, the liability regime provides for strict criminal liability and civil penalties under Section 303 of the FD&C Act (e.g. the provisions for misbranding and adulteration). In Europe, criminal liabilities are set forth in the various Member States' legislations and may considerably differ.

[61] GREENE: When HIPAA Applies to Mobile Applications, in: mobihealthnews, 16 June 2011, http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/.

Non-compliance with medical device regulations may also be deemed an act of unfair competition under applicable laws. Achievement of regulatory compliance is cost-intensive and time consuming, and those adhering to the standard have a legitimate interest in insisting on a level playing field for all participants in the mobile medical apps marketplace. Under this aspect, it is expected that competition may increasingly assume a pro-active role in enforcing regulatory compliance by warning or blaming app developers that do not adhere to prevailing regulatory requirements.

Last, it should be noted that Apple's iPhone Developer Program License Agreement since June 2009 provides for a special section putting the regulatory onus on the app developers. Under the section labeled "Regulatory Compliance", Apple obliges the developers to fulfill any applicable regulatory requirements, including full compliance with all applicable laws, regulations, and policies related to the manufacturing, marketing, sale and distribution of the app in the United States and any other jurisdiction where the app is being made available. However, the developers must not seek any regulatory marketing permissions or make any determinations that may result in any Apple products being deemed regulated or that may impose any obligations or limitations on Apple. Google Play (previously Android Market) does not impose similar obligations on the developers.

With respect to data protection rules, the liabilities under the European data protection regimes are not deterring, but reputational damage may be substantial. HIPAA and HITECH Act on the other hand impose substantial penalties on non-compliant covered entities and business associates.

6. Outlook

a) Medical Device Regulation Policies

Now that awareness of regulatory implications of mobile medical apps is steadily increasing in the relevant market circles, the next couple of years will be earmarked by struggle to balance public safety considerations versus furtherance of innovation. The topic was worth a three days hearing scheduled end of March 2013 by different U.S. House of Representatives Energy and Commerce subcommittees, where some lobbyists of the technology sector advocated for a detachment of regulatory oversight from the FDA. This is not a new desire; there have been earlier attempts to subject FDA's regulatory oversight on mobile medical apps to a special Office for Wireless Health within the FDA with the purported objective to help clarifying and simplifying existing regulations.[62] This is an unrealistic expectation though. With re-

[62] 75 FDA Regulated Mobile Medical Apps, mobihealthnews 2012 Report, p. 15; GARVIN: The Legal Perspective of mHealth in the United

spect to the evolution of medical device regulations, FDA is and will remain the pacemaker in shaping the mobile medical app regulatory environment. The MMA Draft Guidance may be converted into a finalized version still in 2013.

Section 618 of the Food and Drug Administration Safety and Innovation Act (FDASIA) passed in 2012 further requires the Secretary of Health and Human Services to post a report that contains a proposed strategy and recommendations on an appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, which promotes innovation, protects patient safety, and avoids regulatory duplication. This report is required to be published by January 2014. In the European Union, the European Commission is prospected to issue a similar document in 2014 in the format of a Green Paper on mhealth and health in wellbeing apps as part of the Commission's eHealth Action Plan 2012–2020.[63]

Further, the European Commission's proposal for a Medical Device Regulation (MDR)[64] is of some interest. It aims at replacing the current mosaic of harmonized national laws by

States, in: Journal of Mobile Technology in Medicine 2012, pp. 42–45, p. 44.

[63] COM (2012)736 final, p. 9 and 10, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9156.

[64] COM(2012) 542 final, http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf.

a uniform legislative instrument. If eventually adopted, it will significantly enhance uniform application of Community medical device regulations within the EU Member States. For the purposes of mobile medical apps, the definition of accessories is of considerable importance. According to the proposal, contrary to the current state of legislation, but in line with MEDDEV 2.1/6 on stand alone software, a mere support function of the accessory will suffice to succumb it to the regulatory framework. However, since there will be no unified enforcement authority under the MDR, regulatory oversight will remain scattered and relatively weak compared to the powers vested in the FDA.

Whilst the FDA announced to use sound enforcement discretion with respect to non-critical apps, if the adulterated app is intended to treat or diagnose a medical disease or condition and presents risks to patients, one can expect that the FDA will make some examples of its determination in the market. As usual, this will have an automatic spill-over effect on Europe. If a mobile medical app is required to undergo regulatory scrutiny in the USA, the conformity examination required for clearance on the European market will go practically hand-in-hand. Uncertainties will remain for quite some time though. It is naïve to think that once the MMA Guidance finalized, the requirements will be crystal-clear.

b) Data Protection Policies

The proclamation of the EU Commission set forth in the eHealth Action Plan[65] to foster ehealth, telemedical solutions and cross-border medical care entails the need for a practicable data protection framework in that respect. Yet the EU Commission's project of a Data Protection Regulation (DPR)[66] is currently frightening the ICT industry. If the DPR is becoming reality, privacy by design and default obligations, data portability rights and administrative sanctions in case of deliberate or negligent non-compliance may considerably hurt the app industry and have the potential of reshaping current patterns. On the other hand, cross-border data transfers may be assessed on a sectorial basis, which would likely facilitate the transfer of health data to U.S. healthcare providers regulated under HIPAA or HITECH Act.

[65] COM (2012)736 final, p. 9 and 10, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9156.

[66] COM(2012)11 final, http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.