European Journal of ePractice

A publication of epractice.eu

Meet > Share > Learn at www.epractice.eu/en/journal/

Nº 21 · December 2013

# From *e*Health to *m*Health

## *Society Becomes the Driver of its Health Activities*

*mHealth Regulatory Environments*

## Editorial

## Articles

The European Journal of ePractice is a digital publication on eTransformation by ePractice.eu a portal created by the European Commission to promote the sharing of good practices in eGovernment, eHealth and eInclusion.

**Editor-in-Chief**
Trond Arne Undheim

**Issue Editor**
Diane Whitehouse

**Editorial Coordinators**
Alexandros Stylianou
Hugh McCormack
Rodoula Kokmotou

The Information and Communication Management (ICM) team coordinates article submission, undertakes the peer-review process and performs editing of all content.

**Web:**
http://www.epractice.eu/en/journal/

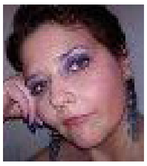
**Email:**
ePractice@eurodyn.com

European Journal of ePractice
A publication of epractice.eu

# Editorial: mHealth Regulatory Environments

Alexandros Stylianou
European Dynamics SA
http://www.epractice.eu/en/people/252935

Hugh McCormack
European Dynamics SA
http://www.epractice.eu/en/people/215139



Rodoula Kokmotou
European Dynamics SA
http://www.epractice.eu/en/people/15990

The ongoing widespread uptake and use of mobile telecommunications and multimedia technologies, including such devices as smartphones and tablet computers, has opened up rich new avenues to exploit in eHealth. Mobile health (mHealth) is now a rapidly developing trend within the field which employs these new technologies in healthcare delivery systems. Issue 21 of the European Journal of ePractice takes up the challenge of analysing mHealth as it is now, and offering some clues about how it should or could develop in the future.

Issue 21 called '**mHealth Regulatory Environments**', is comprised of six papers written by authors from Australia, Spain, Greece, the US, Belgium, and the Netherlands. The first five of these are concerned with the regulations and certification of mHealth applications, or 'apps', software which utilise smartphone platforms to deliver specific types of patient care and management. The rapid evolution of mobile communication devices and their supporting systems has opened up a vast market for healthcare apps. However, many contributors are concerned that the standards and regulations have not kept pace with the technology, bringing problems to manufacturers, healthcare services and patients alike. The papers describe the status quo from diverse perspectives and various responses to this state of affairs, primarily by proposing approaches, strategies and frameworks according to which the healthcare authorities should or could act to improve the standards and regulations. The final paper approaches the potential of mHealth from a totally different perspective, by taking up a more academic and sociological approach to the issues of communication in mHealth systems.

The first paper of Issue 21 is by **Jennifer Lindley** and **Juanita Fernando**. They assert that governance and regulatory guidelines have failed to keep pace with the technology, with serious implications for clinical care, professional practice and the education of healthcare professionals. The authors explore the disadvantages and risks attached to healthcare apps, and how best to educate healthcare professionals in their use. They conclude that there is a need for regulatory guidelines for the use of apps in healthcare, and for a more considered and comprehensive approach for the use of mobile devices and apps.

In the second paper, **Javier Ferrero-Álvarez-Rementería**, **Vincente Santana-López**, **Angela Escobar-Ubreva**, **Marta Vázquez-Vázquez**, **Habibullah Rodríguez-Contreras** and **Carmen Sánchez-Hinojosa** present the Quality and Safety Strategy for Health Mobile Application, a Spanish-language proposal for regulating mobile health applications, aiming to increase their benefits and minimise their risks. This initiative incorporates a guide providing essential recommendations and requirements for the correct use of mobile applications. It has also given rise to an app certification programme comprising a self-assessment carried out by the mobile application owners and an evaluation process performed by a multidisciplinary group of experts. The authors argue that the success of mHealth will be influenced by the trust that it generates in users. Initiatives such as this one are therefore essential.

The paper by **Homer Papadopoulos**, **Vaidehi B. Sheth** and **Michael Wurst** examines the regulation processes for mHealth apps to obtain CE marks in the EU and FDA marks in the US. The authors present the results of a literature review combined with a set of interviews and their own first-hand experiences. They illustrate the challenges with two use cases involving applications by mHealth apps: one is an application to the FDA for the 'myVisionTrack' app, and the other is for a CE mark for an app developed through the USEFIL project http://www.usefil.eu. The aim of the paper is to describe the steps that are necessary to achieve FDA and CE markings of mobile health apps. At the same time, the paper highlights a number of key issues, and helps readers to understand the strengths and limitations of the two regulatory systems.

**Evgenio Montavani**, **Paul Quinn**, **Barry Guihen**, **Ann-Katrin Habbig** and **Paul De Hert** identify prominent issues concerning the use and regulation of apps, in particular in relation to data protection. Given that people's health problems often raise sensitive issues, the need for adequate data protection for the processing of information by healthcare apps is an important priority. The authors discuss this challenge in light of the EU legal medical device framework: they ask what the safety implications are of the decision not to regulate apps as medical devices even when the apps are used to attain medical aims. They conclude that there needs to be greater user control over personal data.

The fifth paper, by **Robert Furberg** and **M. Alexis Kirk**, examines the regulation of apps in the US. They note that patient-generated health information is not covered by US federal regulations, and so is vulnerable to both privacy and security threats. They argue that policymakers must act on this issue. As a result, they provide in their paper a conceptual framework which can be used by public and private sector healthcare actors as a foundation to develop effective policies and procedures on privacy and security issues. They recommend that US federal policymakers should build on the work of the private sector in the development of standards and regulations for mHealth technologies, rather than starting from scratch.

Issue 21 concludes with a paper which departs from its main theme of regulatory environments. **Ben van Lier** takes a sociological approach to the information exchange supported by mHealth systems. He views the interaction of people, organisations and technology not as the interaction of independent elements, but as the internal interactions of an amalgamation of these elements. He calls this amalgamation of people, organisations and technology a 'hybrid combination'. In such a hybrid combination, information exchange and sharing enables organisations to develop different relationships and be part of different networks. This raises new questions about the organisation and governance of mHealth operations and devices, and of the information that is exchanged. The author applies Niklas Luhmann's systems theory to understand this state of affairs more effectively and gain insights into the new possibilities and developments that are opening up.

# Being Smart: Challenges in the Use of Mobile Applications in Clinical Settings

The use of mobile devices such as smartphones and tablets is rapidly increasing in both social and work-based contexts. The development of software applications specifically designed for the medical workplace has led to an escalation in the use of these medical apps without any correlating development in governance or regulatory guidelines. This paper provides an introduction to issues relating to the use of mHealth in clinical practice. The pervasive use of medical apps in clinical settings, without guidelines for best practice use, has significant global implications for clinical care, professional practice and education of health care professionals. Although the use of medical apps on mobile devices provides obvious benefits, there are disadvantages as well as significant risks, which are explored in this paper. The rapidly expanding use of mHealth produces significant challenges regarding the education of health professionals. Curriculum content, together with teaching and learning approaches, need to be designed to engage students in the use of mobile devices in clinical settings and adequately equip them for their future professional practice. Guidelines providing certainty around the use of mobile devices and medical apps in clinical practice are necessary to inform best practices and ensure safety and quality in technology-linked patient care. It is imperative to scrutinise the use of mobile devices and medical apps in health care and develop a more considered and comprehensive approach.

Jennifer Lindley

Monash University,
Australia

Juanita Fernando

Monash University,
Australia

Keywords

Governance, health care practitioners, health profession education, medical apps, mHealth

> “The rapid growth of mobile devices and medical apps provides new possibilities in health care but requires investments in the education of health care professionals as well as the development of appropriate governance measures.”

# 1. Introduction

The use of mobile devices and software applications is pervasive across multiple operating platforms, and is increasing rapidly in social and work-based settings. This is a critical issue for professional practice in health care. This paper provides an overview of mHealth and considers the interface between health care professionals and digital technologies. Health care professionals include both medical and nursing practitioners as well as allied health professionals. In this context the potential benefits of digital technology, current use and appeal for users, risks and disadvantages, issues of governance and control are explored and some implications for health care professionals' education are highlighted.

Smartphones (single devices providing telephone, advanced personal digital assistant, media player, cameras and web browser services) have now been augmented by tablets (slighter larger devices without telephone capability but with similar functions). A range of software applications (apps) to help with specific health-related tasks are available for both kinds of devices. Many of these apps have also been re-designed for the medical marketplace (medical apps).

In 2010 Scientific American estimated that there were 1500 medical apps which comprised two main types (Sahari, 2011): electronic versions of existing references (e.g. drug databases) and apps intended to be used as clinical tools (e.g. colour vision tests, dose calculators). Reports also predict that the number of medical apps available for health care professionals will increase to almost 6 000 before the end of 2012 (Mobihealthnews, 2011). A market study reported 97 000 mobile health (mHealth) applications available in major app stores, 15 % of which were specifically designed for professionals in healthcare.

# 2. Current use

Many health care professionals agree that mobile access to medical apps has opened new practice horizons for health (World Health Organization, 2011). In 2010, US market research indicated that almost 70 % of the participating doctors had downloaded medical apps (Gullo, 2011). Reports on US data show increasing engagement in the use of smartphones and tablets in the healthcare sector (Gullo, 2011; B, 2012a). Other evidence shows that more than a third of physicians and almost three-quarters of nurses use medical apps on smartphones daily for work purposes (Gullo, 2011; Dolan B, 2012b). This evidence is supported by the findings of a global survey (World Health Organization, 2011) on the matter, while the penetration of mobile technologies for health world-wide indicates their ubiquitous application to specific aspects of clinical practice.

Currently, clinical practices appear to be limited to a narrow use of digital technology. Firstly, technology is used to store information such as data, images, videos, texts and publications. It is also used to access web-based repositories, services for health care information and electronic patient records. Communication and telemedicine functions, including voice, video, blogs and social networking tools, are also particularly useful (Gullo, 2011; Dolan B, 2012a; Dolan B, 2012b; Sahari, 2011; Dunbrack, 2011; Lin, 2011; Darien and Atlanta, 2012).

A number of aspects of digital technology are evidently attractive for clinical practice (Sahari, 2011; Gullo, 2011; World Health Organization, 2011). Firstly, decision making can be facilitated by access to data and high quality images when health care professionals are away from fixed working environments. In addition, the technology can also support patient-clinician interaction by providing point of care access to health education resources (Sahari, 2011). Finally, mobile device form features and kinaesthetics are anecdotally reported by medical practitioners to support their ease of use and pleasure to use, while voice activated applications and services, convenience and reduced computer start-up time are attractive to clinical end-users (Sahari, 2011; Dolan P, 2011).

## 3. Potential benefits

The potential benefits resulting from the use of mobile devices in health care have been identified and are related to many of the features that users find attractive (see Table 1). Access of information at point of care allows health care professionals to access patient records as well as decision support and treatment information systems. Telemedicine has provided a new consultation tool for communication using voice, text and images between health care professionals. The technology has also provided an effective platform for communication between health care professionals and patients, through the use of short message services (SMS) for appointment reminders, treatment compliance promotion and health education (World Health Organization, 2011).

**Table 1:** Potential user appeal of digital technologies

| *Category* | *Feature* |
|---|---|
| Resources | Storage of data and clinical tools on one device |
| | Data storage on private 'cyber location' e.g. server, cloud |
| | Quality of data (e.g. images) |
| | Social networking |
| | Access to evidence/educational material |
| | Teleconference options |
| | Telehealth |
| Convenience | Mobility of devices |
| | Speed of access to useful information |
| | Availability of multiple resources via single apps |
| Speedier access | Elimination of boot-up time |
| | Voice activated services and applications |
| Kinaesthetics | Usability ( ease and pleasure of use) |
| | Voice activated resources |
| Work practices | Team based consultation |
| | Improved efficiency (e.g. access data at patient bedside) |
| | Patient – practitioner interface |

Potential benefits of mobile devices and medical apps are certainly alluring, since their technology is not restricted by time or location and has the capacity to provide easy access to current data and evidence. It also has the potential to provide support for distributed health care, which is particularly valuable when spread across a wide geographical area. In addition, improved quality of interaction during consultations can be facilitated by the use of digital resources. The evidence shows that many clinicians are now using mobile technology in health care (World Health Organization, 2011).

## 4. Disadvantages and risks

A range of potential disadvantages and risks associated with the use of digital technology have been widely reported (World Health Organization, 2011; Fernando & Dawson, 2009) as outlined in Table 2. Infrastructure constraints, such as bandwidth availability or speed of interaction, impact on clinical use even though the device itself has a speedy start up time. These constraints are affected by broadcast range, the number of simultaneous users attached to a particular network connection and signal broadcast set up.

**Table 2:** Disadvantages and risks of use of digital technologies

| *Category* | |
|---|---|
| Infrastructure | Broadcast range |
| | Number of simultaneous users |
| | Broadcast set up |
| Distracters | Email sign ups |
| | Pop-ups |
| | Advertising banners |
| | Icons/badges |
| | Notifications |
| | Email alerts |
| Privacy and security | Loss or theft of devices |
| | Voice and video call interception |
| | Social media conversation permanently stored on device |
| | Pervasive root kits |
| | Cookies for data mining |
| App developers | Lack of understanding of health care contexts and standards |
| | Data mining may be embedded in some apps |
| | Limited end-user critique and appraisal of app during development |

Another risk of use includes distracters (i.e., items and event transmitted via mobile telephony that distract the end-user). These distracters have been widely reported in the context of eHealth applications in general (Makeham et al., 2008; Magrabi et al., 2010; Sweidan et al., 2009; Harrison et al., 2007; Fernando, 2012). On mobile devices, distracters include email sign ups required for apps as well as advertising banners and pop-ups. Icon badges, notifications, 'pop-up' alerts and constant availability of emails and Internet access can also lead to distraction (Richtel, 2007).

Privacy and security issues in health care contexts are of particular concern to all stakeholders because of the sensitive nature of the data stored on the many mobile devices (Fernando, 2012; Barton, 2012). Loss or theft of devices storing sensitive information is seen as the most significant security issue (Mearian, 2012). End-users should also bear in mind that voice and video calls, although transient, can be intercepted either in real time or as recorded messages (Lin, 2011). Conversations via social networking tools may also create risks as they are 'permanent' and remain accessible beyond the time of initiation (Hay et al., 2011; Thompson & Black, 2011).

Root kits are stealthy types of software designed to conceal the existence of particular processes or programs from normal methods of detection, enabling continuous privileged access to a digital device. Cookies can be inserted into downloads to track browsing history, which can be sold to other interests such medical suppliers and pharmaceutical companies. The existing culture and practices within the IT industry may also create risks. For example, some developer of apps have considered it acceptable to send a user's entire address book, without their permission, to remote servers and then store the data for future reference (Van Grove, 2012; BBC News technology, 2012).

The development of apps is ad hoc and frequently undertaken without input or critical appraisal by end-users (Barton, 2012). This can result in either variability of features or use of an app or, alternatively, an app that does not perform the expected function (e.g. an electrocardiogram app which does not provide accurate readings), as illustrated in Table 3 (Lin, 2011; Husain, 2010). Apps designed to perform the same function, but for different platforms, may not necessarily perform in same way. An 'intuitive' user may find they cannot translate their expertise across platforms. In addition, the issue of proprietary devices and software has resulted in 'restricted trading' for apps so that they may be limited to a particular device or require additional specific software for use on alternate devices (Husain et al., 2013; Fernando & Peters, 2011).

**Table 3:** Examples of apps with potential user issues (Husain et al., 2013)

| |
|---|
| Electrocardiogram |
| Stethoscope |
| Dose calculators |
| Skin lesion evaluator |
| Human anatomy for medical students |
| Tissue plasminogen activator therapy appraisal |
| Chest radiology |

Although there is a significant trend towards use of mobile devices in health care environments, this is not universal. Clinical practitioners may be reluctant to move away from familiar desktop environments to the use of mobile devices and apps, or they may lack expertise in the selection and use of apps (Lin, 2011). They may download apps with limited usability or lack the time to learn their use, which results in specific apps being virtually useless (Sahari, 2011). End-users who are clinicians or health professionals may also be concerned that using a mobile device during medical consultations can be mistaken by patients as a lack of attention to them (Husain, 2012) or may create a negative impression with colleagues (Nolan T, 2011). These factors may have an impact on the ways in which clinicians engage with mobile technology. Some of these issues have been addressed by clinical end-users who share their personal appraisals of medical apps (Husain et al., 2013).

## 5. Governance and control

Mobile device governance and control shortcomings can erode clinician confidence in the use of the technology. This is a key implementation barrier in upper-middle income regions of the world such as Europe (reported by 56 % of countries) and the Americas (50 %) (World Health Organization, 2011; Fernando, 2012). Many governments have begun to act on this challenge: therefore, the formal guidelines being developed for quality control or the vetting of apps may in the future have significant impact on patient care and safety.

In 2011, the US Food and Drug Administration released draft guidelines on some of the medical apps, especially those that convert a mobile platform into a medical device (US Food and Drug Administration, 2011). They also regulate apps claiming therapeutic benefit (Mearian, 2012). In Australia, legislative frameworks are generally limited to intended purpose, labelling and advertising claims of medical software. The Australian Therapeutic Goods Administration has begun implementing medical apps regulation but the process is not clear and appears to rely on user complaints to trigger an investigation (Giddon, 2011). The Australian National eHealth Transition Authority states that ‘while there is definitely a place for medical apps for clinical tools, practitioners need to be cautious about their use’ (Sahari, 2011).

## 6. Education of health care professionals

Students currently studying in health care courses have had the opportunity to interact with digital technologies from an early age and are often described using the term ‘digital native’ (Prensky, 2001). It is argued that the generations that have grown up with this new technology think and process information in fundamentally different ways from their predecessors (Prensky, 2001). This results from their being socially embedded in a technology-rich environment together with the frequency and nature of their interactions.

However, not all students are situated in the same place and stage; neither do they necessarily share the same knowledge, experience and attitudes regarding mobile devices and apps. Research shows a more complex picture with a range of experience and attitude in students (Jones et al., 2010; Bennett et al., 2008). In addition, the notion that older generations are not able to develop similar skills and become as adept as digital natives has been challenged (Helsper and Eynon, 2010). There is, however, evidence which indicates that medical students are keen to adopt the use of mobile devices in their future professional practice (Koehler et al., 2012).

Qualitative research with students, exploring their understanding of and attitudes to digital creativity suggests, for example, they operate in the mobile realm overwhelmingly ignorant of rights and restrictions of copyright (Palfrey et al., 2009). This shows a lack of insight into the legal and ethical complexities regarding the use of mobile technology. So students’ understanding of their responsibilities relating to the use of mobile devices and associated apps in clinical settings has become an area of concern.

Because the landscape is rapidly changing, evidence collected five years ago is limited to the technology in use at that time. This means that issues relating to new and emerging software applications for mobile devices are absent from the existing evidence. The critical and informed use of digital technology is not apparent, nor generally emerging, in the education and training of students and graduates in the health care professions (Gray et al., 2011).

The development of medical apps for mobile devices has received wide encouragement and support. Competitions which promote the creation of health-related apps have been organised in the US, Australia and the UK (Healthcare Informatics, 2012; Health Informatics Society of Australia, 2012; Kennedy, 2011). This highlights a tension between encouraging innovative development of apps and education in the critical use of the technology.

Guidelines for health care education provided by government bodies that certify these programs provide a scaffold for curriculum development for medical education (Australian Medical Council, 2010; General Medical Council (UK), 2009; Liaison Committee on Medical Education (US), 2012). The guidelines fail to systematically address mobile digital technologies in health care, and do not focus on the critical evaluation of apps and their use. Students need to realise that the apps used do not 'do the thinking for you'. This is a critical gap that would be addressed by the development of pertinent guidelines, curricula and training (Coeira et al., 2012).

There is a mismatch between real-life health care practice and education. In the case of an adverse event, who precisely is responsible: the app developer, the individual clinician user, the health care provider organisation or the government regulators?

# 7. Conclusions

The use of mobile devices and apps can provide significant potential benefits for health care. However, mHealth also has identifiable disadvantages and risks. Best practice use of the technology needs to be incorporated into the education of health care professionals, and curricula need to be developed to provide the appropriate knowledge, skills and attitudes for future professional practice. This paper suggests that new approaches to education for the use of mHealth are required for healthcare practitioners. Engagement of recognised professional bodies and accreditation authorities in the providing guidelines for development of apps may address issues that currently exist and which may emerge in the future. However, this requires certainty around the use of mobile devices and apps in clinical practice, including the clarification of responsibility for technology-linked patient care.

There is a need for regulatory guidelines for use in clinical care, particularly beyond the concept of mobile devices used to mediate a 'face-to-face' consultation or even a clinical 'toolkit' managed by an enthusiastic end-user. This raises significant issues for professionalism in patient care, making imperative a more considered and comprehensive approach to the use of mobile devices and medical apps in health care.

# 8. References

Australian Medical Council. (2010). Standards for Assessment and Accreditation of Medical Schools, retrieved September 9, 2013 from http://www.amc.org.au/images/Medschool/accreditation-standards-medical-schools-2010.pdf.

Barton, A. J. (2012). The regulation of mobile health applications. BMC Medicine, 10, 46.

Bennett, S., Maton, K. & Kervin, L. (2008). The 'digital natives' debate: A critical review of the evidence. British Journal of Educational Technology, 39 (5), 775–786 retrieved September 9, 2013 from http://onlinelibrary.wiley.com/doi/10.1111/j.1467-8535.2007.00793.x/full.

BBC News technology. (2012). Google fined over Safari cookie privacy row, retrieved September 9, 2013 from http://www.bbc.com/news/technology-19200279.

Coeira, E. W., Kidd, M. R. & Haikerwal, M. C. (2012). A call for national e-health clinical safety governance. Medical Journal of Australia, 196 (7), 430-431.

PRNewswire (2011). New mobile health market study forecasts mobile health app services will reach $26 billion, retrieved September 9, 2013 from http://finance.yahoo.com/news/mobile-health-market-study-forecasts-221800413.html.

Darien, C. T. & Atlanta, D. A. (2012). 2012 National Physicians Survey, retrieved September 9, 2013 from http://www.sharecare.com/static/press-release-2012-national-physicians-survey.

Dolan, B. (2012a). Survey: 71 percent of US nurses use smartphones, Mobihealthnews, retrieved September 9, 2013 from http://mobihealthnews.com/17172/survey-71-percent-of-us-nurses-use-smartphones/.

Dolan, B. (2012b). About 62 % of physicians use tablets, Mobihealthnews, retrieved September 9, 2013 from http://mobihealthnews.com/17309/2012-about-62-percent-of-physicians-use-tablets/.

Dolan, P. (2011). Doctors cite ease of use in rapid adoption of tablet computers, American Medical News, retrieved September 9, 2013 from http://www.ama-assn.org/amednews/2011/04/18/bisc0418.htm.

Dunbrack, L. (2011). The second wave of clinical mobility: Strategic solution investments for mobile point of care, IDC Health Insights, retrieved September 9, 2013 from http://www.intel.nl/content/dam/www/public/us/en/documents/white-papers/clinical-mobility-in-healthcare-paper.pdf.

Fernando, J. (2012). Clinical software on personal mobile devices needs regulation. Medical Journal of Australia, 196 (7), 437.

Fernando, J. & Dawson, L. (2009). The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics, 78 (12), 815-826.

Fernando, J. & Peters, N. (2011). Wireless computer games and applications in the medical education curriculum: Adventures in pedagogy. Electronic Healthcare, Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications, 91, 93-96 retrieved September 9, 2013 from http://link.springer.com/chapter/10.1007%2F978-3-642-29262-0_13.

General Medical Council (UK) (2009). Tomorrow's Doctors, retrieved September 9, 2013 from http://www.gmc-uk.org/TomorrowsDoctors_2009.pdf_39260971.pdf.

Giddon, J. (2011). TGA joins global smartphone health trend. eHealthspace retrieved September 9, 2013 from http://ehealthspace.org/news/tga-joins-global-smartphone-health-trend.

Gray, K., Dattakumar, A., Maeder, A. & Chenery, H. (2011). Educating future clinicians about informatics: Review of implementation and evaluation of cases. European Journal for Biomedical Informatics, 7 (2), 48-57, retrieved September 9, 2013 from http://www.ejbi.org/img/ejbi/2011/2/Gray_en.pdf.

Gullo, C. (2011). Half of doctors to use medical apps in 2012, Mobihealthnews, retrieved September 9, 2013 from http://mobihealthnews.com/14703/half-of-doctors-to-use-medical-apps-by-2012/.

Harrison, M. I., Koppel, R. & Bar-Lev, S. (2007). Unintended consequences of information technologies in health care: An interactive sociotechnical analysis. Journal of the American Medical Informatics Association, 14 (5), 542-549.

Hay, A. A., Gamble, R. G., Huff, L. S. & Dellavalle, R. P. (2011). Internet social networking sites and the future of dermatology journals: Promises and perils. Journal of the American Academy of Dermatology, 65 (3), e81–e83, retrieved September 9, 2013 from http://www.sciencedirect.com/science/article/pii/S0190962211005512.

Health Informatics Society of Australia. (2012). HISA Mobile App University Challenge 2012, retrieved September 9, 2013 from http://www.healthbeyond.org.au/hisaApp.html.

Healthcare Informatics. (2012). IOM opens health app challenge, retrieved September 9, 2013 from http://www.healthcare-informatics.com/news-item/iom-opens-health-app-challenge.

Helsper, E. J. & Eynon, R. (2010). Digital natives: where is the evidence? British Educational Research Journal, 36 (3), 503-520.

Husain, I. (2010). iStethoscope app will not replace a physicians stethoscope – story by The Guardian is borderline reckless. iMedicalapps, retrieved September 9, 2013 from http://www.imedicalapps.com/2010/09/istethoscope-iphone-medical-app-review/.

Husain, I. (2012). Do you avoid using your iPhone’s medical apps in the hospital for social reasons? iMedicalApps retrieved September 9, 2013 from http://www.imedicalapps.com/2012/06/iphone-medical-apps-hospital-social/.

Husain, I., Misra, S. & Wodajo, F. (eds). iMedicalApps.com iMedical Web Apps (splash page). iMedicalApps.com, retrieved September 9, 2013 from http://www.imedicalapps.com/about/.

Jones, C., Ramanau, R., Cross, S. & Healing, G. (2010). Net generation or Digital Natives: Is there a distinct new generation entering university? Computers and Education, 54 (3), 722-732.

Kennedy, J. (2011). NHS launches apps competition for better citizen healthcare, Silicone Republic, retrieved September 9, 2013 from http://www.siliconrepublic.com/innovation/item/23254-nhs-launches-apps-competiti.

Koehler, N., Yao, K., Vujovic, O. & McMenamin, C. (2012). Medical students’ use of and attitudes towards medical applications. Journal of Mobile Technology in Medicine, 1 (4), 16-21.

Liaison Committee on Medical Education (US). (2012) Standards for Accreditation of Medical Education Programs Leading to the M. D. Degree, retrieved September 9, 2013 from http://www.lcme.org/functions.pdf.

Lin, K. (2011). The Promise and Pitfalls of Medical Apps for Doctors, US News and World Report, retrieved September 9, 2013 from http://health.usnews.com/health-news/blogs/healthcare-headaches/2011/08/26/the-promise-and-pitfalls-of-medical-apps-for-doctors.

Magrabi, F., Ong, M.S., Runciman, W. & Coiera, E. (2010). An analysis of computer-related patient safety incidents to inform the development of a classification. Journal of the American Medical Informatics Association, 17, 663-670.

Makeham, M. A. B., Saltman, D. C. & Kidd, M. R. (2008). Lessons from the TAPS study — recall and reminder systems. Australian Family Physician, 37, 923-924.

Mearian, L. (2012). ‘Wall of Shame’ exposes 21M medical record breaches. Computerworld, retrieved September 9, 2013 from http://www.computerworld.com/s/article/9230028/_Wall_of_Shame_exposes_21M_medical_record_breaches.

Mobihealthnews (2011). Professional medical Apps for Apple's iPhone Report, retrieved September 9, 2013 from http://mobihealthnews.com/professional-medical-apps-for-apples-iphone/.

Nolan, T. (2011). A smarter way to practise. British Medical Journal (Internet), 342, retrieved September 9, 2013 from http://www.bmj.com/content/342/bmj.d1124.

Palfrey, J. Gasser, U. Simun, M. & Barnes, R.F. (2009). Youth, Creativity, and Copyright in the Digital Age. International Journal of Learning and Media, 1 (2), 79-97.

Prensky, M. (2001). Digital native, digital immigrants. On the Horizon, 9 (6), 1-6.

World Health Organization (2011). mHealth: New horizons through health for mobile technologies. Global Observatory for eHealth series – Volume 3, retrieved September 9, 2013 from http://www.who.int/goe/publications/ehealth_series_vol3/en/.

Richtel, M. (2011). As Doctors Use More Devices, Potential for Distraction Grows. The New York Times, retrieved September 9, 2013 from http://www.nytimes.com/2011/12/15/health/as-doctors-use-more-devices-potential-for-distraction-grows.html?pagewanted=all.

Sahari, S. (2011). Appy Days, Australian Doctor, retrieved September 9, 2013 from http://www.australiandoctor.com.au/in-depth/work-wise/appy-days.

Sweidan, M., Reeve, J. F., Brien, J. E., et al. (2009). Quality of drug interaction alerts in prescribing and dispensing software. Medical Journal of Australia, 190, 251-254.

Thompson L. A. & Black E. W. (2011). Nonclinical use of online social networking sites: new and old challenges to medical professionalism. Journal of Clinical Ethics, 22 (2), 179-82.

US Food and Drug Administration (2011). Draft guidance for industry and food and drug administration staff - mobile medical applications, retrieved September 9, 2013 from http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ucm255978.htm.

Van Grove, J. (2012). Your address book is mine: Many iPhone apps take your data. Venture Beat retrieved September 9, 2013 from http://venturebeat.com/2012/02/14/iphone-address-book/.

World Health Organization (2011). mHealth: New horizons through health for mobile technologies. Global Observatory for eHealth series – Volume 3, retrieved September 9, 2013 from http://www.who.int/goe/publications/ehealth_series_vol3/en/.

## Authors

**Jennifer Lindley**
Monash University, Australia
Jennifer.Lindley@monash.edu
http://www.epractice.eu/en/people/357778

**Juanita Fernando**
Monash University, Australia
juanita.fernando@med.monash.edu.au
http://epractice.eu/en/people/89931

# Quality and Safety Strategy for Mobile Health Applications: A Certification Programme

mHealth technologies have the potential to improve the quality of life and patient safety. In order to benefit from these technologies, however, health organisations and patients face major challenges. Considering the increased proliferation of mobile health applications, ensuring patient safety in using them also becomes a priority.

The Quality and Safety Strategy in health mobile applications developed by the Andalusian Agency for Healthcare Quality, a pioneer initiative in the Spanish language worldwide, presents a proposal for regulating mobile health applications, increasing their benefits, encouraging improvement and minimising the risks of misuse.

In order to ensure the safety and reliability of mobile health applications, the Andalusian Agency for Healthcare Quality has created the 'Guide of recommendations for the design, use and evaluation of mobile health applications'. This guide includes essential recommendations and requirements for the correct use of mobile applications, and is intended for all the stakeholders involved in mHealth: citizens, health professionals, health service providers and developers.

Javier Ferrero-Álvarez-Rementería

Andalusian Agency for Healthcare Quality, (ACSA), Spain

Vincente Santana-López

Andalusian Agency for Healthcare Quality (ACSA), Spain

Angela Escobar-Ubreva

Andalusian Agency for Healthcare Quality (ACSA), Spain

Marta Vázquez-Vázquez

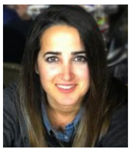
Andalusian Agency for Healthcare Quality (ACSA), Spain

This initiative gave rise to AppSaludable Distinctive, an app certification programme. The AppSaludable Distinctive represents public recognition for developers and owners of health apps, as well as a seal of guarantee for users. Its certification programme is based on a methodology consisting first of a self-assessment phase performed by the mobile application owners, followed by an evaluation process carried out by a multidisciplinary group of experts that is aimed at identifying improvement areas within the mobile application.

The enormous transformative possibilities for health organisations and the potential benefits for both patients and health services are not exempt from risks and challenges. It is imperative to provide citizens with criteria for distinguishing and selecting the most appropriate mobile applications, thus permitting them to counter such adverse events as fraud that could put patients' health at risk.

Habibullah Rodríguez-Contreras

Andalusian Agency for Healthcare Quality (ACSA), Spain



Carmen Sánchez-Hinojosa

Andalusian Agency for Healthcare Quality (ACSA), Spain

Keywords

App certification, AppSaludable Distinctive, mHealth, mobile medical applications, patient safety, quality, quality and safety strategy in health mobile applications, recommendations for design, use and evaluation of mobile health applications

> “The AppSaludable Distinctive represents public recognition for developers and owners of health apps, as well as the first seal of guarantee for Spanish-speaking users.”

# 1. Introduction

mHealth can transform the way in which health services are delivered to the world: more efficient ways of working, optimisation of care processes, building up patient safety, participation and involvement of citizens, etc. (World Health Organization, 2011). The health system is highly mobile in nature: smartphones combine mobile communication and computing in the palm of a person's hand, at the point of patient care (Mohammad Mosa et al., 2012). In a context of intense budget pressures and an ageing and more chronically ill population, mHealth opens opportunities to new and more efficient ways of working, inviting the exploration and potential optimisation of healthcare processes, and the participation and involvement of citizens, that can lead to an improvement in health outcomes.

As a result, mHealth technologies can improve the quality of life and patient safety; however, they can contribute to several major challenges for health organisations and patients. Therefore, the development and proliferation of new mHealth technologies have been based on the recognition of fundamental rights and legal obligations: right to health, access to information, principle of non-discrimination, privacy and data protection. The expansion of mHealth and mobile health applications should not harm these fundamental rights. Rather, on the contrary, they must help to spread the values supported by these rights. As such, ensuring patient safety in the use of mobile health applications also becomes a priority.

The objective of the MovingLife project (2013) is 'to deliver a set of roadmaps for technology and application research and innovation, implementation practice and policy support with the aim to accelerate the establishment, acceptance and wide use of mHealth solutions at a global scale'.The future of mHealth depends on a large number of dimensions and variables, of which technology is one and perhaps not the most decisive. The roadmap for socio-economic and policy frameworks identifies socio-economic and policy drivers and inhibitors for massive deployment of mHealth related to: user acceptance; ethical issues; security, privacy and trust models. The uptake of mHealth solutions highly depends on trust. Currently, this trust is often lacking.

The field of medical apps is presently one of the most dynamic in medicine, with real potential to change the way evidence-based healthcare is delivered in the future. Establishing appropriate regulatory procedures will enable this potential to be fulfilled, while at all times ensuring the safety of the patient (Gerard, et al., 2013).

It is essential to clarify the regulatory framework applicable to mHealth, as it is considered the biggest barrier impeding mHealth deployment in Europe (Peetso, 2013). In its report of May 2012, the European Commission's eHealth Task Force emphasised that there are no quality criteria for these tens of thousands of health apps available on the market, and no standards for data management and consumer information. Following the eHealth Task Force report, the European Commission recognised in its eHealth Action Plan 2012-2020 the importance of tackling clarity on legal and other issues surrounding mobile health applications.

Currently there are several on-going proposals for developing health app certification programmes in the English-speaking world[1], which begin to outline possible quality guidelines and recommendations on mobile health applications:

[1] No such guidelines have been identified in the Spanish language so far, with the exception of those developed in Andalusia.

- The company Happtique offers an app certification programme based on the following standards: operability; privacy; security; and content standards. (Leroux & Rivas, 2013).
- The UK National Health Service (NHS) has launched the Health App Library[2], a library of ‘apps’ that has been endorsed by the NHS for patients which can be ‘prescribed’ by doctors. All submitted apps meet three minimum requirements: they are relevant to people living in England; they comply with data protection laws; and they comply with trusted sources of information, such as NHS Choices.
- The US Food and Drug Administration (FDA) would regulate only a small portion of the rapidly expanding universe of mobile health applications (Tavernise, 2013). The FDA issued the Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff on 25 September 2013, which explains the agency’s oversight of mobile medical apps as devices (FDA, 2013).

Most health-related apps are thus defined as non-devices and will not be subject to regulation (Kamerow, 2013). This exception includes electronic versions of medical books, educational apps, and communication aids. With regard to the set of apps that do reach the level of ‘device’ and can be used in the diagnosis, treatment or prevention of disease, the FDA will exercise ‘enforcement discretion’ and not regulate those that pose a low risk to the public (which includes most of the disease-tracking apps, such as for diabetes, smoking cessation, or dieting). According to Kamerow (2013) ‘regulating these may not be the FDA’s job, but it should be someone’s’.

## 2. The Andalusian Agency for Healthcare Quality

The Andalusian Agency for Healthcare Quality[3] is a public organisation whose mission is to promote a culture of quality, patient safety and continuous improvement in healthcare, that was set up in March 2012. It created several recommendations for the development, use and evaluation of mobile health applications. This initiative arose from the experience gained with other initiatives in Andalusia like the Accreditation Programme of websites on health[4] and different Distinctions awarded by the Observatory for Patient Safety[5].

Before the development of materials related to quality and safety strategy in mobile health applications, a comprehensive literature review on the subject was conducted, with a first systematic search on health sciences databases followed by an unstructured search through the Web.

A panel of experts contributed to the development of the project. This panel was composed of health professionals, application developers, patient representatives, managers from the Andalusian Public Health System, and experts from different knowledge areas (such as accessibility, usability, security, and data protection, etc.), from both within and beyond Andalusia.

[2] http://apps.nhs.uk
[3] www.juntadeandalucia.es/agenciadecalidadsanitariadeandalucia
[4] www.calidadwebsalud.com/el-programa-de-acreditacion
[5] www.juntadeandalucia.es/agenciadecalidadsanitaria/observatorioseguridadpaciente/opencms/es/index.html

The Quality and Safety Strategy for Health Mobile Applications officially started with a press conference offered by the Andalusian health regional minister. It is a dynamic and integrated process featuring suggestions that range from ideas members of the general public to a body of recommendations for the application's developers and owners and a health app certification programme.

The Quality and Safety Strategy for Health Mobile Applications aims to create a community around these types of initiatives in order to promote mobile technologies in the fields of health and wellness, relying on the social involvement initiated through the portal created for this purpose and diffusion through social networks.

## 3. Recommendations for the design, use and evaluation of mobile health applications

The guide of recommendations for the design, use and evaluation of mobile health applications, developed in Andalusia, was conceived as a resource for all stakeholders involved in mHealth: citizens, health professionals, health service providers and developers. These recommendations focus on the following areas: design and pertinence, information quality and safety, service provision, confidentiality and privacy (Table 1).

**Table 1:** List of Recommendations ordered by Group and Criteria

| Group | Criteria | Standard |
|---|---|---|
| Design and Pertinence | Pertinence | 1. The health app clearly defines its functional scope and the purpose for which it was developed, identifying the groups to which it is addressed and the objectives pursued with respect to these groups. |
| | Accessibility | 2. The health app follows the principles of universal design, as well as standards and references from accessibility recommendations. |
| | Design | 3. The health app complies with the design standards and recommendations set out in the official guidelines provided by the different markets. |
| | Usability | 4. The health app has been tested with potential users prior to its availability to the public. |

| | | |
|---|---|---|
| Information Quality and Safety | Adaptation to the audience | 5. The health app is adapted to the type of targeted audience. |
| | Transparency | 6. The health app provides transparent information on the identity and location of their owners. |
| | | 7. The health app provides information on sources of funding, promotion and sponsorship, as well as potential conflicts of interest. |
| | Authorship | 8. The health app identifies the authors / responsible parties for its content, as well as their professional qualifications. |
| | Information Update/Reviews | 9. The health app contains the last review date for the published material. |
| | | 10. The health app notifies the users of updates that affect or modify content or functionality about health or any other sensitive data. |
| | Contents and sources of information | 11. The health app is based on one or more reliable sources of information and takes into consideration the available scientific evidence. |
| | | 12. The health app provides concise information about the process used to select its contents. |
| | | 13. The health app is based on ethical principles and values. |
| | Risk management | 14. The health app identifies possible risks on patient safety |
| | | 15. Appropriate actions are taken on possible known risks and adverse events |
| Service Provision | Technical Support / Help | 16. The health app has a help section. |
| | | 17. The health app provides technical support, ensuring a certain response time for the user. |
| | eCommerce | 18. The health app describes the terms and conditions regarding the marketing of their products and services. |
| | Bandwidth | 19. The health app makes efficient use of communication bandwidth |
| | Advertising | 20. The health app notifies of the use of advertising and how to disable or skip it |

| | | |
|---|---|---|
| Privacy and Confidentiality | Data protection | 21. Prior to its download and installation, the app declares what user data is collected and for what purpose, its policies on data access and processing, as well as possible trade agreements with third parties. |
| | | 22. The health app describes which personal information is recorded, in a clear and understandable terms and conditions. |
| | | 23. The health app preserves the privacy of the information recorded, contains explicit consent of the user and warns about the risks of using mobile health applications through public networks |
| | | 24. If the app collects health or health information exchanges or any other particularly sensitive data on its users, it ensures the appropriate security measures. |
| | | 25. The health app informs users when accessing any device resources, user accounts or social networking profiles. |
| | | 26. The health app ensures at anytime the right of access to recorded information, as well as to any update or change in its privacy policy. |
| | | 27. The health app implements measures to protect children in accordance with current legislation. |
| | Security | 28. The health app does not contain any known vulnerability or any type of malicious code. |
| | | 29. The health app describes its security procedures to prevent unauthorised access to personal information collected, as well as access restriction to protected data by third parties. |
| | | 30. The health app offers data encryption mechanisms for information storage and exchange, and password management mechanisms. |
| | | 31. The health app states the terms and conditions of cloud services used, including the security measures for this purpose |

These recommendations include requirements, and more specific statements concerning features or characteristics that should be considered to ensure the correct use of mobile applications. These requirements can be essential (indispensable for achieving a distinction) or non-essential in contributing to the overall compliance of recommendations.

The publication of this guide, which is the first edition available worldwide in the Spanish language, achieved two objectives: the identification and recognition of secure and reliable mobile applications by users; and the recommendation of good practices for designing and optimising apps for application developers.

The guide, like the whole mHealth strategy in Andalusia, is a continuous process that is open to suggestions and contributions. Through this collaboration, the information, guidelines and the content will be improved as a result of the comments made and sent via the web platform.

## 4. AppSaludable Distinctive: quality and safety assurance for mobile apps

In another step towards the recognition of best practices in mHealth, beginning with the guidance and recommendations within the Quality and Safety Strategy in Health Mobile Applications, the Andalusian Agency for Healthcare Quality created the AppSaludable Distinctive, a seal of guarantee which recognises mobile applications that are safe and reliable for users.

The process is based mainly on self-assessment and subsequent evaluation by an expert committee of the Agency, who oversees the compliance with these recommendations and identifies possible improvements for each app.

The entire process is fully supported by a web information system available at: http://www.calidadappsalud.com/distintivo/login?accion=logar&idTipoSolicitud=9

Through this platform, those responsible for the app can request and manage the evaluation process for obtaining the distinction. Upon accepting the application form, and providing credentials for access, the user initiates a self-assessment of the requirements, and submits evidence on quality and safety requirements when necessary. After this phase, the project progresses to the evaluation stage where the expert committee assesses both the mobile application and the submitted evidence.

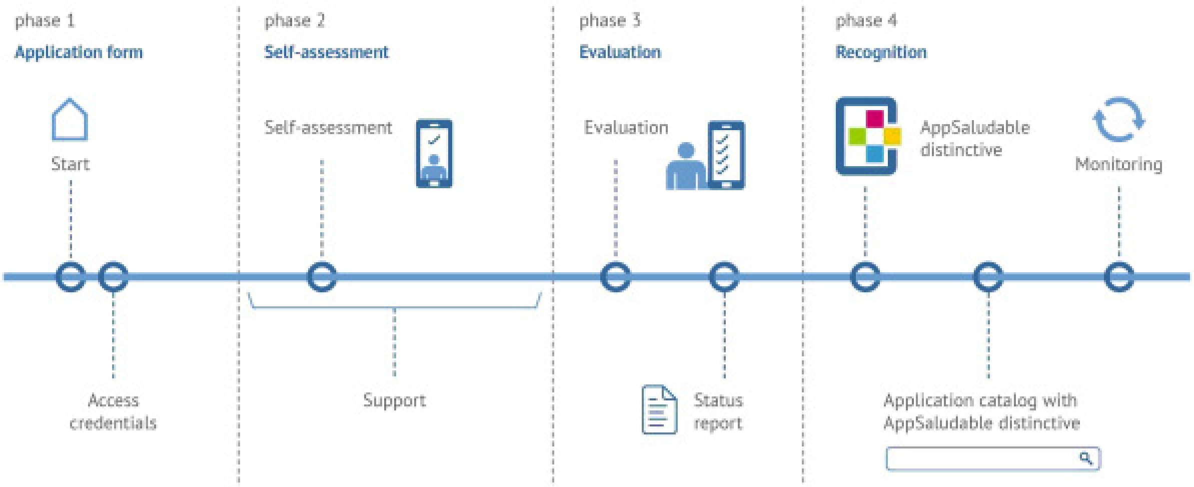


**Figure 1:** Methodology of Quality and Safety Strategy in Health Mobile Applications

The comprehensive evaluation carried out by health professionals, experts in patient safety, usability and design, leads to the reopening of a new self-assessment process, with suggested improvement areas to complete the process, or at best cases, with the awarding of AppSaludable Distinctive.

The granting of this distinction, which is the first in the Spanish language worldwide, is intended as a guarantee of confidence for app users. It is available for all mobile applications from both public and private initiatives upon request and free of charge.

## 4.1 Piloting the AppSaludable Distinctive

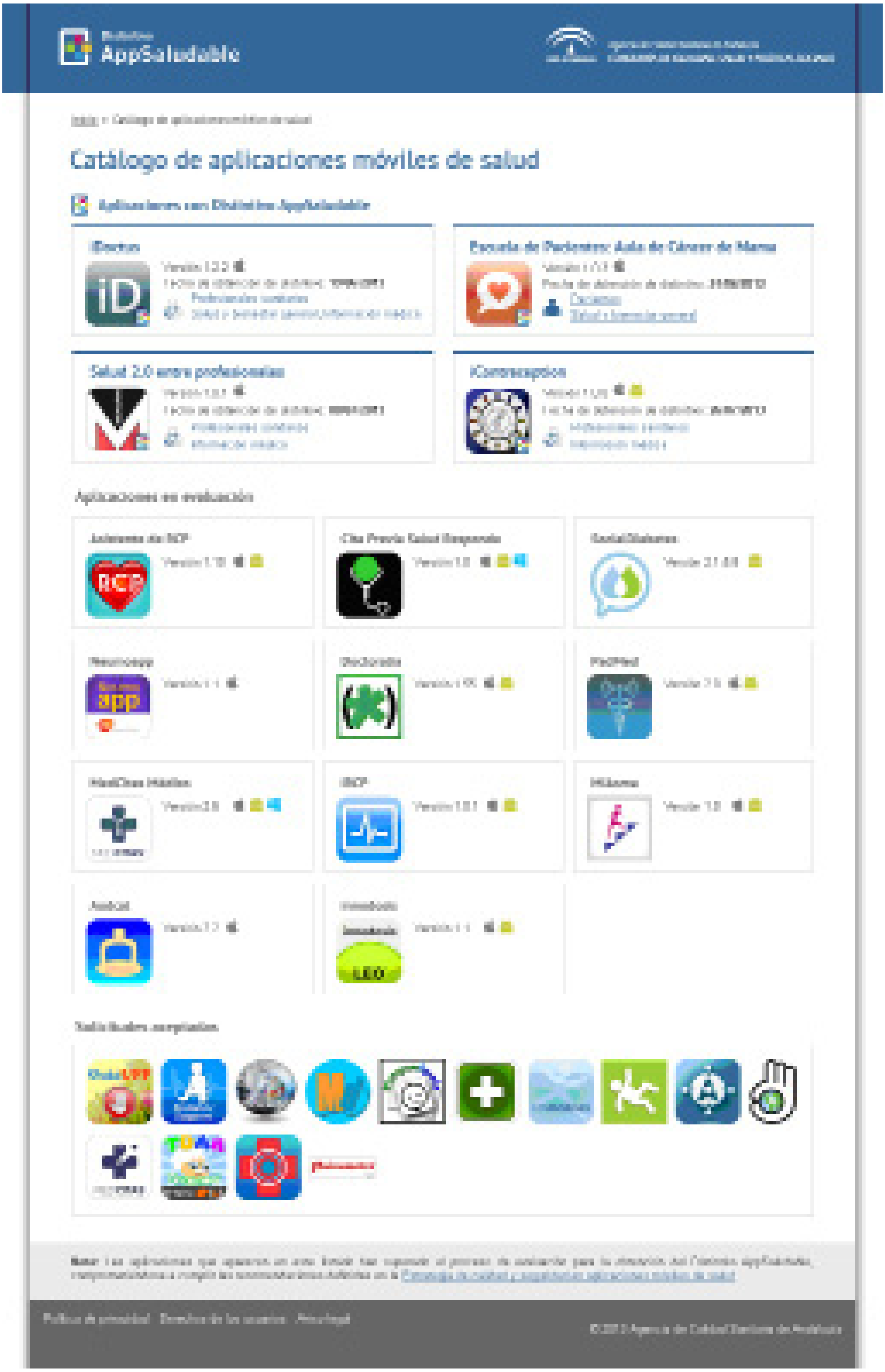
During the first half of 2013, the AppSaludable Distinctive was piloted with three mobile health applications, one for health professionals and two for patients. The aim was to identify improvements in the self-assessment procedure, evaluation and web application for support, as well as in the content of the recommendations.

After several self-assessment and evaluation cycles, some improvements were identified and incorporated into the process. The first distinctions were awarded, leading to the official inauguration of the AppSaludable Distinctive in May 2013. Currently there are more than 60 mobile health apps that have requested the distinction and they are found in the different phases of the project.

## 4.2 App library

Once the first distinctions were granted, a Featured Application List (see Figure 2: Health Apps Library) was created that showed:

- Health apps which have AppSaludable recognition (showing names, icons and descriptions);
- Health apps that are in the process of improvement (showing names and icons);
- Health apps which have applied for the distinction or have been accepted to enter the process (showing icons).



Distintivo AppSaludable

Inicio > Catálogo de aplicaciones móviles de salud

Catálogo de aplicaciones móviles de salud

Aplicaciones con Distintivo AppSaludable

iDoctus
Versión 1.2.2
Fecha de obtención de distintivo: [illegible]
Profesionales sanitarios
Salud y bienestar general, Información médica

Escuela de Pacientes: Aula de Cáncer de Mama
Versión 1.7.0
Fecha de obtención de distintivo: [illegible]
Pacientes
Salud y bienestar general

Salud 2.0 entre profesionales
Versión 1.0.1
Fecha de obtención de distintivo: [illegible]
Profesionales sanitarios
Información médica

iContraception
Versión 1.1.0
Fecha de obtención de distintivo: [illegible]
Profesionales sanitarios
Información médica

Aplicaciones en evaluación

Asistente de RCP
Versión 1.10

Cita Previa Salud Responde
Versión 1.0

SocialDiabetes
Versión 2.1.4.8

Neumoapp
Versión 1.1

Dislexia
Versión 1.9.5

PedMed
Versión 7.5

MediChas Móviles
Versión 2.8

iRCP
Versión 1.0.1

[illegible]
Versión 1.0

[illegible]
Versión 1.7

[illegible]
Versión 1.1

Solicitudes aceptadas

Nota: Las aplicaciones que aparecen en esta lista han superado el proceso de evaluación para la obtención del Distintivo AppSaludable, comprometiéndose a cumplir las recomendaciones definidas en la Estrategia de calidad y seguridad en aplicaciones móviles de salud

Política de privacidad · Derechos de los usuarios · Aviso legal

© 2013 Agencia de Calidad Sanitaria de Andalucía

**Figure 2:** Health Apps Library

## 5. Conclusions

Mobile health applications represent a technology with enormous potential to transform health services, and with tremendous potential benefits for both patients and health services.

mHealth can enable new models of care that improve quality, access, individualisation, professional-patient interaction, patient empowerment and healthcare system efficiency.

However, significant challenges need to be addressed ahead of quality guarantees:

- The establishment of uniform regulations to increase trust;
- Usability and quality assurance for mHealth solutions.

The success of mHealth will be determined in particular by the degree of trust of them by users. Thus, it is essential to provide users with criteria for a proper identification and selection of the most desirable mobile apps, helping to differentiate them from those that are fraudulent and unreliable and which could endanger the health of patients. In this sense, public administrations should play a predominant role in garnering this degree of trust.

The Quality and Safety Strategy for Health Mobile Application by the Andalusian Agency for Healthcare represents a proposal to regulate the use of mobile health apps, thus enhancing its benefits, boosting its improvement and minimising the risks of misuse. In this context, the AppSaludable Distinctive represents the first seal of guarantee for the Spanish-speaking world, which recognises mobile applications that are safe and reliable for users. In the same innovative way, with the Health App Library, the Andalusian Agency for Healthcare Quality, tries to make it simple for users to easily find safe and trusted apps to help them manage their health.

Alongside these initiatives, in the near future the Andalusian Agency for Healthcare Quality is planning to create communities of practice that will be accessible to the different stakeholders related to mHealth, in an effort aimed at facilitating and contributing to the development of mHealth technologies.

## 6. References

Barton, A. J. (2012). The regulation of mobile health applications. BMC Medicine, 10-46, retrieved September 10, 2013 from http://www.biomedcentral.com/content/pdf/1741-7015-10-46.pdf.

Buijink, A.W., Visser, B.J. & Marshall, L. (2013). Medical apps for smartphones: Lack of evidence undermines quality and safety. Evid Based Med, 18(3): 90-2, retrieved September 8, 2013 from http://www.ncbi.nlm.nih.gov/pubmed/22923708.

Camerini, L. & Schulz, P. J. (2012). Effects of functional interactivity on patients' knowledge, empowerment, and health outcomes: An experimental model-driven evaluation of a web-based intervention. Journal of Medical Internet Research, 14 (4), retrieved July 22, 2013 from http://www.jmir.org/2012/4/e105.

Devices 4 Limited (2012). Regulation of health apps: A practical guide, retrieved March 2013 from http://www.d4.org.uk/research/regulation-of-health-apps-a-practical-guide-January-2012.pdf.

European Commission (2012a). eHealth Action Plan 2012-2020: Innovative healthcare for the 21st century, retrieved May 6, 2013 from

https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century.

European Commission (2012b). E-Health Task Force Report: Redesigning health in Europe for 2020. Brussels: European Commission, retrieved March 20, 2013 from http://www.president.ee/images/stories/pdf/ehtf-report2012.pdf.

FDA (2013a). Mobile Medical Applications. FDA, U.S. Food and Drug Administration FDA, retrieved September 15, 2013 from http://www.fda.gov/medicaldevices/productsandmedicalprocedures/ucm255978.htm

FDA (2013b). Mobile medical applications: Guidance for industry and Food and Drug Administration staff, retrieved September 16, 2013 from www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

GSMA (2012). Understanding medical device regulation for mhealth: A guide for mobile operators, retrieved September 9, 2013 from http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmaunderstandingmedicaldeviceregulationformhealthreport1.pdf.

Happtique (2013). Health app certification program. Certification Standards. Happtique, retrieved October 6, 2013 from http://www.happtique.com/docs/HACP_Certification_Standards.pdf.

Leroux, E. & Rivas, H. (2013). Evidence Based mHealth (EBmH), Mobile Health Without Borders, retrieved October 2, 2013 from https://novoed.com/mhealth/reports/52109.

Mohammad Mosa, A. S., Yoo, I. & Sheets, L. (2012). A systematic review of healthcare applications for smartphones. BMC Medical Informatics and Decision Making, 12, 67, retrieved September 26, 2013 from http://www.biomedcentral.com/1472-6947/12/67.

MovingLife Project (2013). The future of mobile eHealth in Europe: A stakeholder conference on roadmaps for mHealth. MovingLife Project, retrieved April 18, 2013 from http://moving-life.eu/downloads/events/MovingLife_Stakeholder_Conference_Agenda_18_April_2013.pdf.

PatientView (2012). European Health App Directory 2012-2013, retrieved April 2, 2013 from http://stwem.files.wordpress.com/2012/10/pv_appdirectory_final_web_300812.pdf.

Peetso, T. (2013). Health at your fingertips. Quarterly of the European Observatory on Health Systems and Policies, 9 (3), 21-22, retrieved September 9, 2013 from http://www.euro.who.int/__data/assets/pdf_file/0006/216843/Eurohealth_v19-n3.pdf.

Tavernise, S. (2013). FDA will apply its rules to only some health apps. The New York Times, September, 24, 2013: A12, http://www.nytimes.com/2013/09/24/health/fda-to-regulate-only-some-health-apps.html?_r=0.

WHO (2011). mHealth: New horizons for health through mobile technologies. Global Observatory for eHealth, v.3: World Health Organization, retrieved September 4, 2013 from http://www.who.int/goe/publications/ehealth_series_vol3/en/.

## Authors

**Javier Ferrero-Álvarez-Rementería**
Andalusian Agency for Healthcare Quality, ACSA, Spain
javier.ferrero@juntadeandalucia.es
http://epractice.eu/people/jferrero

**Vincente Santana-López**
Andalusian Agency for Healthcare Quality, ACSA, Spain
vicente.santana@juntadeandalucia.es
http://epractice.eu/people/vsantana

**Angela Escobar-Ubreva**
Andalusian Agency for Healthcare Quality, ACSA, Spain
angela.escobar@juntadeandalucia.es
http://epractice.eu/people/aescobar

**Marta Vázquez-Vázquez**
Andalusian Agency for Healthcare Quality, ACSA, Spain
marta.vazquez.vazquez@juntadeandalucia.es
http://epractice.eu/people/mvazquez

**Habibullah Rodríguez-Contreras**
Andalusian Agency for Healthcare Quality, ACSA, Spain
habibullah.rodriguez.ext@juntadeandalucia.es
http://epractice.eu/people/habibi

**Carmen Sánchez-Hinojosa**
Andalusian Agency for Healthcare Quality, ACSA, Spain
carmen.sanchez@s-dos.es
http://epractice.eu/people/sanchiino

# Comparison of US and EU Regulatory Approaches to Mobile Health Apps: Use Cases of myVisionTrack and USEFIL

The aim of the paper is to present, analyse, compare and discuss the necessary steps to FDA and CE marking of mobile health apps. The paper identifies and highlights those key issues that could facilitate developers/companies involved in the development of mobile health applications to obtain a deeper understanding of the regulation requirements for getting the CE and FDA marks.

To achieve the above objectives the paper studies two use cases to compare the CE marking and the FDA regulation process for mobile health apps. These are: 'myVisionTrack' and an under-development Android SmartWatch-compatible mobile health app within the realm of the USEFIL project. The paper discusses the necessary steps the myVisionTrack took to achieve the FDA regulatory approval and the necessary steps the Android SmartWatch app needs to take for the CE regulatory approval. The paper also discusses the two use cases from the point of view of payers by analysing their reimbursement mechanisms where this is possible.

These two use cases help readers to identify the strengths and limitations of the two regulation systems concerning mobile health applications. They also reveal the most important topics that have to be considered by the main actors (developers, investors, entrepreneurs and others) that wish to develop such apps before submitting for regulation approval. Furthermore the degree of uncertainty regarding the regulation frameworks in both the US and the EU for mobile health applications is discussed.

The research methodology adopted for this paper mainly consisted of desktop research to understand the CE and FDA process of mobile health applications, interviews with the CEO of the myVisionTrack, and an examination of first-hand data extracted from the EU-funded project USEFIL. Data analysis and filtering were mainly based on the professional experience of the three members of the team.

Homer Papadopoulos

Demokritos Research Centre, Greece

Vaidehi B.Sheth

eClinicalWorks, USA

Michael Wurst

InvisionHeart, USA

Keywords

CE, FDA, mobile health applications, medical devices, regulation processes

> “Mobile health applications have to be considered as typical medical devices when used for diagnosis and treatment and thus have to be regulated under the classification rules of the regulatory systems.”

## Acknowledgments

We acknowledge the help and guidance we received from Professor Jan Benjamin Pietzsch of Stanford University for this project paper, and we wholeheartedly thank him for his support. We also want to acknowledge the assistance received from Mr Michael Bartlett, President of Visual Art and Science Inc. whose constructive discussions regarding myVisionTrack mobile health app were essential to the project. Lastly, we would like to thank Lauren Cipriano for managing the process of completing this paper.

The 'USEFIL: An Unobtrusive Smart Environments for Independent Living' project (www.usefil.eu) is running under a funding scheme of small or medium scale focused research project (STREP) by FP7-ICT-2011-7. The partners of USEFIL are the: National Center for Scientific Research 'Demokritos' (Greece), VTT Technical Research Center (Finland), University of Bremen (Germany), University of Warwick (UK), Aristotle University of Thessaloniki (Greece), Fraunhofer Heinrich Hertz Institute (Germany), Maccabi Healthcare (Israel), and TP Vision (Netherlands).

# 1. Introduction and background

The use of health apps is exploding[1]. For example, in the US 52 % of smartphone owners gather health information via their phone (Fox et al., 2012). The World Health Organization (2011) defines mHealth 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'. According to the Groupe Speciale Mobile Association (GSMA)[2] 'apps' are defined as discrete, independent pieces of software that run on mobile devices. The applications on mobile devices to aid medical diagnosis and treatment have gained popularity while an estimated half a billion users are expected to utilise mHealth applications by 2015 (Merrill, 2010).

The EU and US represent the two largest medical device markets in the world. Therefore, a deep understanding of the regulatory process for mobile health applications and medical devices is fundamentally important to current and potential manufacturers and developers of mobile health applications and medical devices. There is a need for a better understanding and more detailed study of the regulation policies that manufacturers of mobile health applications have to consider.

The Food and Drug Administration's (FDA) current mission is to promote, protect and advance public health in the US[3]. Specifically concerning medical products such as mobile health applications, the FDA's role is to regulate the marketing and subsequent utilisation of medical devices. There are three FDA regulatory classifications of such devices: Class I, Class II and Class III. The classifications are assigned by the risk that the medical device presents to the patient and the level of regulatory control the FDA determines is needed to market the device legally. As the classification level increases, the risk to the patient and the required regulatory controls increase.

Similar to the regulations of the FDA, the main purpose of the relevant European directives is to allow free movement of medical devices throughout the European Community, whilst ensuring device performance and safety. The directives replace any previously existing  national systems in each Member State. Medical devices, as defined by the directives[4], generally carry a 'CE' mark to show that they comply with the essential requirements that products must meet. Three directives regulating the safety and marketing of medical devices throughout the EU came into effect on 1 January 1993. Over time, they have been supplemented by several modifying and implementing directives.

In parallel, the US and the EU Cooperation on eHealth Memorandum of Understanding[5] plans to foster a mutual understanding of challenges faced by both continents in the effective use of eHealth related technologies and software. It argues that there is a need to strengthen the global cooperation in mobile health apps in order to facilitate a more effective use of smartphones and other relevant technology and software.

[1] www.medscape.com/viewarticle/803503

[2] www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf

[3] www.fda.gov/opacom/morechoices/mission.html

[4] www.mhra.gov.uk/home/groups/es-era/documents/publication/con007494.pdf

[5] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1784

This paper therefore seeks to provide an overview of the CE and FDA marking processes for the regulatory approval of mobile health applications, to address safety, efficacy and reimbursement considerations, to provide a comparison of both regulatory processes, and to present upcoming modifications of these regulations that may present potential implications for software developers and medical device manufacturers. In Section 2, the paper provides a short overview of the FDA and CE marking processes for regulatory approval of mobile health applications. It addresses the specific steps that are necessary for mobile health applications to obtain FDA and CE approval. In Sections 3 and 4 respectively the paper describes the basics of the FDA and CE mobile app approvals process for two use cases: i.e., FDA approval of myVisionTrack and CE marking for SmartWatch, which targets among others the elderly population.

More specifically:

- ‘myVisionTrack’ is an iPhone 5 compatible mobile health app that allows patients with degenerative eye disease such as diabetic retinopathy (DR) and Age Related Macular Degeneration (AMD) to quickly and accurately test their own visual function at home. It has been recently approved by the FDA;
- The Android SmartWatch-compatible mobile health app, which is currently under development, will unobtrusively record behavioural indicators of elderly people, such as cognitive decline, emotional status and health vital signs. Its development is funded by the FP7 EU research project USEFIL, and the project partners intend to apply for CE approval for the app.

Finally, the paper discusses and compares the CE marking and FDA mobile health app regulations.

In order to provide greater depth of insight in a paper of such limited scope, the focus of the discussion is specifically on the regulation surrounding these two specific mobile health application use cases. Although the decision to analyse only two use cases, that are both different in nature, can be considered as a limitation, this is nevertheless one of the competitive advantages of this paper. By specifically focusing on different use cases, an in-development in the EU mobile health app and an off-the-shelf mobile health app in the US, allows the identification of key requirements of CE and FDA marking. This investigation is important for the companies involved in the development of mobile health apps, from the design phase of the app to its commercialisation phase.

With large-scale changes to ICT technologies and mobile health applications, a portion of this paper discusses potential implications of the upcoming modifications on the specific regulations regarding health applications. Furthermore following the EU-US Cooperation on eHealth Memorandum of Understanding (MoU) that has been signed highlights the need for harmonisation in this domain.

## 2. Basics of mobile health applications (FDA vs CE)

This section of the paper explores the basic differences between how mobile health apps are considered by both the FDA and CE markings and other considerations. It covers an overview of requirements and of the relevant challenges in both the US and the EU; various barriers to approvals processes; hardware, software, and network considerations; and essential patient considerations.

## 2.1 Overview of requirements for mobile health applications

Mobile health applications can take a number of different forms. However, it is critical to note that the FDA will apply its regulatory overview to only a subset of mobile health applications as listed in the guidance document[6]. Similarly, mobile health applications that transform a mobile platform into a regulatory mobile device will also fall under the particular regulatory overview. Mobile apps that the FDA does not consider to be mobile health apps can be, among others, apps that perform the functionality of an electronic health record system or personal health record system[7]. There are three classes of regulatory control for mobile health apps intended for medical use[8].

EU regulations that deal with mobile health applications are still under a process of modification. Regulators are struggling to keep pace with the ever-evolving technology innovations. Despite this challenge, every mobile health app that influences an end user's health condition is subject to consideration as a regulated entity. Developers should assess the existing regulations and determine if it should carry the CE mark to demonstrate its conformity with the appropriate regulation.

The Medical Device Directive 93/42/EEC[9] is the primary source of regulation governing electronic health applications across the EU. Article 1 of the directive in Article 1 defines what constitutes a medical device, how medical devices should be regulated according to different classifications, and how devices should be marked to demonstrate their conformity. This directive was most recently reviewed and amended by the 2007/47/EC[10] and a number of changes were made. Compliance with the revised directive came into effect on 21 March 2010 which amended the definition of a medical device to include the reference to standalone software used for diagnostic and therapeutic purposes. This amendment simply clarified that mobile health applications could be regarded as being medical devices when intended to be used for one or more of medical purposes such as diagnoses, suggestions and treatment.

Following the EC's latest guidelines[11], which date, from January 2012, software is a medical device if it has a controlling function, such as drug delivery. Similarly, the MHRA[12] appears to be drawing a line between software that simply stores and retrieves medical data and more sophisticated applications such as mobile apps that produce diagnoses.

One interesting challenge to EU member nations is to establish a harmonised regulatory approach for all countries. Each member country has its own national legislation and national competent authorities. Unfortunately, this generates country-by-country variations with regard to how the European directives have been transposed into national law.

Although many directives have been produced, there is still more that needs be done regarding the regulation framework of mobile apps. Within this realm, the mHealth Regulatory Coalition[13] is now extending its efforts to Europe while the EU is planning new regulations[14] for medical devices. The regulators are addressing some fundamental concerns such as regulating wellness versus disease, accessories to medical devices and standalone software and privacy issues.

[6] http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmaunderstandingmedicaldeviceregulationformhealthreport1.pdf
[7] http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm263280.htm
[8] http://www.slideshare.net/RockHealth/fda-101-a-guide-to-the-fda-for-digital-health-entrepreneurs
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF
[10] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2007:247:0021:0055:en:PDF
[11] http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf
[12] http://www.mhra.gov.uk/Howweregulate/NewTechnologiesForums/DevicesNewTechnologyForum/Forums/CON084987
[13] www.mhealthregulatorycoalition.org
[14] http://ec.europa.eu/health/medical-devices/files/revision_docs/com_2012_540_revision_en.pdf

Despite the regulatory uncertainty, mobile health apps - both for payment and free of charge - must comply with the current CE regulation framework under the Medical Devices Directives. The developer/manufacturer has to determine the correct risk class for the app following the classification guidelines MEDDEV 2. 4/1 Rev. 9 June 2010[15].

## 2.2 Overview of challenges

Here, two sets of challenges are explored: those that affect the US and those that impact the EU. Generally, the challenges cover such issues as policy directions, enforcement, and the pace of technology development.

In the US, there are over 40 000 medical applications available for download on smart-phones and tablets. Which ones need FDA approval? The FDA has proposed policing only those apps that use supplemental attachments to transform a mobile platform into a medical device and others that act as accessories to an already regulated medical device[16]. However, that said, the draft guidance from the FDA regarding the certification of a mobile platform as a medical device still lacks of clarity. It has caused the FDA to open several cases in which manufacturers have asked for relevant certification. Together with the fact that the FDA certification process is quite specialised and requires a certain degree of qualification, it is advisable for the manufacturers/developers to bring an experienced consultant in-house, who has worked with the FDA before if possible, in order to provide long-term consultation and develop methods that are workable and appropriate for the company.

In Europe the progressive ageing[17] of its population is leading to an increase in the proportion of people with disabilities, mental disorders, cancers, and experiencing strokes, dementia, depression and chronic illnesses such as diabetes, heart diseases and respiratory conditions. This is resulting in new demands being placed on society's care and medical services.

The medical device and in vitro diagnostic medical devices sectors have already proven to be key drivers of European economic growth while electronic health apps and technologies save time and money for patients, healthcare providers and social security systems. However, to comply with the necessities of the Europe 2020 Strategy for Innovation Union[18], the Digital Agenda for Europe, the eHealth Action Plan  and the Directive on the application of patients' rights in cross-border healthcare[19] there is need to achieve interoperable electronic health services in the Union. Following GSMA[20] comments regarding the upcoming revisions in the regulation framework, the EU needs to focus on and consider the mobile medical device definitions and classification, 'intended use', boundaries between wellness and medical solutions, the risk assessment of mobile health apps, the standards and the clarity on regulatory status, post-market surveillance and traceability.

[15] http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf
[16] www.fdanews.com/store/product/detail?productId=40513
[17] http://ec.europa.eu/economy_finance/publications/european_economy/2011/pdf/ee-2011-4_en.pdf
[18] http://ec.europa.eu/research/innovation-union/pdf/innovation-union-communication_en.pdf
[19] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:FULL:EN:PDF
[20] http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf

## 2.3 Approval steps and barriers to approval

In the US, the Premarket Notification[21] - also called PMN or 510(k) - process requires considerable investment in both time and financial resources. An independent study conducted by a number of parties, including the Medical Device Manufacturers Association, the National Venture Capital Association and Stanford University medical professors, concluded that the average approval time for a 510(k) application was 31 months from the first communication to the FDA and 10 months from the first filing for clearance. The FDA's 510(k) approval process is cumbersome, costly and time-consuming. All these constraints come together to create a wall of regulatory hurdles that could stifle mobile medical app innovation[22]. Another issue is not being able to talk to the FDA during the time of writing a 510(k) application. The whole process seems to be frustrating for the applicant because every organisational group in the FDA seems to work in its own way. Since there is no feedback provided from the FDA following their internal process, it is advisable for the applicant to hire consultants with FDA experience and wait for the FDA review.

To define the criteria for the qualification of mobile applications in the EU, used in a healthcare setting, EU the guidelines[23] relating to medical devices and the application of the classification criteria to such software must be applied. The current classification rules were formalised as a regulation in 2010 and were not written with software in mind. The definitions[24] of the 'intended purpose', the 'accessory', the 'modules', the 'medical device', the 'active medical device' and the 'standalone software' can help a manufacturer to define the classification of its mobile health app in the EU.

Mobile health apps can be considered as standalone software since these can provide immediate decisions triggering information (e.g. heart rate, blood glucose meters and others) and support for healthcare professionals (e.g. ECG interpretation). The decision matrix shown in the EU Flowchart for Qualification of Software (SW) as Medical Device[25] can help identify a regulated mobile medical app. The key test is whether the application provides a proper diagnostic or therapeutic purpose and if it influences a clinician - and possibly a patient- and results in subsequent therapy.

Standalone software must have a medical purpose to be qualified as medical device. For example, such software could carry out calculations or interpretations of patient data captured for a therapeutic purpose or could carry out calculations, enhancements or interpretations of data captured for a diagnostic purpose. Standalone software that meets the definition of a medical device shall be considered as an active medical device (Annex IX, section 1.4, of Directive 93/42/EEC). Only the intended purpose of the product as described by the manufacturer is relevant regarding the qualification and classification of any device, even if a user decides to use it for a medical purpose. According to Rule 10 of Annex IX to Directive 93/42/EEC, active devices intended for diagnosis are in Class IIa, i.e., mobile health apps for the presentation of the heart rate or other physiological parameters (such as vital signs).

[21] http://en.wikipedia.org/wiki/Federal_Food,_Drug,_and_Cosmetic_Act#cite_note-19

[22] http://thehealthcareblog.com/blog/2012/10/24/a-coming-storm-fda-regulation-of-mobile-medical-applications/

[23] http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf

[24] http://ec.europa.eu/health/medical-devices/files/meddev/2_1-1___04-1994_en.pdf

[25] http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf

## 2.4 Hardware, software and network considerations

In the US, a governing principle in medical device regulation for the FDA is that it applies medical device regulations to a product or service based on the intended purpose of the product and its mode of action. This enables the manufacturer to decide whether the product will fall within the scope of the regulations for medical purposes or not. The FDA makes a clear distinction between a mobile medical application, and an accessory medical device or a medical device component; each of which is regarded and managed differently in the FDA regulation process. The hardware elements of a mobile health solution may include sensors, mobile phone and an associated network, accessory or a component of a medical device, depending on the construction of the specific product and the intended use. The FDA Proposition for Mobile Medical App Classification[26] illustrates the decision tree used to determine whether the mobile health app should be regulated.

Software development may, however, be assigned to an external organisation that will not manufacture the device. However, the manufacturer remains accountable, according to regulations, to ensure quality standards that must be applied such as ISO 13485, ISO 14971, and software standards that are accountable for ensuring and verifying that the standards have been met. Currently distributors (for example, iTunes) are exempt from medical device regulation, however app authors are required to follow limited template development rules. Some distributors undertake a perfunctory peer review to check the performance of the app (according to generic app guidelines). Mobile health apps will have to undergo a more rigorous development and approval process such as post-market maintenance, version control, surveillance reporting of adverse events and others. The app author therefore needs to consider how these requirements will be met. If the app is marketed for medical use then the development process is affected by the FDA's medical device regulation which involves supporting specification, testing and documentation according to ISO 13485.

Regarding the general purpose technologies used by healthcare providers (Wi-Fi, cellular, mobile medical networks or any other Internet channels), these typically do not qualify for medical device regulations.

In the EU regulators[27] draw a distinction between a medical device, an accessory and a component, each of which is regarded and managed differently in the regulations. This raises the issue as to whether a whole product can be CE marked when not all applications and subsystems have a medical purpose. It is the obligation of the manufacturer/vendor/developer to identify the boundaries and the interfaces of the different subsystems/modules/applications. The applicant must also ensure application of the quality system approved for the design, manufacture and final inspection of the products concerned. According to the Data Set Change Notice (DSCN)[28] 14/2009 the whole combination of software modules and hardware components, including the connection system, must be safe and must not impair the specified performances of the modules which are subject to the medical device directives.

[26] http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmaunder-standingmedicaldeviceregulationformhealthreport1.pdf

[27] www.gsma.com/connectedliving/wp-content/uploads/2012/03/gsmaunderstandingmedicaldeviceregulationform-healthreport1.pdf

[28] http://www.isb.nhs.uk/documents/isb-0129/dscn-14-2009/dscn142009v12.pdf

In 2011 the Council of the European Union[29] invited the Commission and the Member States to pay particular attention to interoperability and safety issues related to the integration of medical devices in eHealth systems, especially personal health systems and mobile health systems (mHealth). The various standards[30] for medical devices that have been developed in Europe are not mandatory. However, they are almost universally applied in design, development and manufacturing of medical devices.

Under the existing regulatory framework[31], a medical device should conform to the essential requirements if it meets the appropriate harmonised standard. The international standard EN/IEC 62304 has now emerged as a global benchmark for evaluating software development. This standard expects a manufacturer/developer/vendor to assign a safety class to the software application based on the potential for injury that could result to the user, the patient or other people.

According to EU regulation directives, 'serious injury' means life threatening, permanent impairment of a body function or permanent damage to a body structure that necessitates for medical or surgical intervention. Most health apps are expected to be classified under Class I. Standalone software is considered to be an active medical device. The rule set for classification of these devices is relatively straightforward[32].The classification of the medical devices has an impact on the conformity assessment route that the manufacturer should follow in order to affix the CE marking on the medical device. This is illustrated in the CE Marking Conformity Assessment Matrix[33]. Technical documentation relating to products in both Class IIa and Class IIb must be reviewed by a notified body[34] (which is an organisation that has been accredited by a European Member State to assess whether a product meets certain preordained standards).

Communication systems are usually based on software for general purposes. They use a transmitter to send the information over the Internet, a landline telephone or a mobile network and handle both medical and non-medical information. They do not fall within the definition of a medical device. Examples include video appointment software. Communication systems such as radio and telecoms equipment that is marketed in the EU have to comply with the Radio and Telecommunications Terminal Equipment (RTTE) Directive[35] in order to place a CE Mark on these products.

## 2.5 Post-approval requirements and considerations

The FDA states that mobile medical applications and mobile health apps intended as medical device, their manufacturers and other firms involved in the distribution of such application must follow certain requirements and regulations once devices are on the market. These include tracking systems and applications, reporting of application or device malfunction, serious injuries or death, and registering the establishment where application or devices are produced or distributed. Medical device reporting is another area where mobile medical devices differ from conventional mobile devices. The goal of the regulation is to detect and correct problems in a timely manner in order to assure the safety of end users. In order to report device-related deaths, serious injuries and reportable malfunctions, the FDA requires distributors and manufacturers to certify and place appropriate systems to enable reporting of problems.

[29] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:202:0007:0009:EN:PDF

[30] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=54892

[31] http://europa.eu/legislation_summaries/internal_market/single_market_for_goods/technical_harmonisation/l21001d_en.htm

[32] http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf

[33] http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf

[34] http://en.wikipedia.org/wiki/Notified_Body

[35] http://ec.europa.eu/enterprise/sectors/rtte/index_en.htm

At the European level, post-market activities can be divided into proactive and reactive categories following the European directives[36]. The vigilance and post-market surveillance directive[37] seeks to improve the protection of health and safety of patients by reducing the likelihood of similar incidents being repeated. The regulation and guidelines require the developer/vendor/manufacturer to immediately notify the competent authority if the product has led, or might have led, to a death or caused a serious injury or serious deterioration in the state of health.

## 2.6 Patient considerations

There may be various considerations that are important for patients. They can include patient identities (IDs), security, privacy, and ease of use.

Irrespective of whether a mobile health app falls within the FDA's regulatory authority, developers, manufacturers and patients (users) must consider the significant privacy and security concerns surrounding mobile healthcare technology. Any mobile health app that can store or transmit protected health information and can be used by a covered entity like physician, healthcare facility or health plan, will mostly fall within the purview of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[38]. Although HIPAA compliance stands outside of FDA guidelines, it remains a critical consideration for patient data safety and security. This includes any mobile medical app that permits physicians and patients to communicate about protected health information.

A mobile health app used solely by an individual, such as an app that allows the individual to track dietary intake, weight and exercise, is not covered by HIPAA. However, once the information is transmitted to a covered entity, whether directly to a physician or uploaded onto a health plan's server, the information will fall under the HIPAA requirements. Any mobile health app which needs to transmit protected health information must comply with the HIPAA regulations, including utilising password protection and implementing policies related to lost or stolen devices. The HIPAA also proposes default password encryption for data stored in certified electronic health record (EHR) technology, after recent findings that nearly 40 % of large data breaches involve lost or stolen devices[39]. Developers also need to ensure that mobile health apps allow the secure and confidential transmission of data.

In Europe, since mobile Health is a new market and the regulatory environment is evolving, EU directives are trying to safeguard the public while at the same time supporting innovation. Appropriate legislation[40] should give patients, consumers and healthcare professional's confidence in the mobile health apps which they might use every day. Based on a practical guide[41], specific recommendations should be considered regarding mobile health applications. Furthermore the developers and the publishers should consider the ethics, privacy and security issues that should be borne in mind during the development of the mobile health apps. In that case, they should proceed with design based on ISO 27000 Standard[42] with HIPAA[43] and EU Data Protection Directive[44] 95/46/EC compliance in mind. This would permit them to set strong access and authentication policies, unique user identification/patient ID, protection of data measures such as secure logins and SSL, and to separate data both physically and logically.

[36] Active Implantable Medical Devices Directive (AIMDD 90/385/EEC - Article 8 and Annexes II, IV, V)
Medical Devices Directive (MDD 93/42/EEC - Article 10 and Annexes II, IV, V, VI, VII)
In-Vitro Diagnostics Devices Directive (IVDD 98/79/EC-Article 11 & Annexes III, IV, VI)

[37] http://ec.europa.eu/health/medical-devices/files/meddev/2_12_1_ol_en.pdf

[38] http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[39] http://mobihealthnews.com/18314/stage-2-meaningful-use-regs-account-for-popularity-of-mobile-devices/

[40] http://ec.europa.eu/health/medical-devices/files/revision_docs/com_2012_540_revision_en.pdf

[41] http://www.d4.org.uk/research/regulation-of-health-apps-a-practical-guide-January-2012.pdf

[42] http://www.27000.org/

[43] http://www.hhs.gov/ocr/privacy/

[44] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

## 3. FDA – MyVisionTrack use case

As described in the product brochure, 'myVisionTrack is an accurate, portable, and user-friendly system that allows patients with degenerative eye disease such as diabetic retinopathy (DR) and Age Related Macular Degeneration (AMD) to quickly and accurately test their own visual function at home'[45]. MyVisionTrack received FDA class II approval on 22 February 2013 for use with the iPhone. Users can quickly and efficiently monitor their condition at their convenience using an iPhone. The results are stored and compared with prior tests. Any test that is statistically significant is forwarded to the physician's office for further evaluation. The application uses a shape discrimination hyper acuity (SDH) test[46] as illustrated in Figure 1.

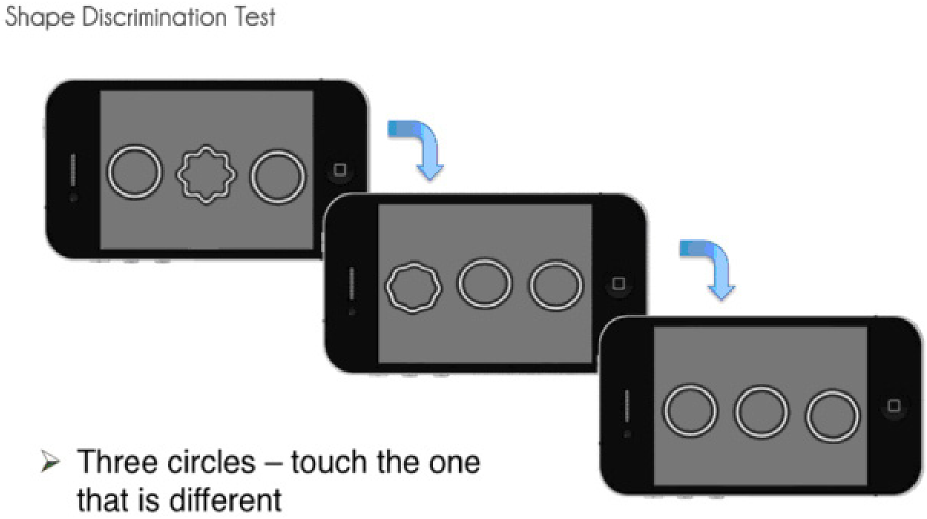

Shape Discrimination Test
➢ Three circles – touch the one that is different

**Figure 1:** myVisionTrack SDH Example

The SDH test is administered on the iPhone. The user is presented with three circular shapes. One is distorted and the other two are undistorted. The user is required to identify by touch input which of the three shapes is distorted. The results of each test are forwarded to the clinician for future evaluation.

### 3.1 Clinical application

There are five primary applications for the myVisionTrack solution[47]. The product provides value via self-monitoring of the disease progression. It assists in early diagnosis of disease and it enables more timely treatment of the condition which can result in improved compliance. It also offers a more efficient treatment pathway whereby user visits can be coordinated with the progression of the disease.

[45] http://myvisiontrack.com/myvisiontrack/myvisiontrack-overview/
[46] http://www.iovs.org/content/43/6/2055.full.pdf
[47] http://myvisiontrack.com/myvisiontrack/applications-for-myvisiontrack/

## 3.2 Changes from current state of the art

Prior to using myVisionTrack, users would need to have scheduled an appointment with a clinician. They would then spend time travelling to the clinician's office. Finally, they would take an on-site vision test and have a clinician evaluate the results. This approach consumes considerable resources on the part of both the user and the clinician. With myVisionTrack, the test is administered by the user at their convenience and any statistically significant results are automatically sent to the clinician for further evaluation.

myVisionTrack can be used in combination with a drug therapy such as Macugen[48], Lucentis[49] and others. These therapies are typically administered monthly through injections in the eye. myVisionTrack is an effective complementary diagnostic tool for this condition. Users can perform regular and frequent in-house testing without the inconvenience of scheduling an appointment with the clinician. The diagnostic results are used to ensure that treatment is performed as the disease progresses rather than at some scheduled interval. Treatment is performed more or less often depending on the user's condition rather than at a fixed interval. Test frequency and treatment is coupled to disease progression rather than physician/user schedules.

## 3.3 Safety considerations

The myVisionTrack app is a medical diagnostic solution. The test is administered at home by the user using an iPhone. The primary FDA concern is that the test results are interpreted by the clinician and not the user. In fact, the test results are not even made available to the user. Currently, all results are transmitted to the clinician for evaluation. The FDA is very concerned that the user might use the test data to decide not to go to their usual doctor appointments, and so it preferred that the user did not have ready access to the test results.

This is the fundamental concern for mobile app solutions. These technologies, like myVisionTrack, are available by 'prescription only'. Mature home diagnostic technologies like weight, blood pressure, blood glucose and pulse oximeters are approved for 'over-the-counter' use. In every case, these do allow the user to evaluate results.

## 3.4 FDA approval

Regulatory consideration is a critical component of any medical device business model. The myVisionTrack team knew from early on that, for doctors to use the product in their daily practice, it had to have regulatory approval.

Independent clinical trials for myVisionTrack were completed in December 2011. The 510(k) application was submitted to the FDA on 12 June 2012. The FDA put the application on hold and requested additional information which took nearly five months to process. The responses were filed on 16 January 2013 and FDA approval was received on 22 February 2013.

Several factors contributed to the lengthy approval timeline. The application's principal author, Michael Bartlett, President of Visual Art and Science Inc., had never written a 510(k). In addition, the regulatory consultant his company hired was not familiar with software-based medical devices. Lastly, the FDA-required IEC-60601-/2[50] certification took many months to achieve.

[48] http://en.wikipedia.org/wiki/Pegaptanib
[49] http://en.wikipedia.org/wiki/Ranibizumab
[50] http://www.iso.org/iso/catalogue_detail.htm?csnumber=45605

Mr Bartlett predicts future applications should go much quicker. ‘This first time through we did not know what the FDA would require, and our predicate was similar to our test, but different in several ways. In future filings our now approved app would be the predicate and so the changes from the predicate will be much smaller, and we [will] know what to submit.’ However, the regulatory landscape is still evolving, and therefore may introduce new requirements with future filings.

Perhaps the most important consideration when developing a medical app is the cost of regulatory approval. Mike Bartlett estimates the 510(k) process increased development cost by a factor of 10 times. ‘If we had just defined our vision test, coded it up with a little testing and released it on the App Store we think it would have taken six months and cost less than $100k.’

To develop a medical device according to FDA requirements needed the following steps. ‘To do all this we estimated that it took us four years and over $1 million. This is still cheaper than development of most FDA 510(k) approved devices which are normally quoted as being in the range of $5-15 million cost.’

1. Implement a quality system – Visual Arts and Science Inc. is independently ISO 13485 certified and all work was performed and documented as per the prescribed process (IEC 62304 and IEC 62304 - Medical Device SW Quality Control)
2. ISO and IEC standards compliance – Compliance to ISO and IEC standards including ‘ISO 14971-Risk Analysis and Management’, ‘IEC 62304 - Software Life Cycle Processes’, ‘IEC 62366-Usability Engineering’ and ‘ISO 14155 Clinical Investigations of Medical Devices’ Independent Certification of the iPhone with the app running on it to:

- IEC 60601-1 Medical Elec. Equip. – Basic Safety
- IEC 60601-1-2 Medical Elec. Equip. – Electromagnetic

3. Cross-sectional clinical studies – Clinical studies to ensure the target users could effectively use the app.
4. Longitudinal Studies – Two in-home user studies. The first study involved 36 users for 6 months. The second involved 160 users in 24 centres around the US using the device at home for four months. The second study was funded by a large pharmaceutical company and cost an additional $2 million.

The regulatory uncertainty was perhaps the biggest issue faced by the myVisionTrack team. Not only are the regulations under development, but finding qualified consultants and achieving access for small businesses to the FDA is a challenge. Mr Bartlett points out: ‘The biggest issue we [faced was] not being able to talk to the FDA during the time we were writing up our 510(k) application. You file and then they tell you what else they want.’ Without feedback it can be difficult to understand what is required by the FDA. Mr Bartlett continues: ‘The only method was to do the best you could on the application and then wait to see what they would come back with.’

One final consideration of software apps are software and hardware changes. The FDA has regulatory demands that require the manufacturer to identify major and minor changes. Any major changes must go back through FDA for approval: for the moment this includes any hardware platform changes. Minor changes must be well documented and verified but do not require FDA approval.

## 3.5 Reimbursement

There is no proven model for reimbursement of mobile health apps. One possible option is to follow the current mobile apps model and require users to self-pay the app stores.

However, there are a number of challenges for this model. First, US consumers are not used to purchasing medical devices directly from manufacturers. Secondly, targeted distribution to users – meaning prescription-based download – is not supported in the app stores. A third challenge is the development of new codes for health apps and their application. This is both time-consuming and expensive and adds an additional barrier to reimbursement.

Another reimbursement option is to partner with an existing therapy. Mobile app reimbursement may come from direct payment from the partner. For example, myVisionTrack has worked closely with a large pharmaceutical company in clinical trials. The partner may provide the app to the user for free and reimburse myVisionTrack directly.

## 3.6 Conclusions and observations

FDA approval of a medical app is a costly endeavour – both in terms of time and money. Approval can take up to a year as the myVisionTrack example shows. The monetary investment can exceed ten or more times the cost of non-regulatory solutions. Therefore, careful consideration of the business case, marketing message and potential Return on Investment (ROI) must be undertaken very early in the lifecycle of the product.

The regulatory process itself is under construction. The FDA's draft regulation is under revision and the publication of new guidelines is expected until the end of 2013. Even with updated regulations, companies should expect to encounter challenges with this process due to the 'newness' of these technologies and their application, a shortage of qualified regulatory consultants, and the 'art' of regulatory approval. Companies will have to be nimble in traversing this regulatory minefield.

FDA's fundamental concern with these emerging diagnostic tools is how it may influence the user's reaction to treatment. There is clearly an upside – as the myVisionTrack illustrates – users can perform diagnostic tests at 'their' convenience rather than having to make it to traditional scheduled visits to the clinician's office. In addition, this diagnostic data can be made available to clinicians in near real-time so that they can treat the disease more effectively as it progresses. However, the design must eliminate any consideration that the user performs self-diagnosis. myVisionTrack addressed this issue by eliminating any testing feedback from the app going to the user, thereby requiring the clinician – rather than the user – to evaluate, interpret and treat the disease. This eliminates any possibility of the user skipping appointments and keeps the clinician in control of the therapy.

# 4. CE Marking - Smartwatch use case

The USEFIL project[51], aims to address the practical needs of elderly people by developing advanced unobtrusive monitoring and web communication solutions that will assist older adults in maintaining their independence and daily activities. The applications that will be developed will unobtrusively record elderly people's behavioural indicators such as cognitive decline, emotional status and health vital signs. Technology implementation will be based on user acceptance and an understanding of user interactions that will truly address user needs. The project will use an off-the-self Z1 Android Smartwatch[52] as shown in Figure 4.

[51] www.usefil.eu

[52] http://en.wikipedia.org/wiki/Z1_Android_Watch-Phone

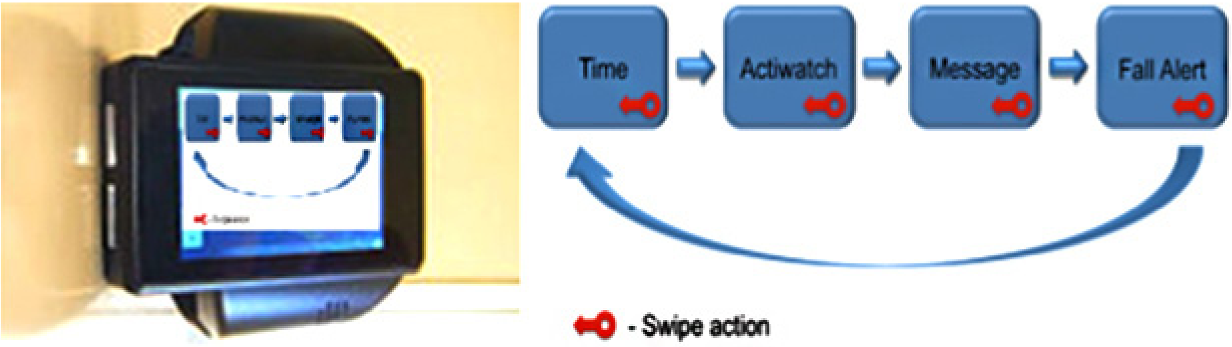


**Figure 4:** Z1 Android Smartwatch

This device is an unlocked GSM quad-band smartwatch. The device uses the Google Android version 2.2 operation system giving software developers the freedom to create many mobile apps. The Smartwatch[53] provides smartphone functions to its users through a Capacitive Touch screen, a Wi-Fi, web browser, a 2.0 MP camera, a G-Sensor, Bluetooth functionality, a mass storage device SD card, a multimedia player and recorder for music (mp3) and video (mp4), and an internal GPS antenna that supports satellite navigation.

The Smartwatch will be used to monitor the user continuously anytime and anywhere and provide the relevant ease of use mobile apps. The Smartwatch is assumed to be ubiquitous; thus experiments will not interfere with the subjects in research habits as they usually do in the case of using additional sensors. As motion is an important modulator of other vital human organic functions such as respiration, heart rate, blood oxygen saturation and pressure, the automatic classification of human motion during daily activities is also important in completing the puzzle of preventive medicine. The monitoring of elderly people and their vital signs monitoring will be conducted using solely the Z1 internal sensors.

The mobile applications that will be developed will monitor low-level events which will produce the high level events illustrated in Figure 5 through the use of data fusion algorithms.

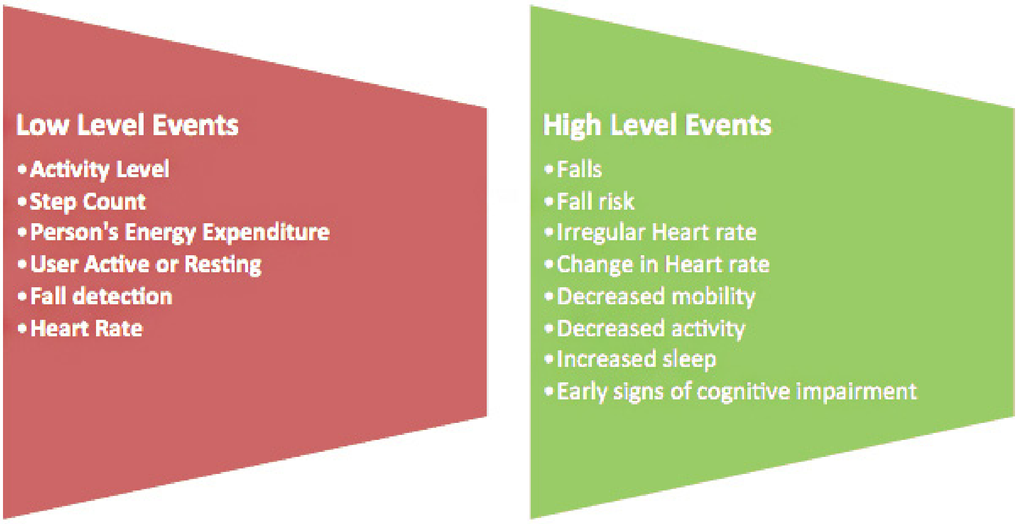


**Figure 5:** Low-Level and High-Level events from the Z1 Android Smartwatch

[53] http://www.pegaso2.biz/public/Pegaso2/asp/dblog/articolo.asp?articolo=262

## 4.1 Clinical application

Detection of activity behaviour forms an important element of health policy approaches for older people. Z1 Smartwatch will be able to monitor and track different activity parameters whilst the user carries out different daily activities. Techniques to detect deviation from normal activity signatures can be derived and used to issue an alert when changes are detected – even subtle changes. This has been shown to be possible using an accelerometer to monitor changes in activity destined for use with psychiatric users (James et al., 2008).

## 4.2 How this app changes the current state of the art

The USEFIL mobile monitoring application goes beyond the limited functionalities of the commercial monitoring devices and provides a more generic solution in terms of monitoring and combining several parameters, to prevent or mitigate the consequences of adverse health events (if such events occur) as well as to assist diagnosis.

## 4.3 Disease state and value added offer of the mobile health app

The latest trends on ageing indicate that healthcare systems are likely to face 'substantial challenges in the future' with public expenditure on healthcare likely to grow by 1.5 % of GDP across the EU by 2060. Civil society has a common desire to prolong the period of independent living for elderly citizens (Prigerson, 2003). In this context, the provision of healthcare services using ease of use health applications is seen to be one of the several elements helping the containment of healthcare delivery costs[54] while maintaining the expected levels of quality of care and safety (Stroetmann, 2007).

The proposed unobtrusive in nature wrist-worn mobile unit equipped with the mobile health app promises proven concepts for early detection of ageing-related risks and substantial reduction in cost while reducing hospitalisation through provision of precise assessment of health status and improved health management of the elderly people while staying independent in their residencies.

## 4.4 CE Marking approval

Regulatory consideration[55] is a critical component of any medical device business model. The app will be used on its own to supply information for detecting, diagnosing and monitoring physiological conditions and states of health. Therefore, the app is considered to be a 'stand alone software' and an active medical device. According to Rule 10 of Annex IX to Directive 93/42/EEC, active devices intended for diagnosis are in Class IIa if they are intended for direct diagnosis or monitoring of vital physiological processes.

The regulatory approval efforts for the mobile health monitoring app will start after the clinical trials for the app are completed in October 2014. Therefore, the developed monitoring mobile health app will be considered as an active device for diagnosis. The modules of the application have to be identified that will be classified as an active medical device having in mind that:

- Monitoring of heart rate (i.e., vital physiological sign) during daily routine check-ups will be conducted.

[54] http://www.continuaalliance.org/static/binary/cms_workspace/IEEE_Pervasive_Computing_Q407_Continua_Article_2.pdf

[55] Annex IX, section 1.6, of Directive 93/42/EEC

- Monitoring of activity data which produce diagnosis for health-related cases.
- Mobile phone, telephone network, database and website are general-purpose systems and are not designed for a medical purpose.
- No specific medical function is implemented in the transfer of data. Meaning that no changes are made to the original data transmitted by the mobile phone to the personal health record through the Web, the translation of the data from binary to HTML format does not change the initial data but brings it into another format and the user device data presented on the Web for the medical personnel to work with this data cannot be changed.

Three validation studies will validate different aspects of the app such as its usability of the application (meaning the ability of the target patients to effectively use the application), its ability to provide diagnosis, provide data protection and secure privacy. These will provide the necessary evidence for the safety and efficacy aspects of the application that will ensure the activities for the CE regulatory approval.

## 4.5 Reimbursement

Although mobile health apps are booming, reimbursement payments for mobile or remote care are largely limited to remote rural areas. According to studies[56], the transformation of a system of incentives from pay-for-service to pay-for-performance is likely to take time which may slow down the adoption of mHealth technology. The main question, after the mobile app will be placed in the market, is whether to seek reimbursement or not. To get reimbursement directly from health payers, although it's a time and effort consuming complicated exercise, bares huge benefits since reimbursement status makes the technology widely available to the majority of the population and allows controlling costs.

So potential approaches could be the following:

- Understand exactly which agency pays for what in any particular country that is considered to be a potential market.
- Target the 'social care systems' since these are funding the most mature of all mobile health applications in the form of 'social alarms' for the elderly.
- Look for reimbursement status in the countries that are friendly oriented towards health mobile applications and services.
- Start promoting the application and influencing the policy environment in potential markets and countries while trying to convince the key stakeholders that the application will provide them innovation and tangible value creation.
- More specifically the benefits of the solution should be addressed emphasising the competitive advantage of the mobile health app.

This competitive advantage concerns the power of the app to address the problems of early detection of ageing-related risks and in particular the ability to reduce system costs by reducing hospitalisation. This will be done through provision of precise assessment of health status and improved health management of elderly people whilst remaining independent by staying in their own residence, thus achieving dramatic improvements in health outcomes at a low cost

[56] http://www.ey.com/Publication/vwLUAssets/mHealth_Report_January_2013/$FILE/mHealth%20Report_Final.pdf

## 4.6 Conclusions and observations

The USEFIL mobile application is currently under development. It is expected to go for clinical and pilot trials within the last quarter of 2013. Regulatory activities are expected to begin towards the end of 2014. The CE mobile health app regulatory process itself is currently under development and changes are anticipated in the regulations that may influence the project. Despite the regulatory uncertainty development of the mobile app will be conducted under the current regulations. The following are some concerns regarding the project:

- Consider the business case of the mobile health app, with continuous consideration of the potential competition;
- Achieve early and continuous involvement of a notified body (summer 2014);
- Have as guidelines the different standards that cover software development such as risk management, software development, validation of software, device life cycle and others;
- Focus on data integrity, security and privacy (since the mobile health app will deal with elderly people, their vital signs and their 'personal daily activity signature');
- Cooperate closely with the manufacturer, taking control and management of the components of the device and control the quality and advancements of the next models (since the mobile health app is closely related to the wrist mobile watch);
- Place the app in the market initially as a passive application that will not produce suggestions and diagnosis but only trends and support to the medical professionals.

# 5. Conclusions

Both the EU and US regulators are struggling to keep up with recent advances in technology. CE marking and FDA regulations have not kept pace with the technical innovations and this is most clearly seen with advances in mobile medical devices and applications. Both regulatory bodies have launched programmes to solicit feedback from the user community and update regulations. It is very clear that the FDA intends to use its authority to regulate mobile medical applications that will impact a variety of industries developing, marketing and selling mobile health products, but it is not yet evident how much the FDA intends to extend its regulatory arm. The FDA still appears to be ahead in this regard, as compared to the EU, with formal updates anticipated by the end of 2013. EU regulations are not as mature and are still in the discovery stage. Fundamental changes in CE marking regulations are anticipated in a 2015/16 timeframe.

This study has provided conclusions to inform those who are involved with the mobile health application regulation process. Several aspects of this paper offer a valuable information to a variety of different audiences. They include, among others, organisations representing the interests of health professionals and patients, policy makers and regulators, medical device companies, mobile device manufacturers, mobile network operators, software developers and the general public as a whole.

Especially the manufacturers that intend to develop mobile health apps that will produce suggestions and/or diagnosis and/or treatment and wish these apps to obtain the FDA regulation and CE mark should follow the steps that have been described in the paper. They need, of course, to bear in mind that the existing regulation framework will probably be modified in the near future. Nevertheless, the definition of a regulated mobile medical app is a grey area for both FDA and CE marking, and perhaps this is deliberate given the recent introduction of mobile devices.

There are, however, some interesting similarities between the two regulatory bodies. Both bodies treat applications that are used for diagnosis or treatment of disease as regulated medical devices. In addition, both consider software used as a controlling function – like drug delivery – to be a regulated medical app. Yet there are some subtle differences. The CE marking definition of a regulated medical app makes a deliberate point of excluding apps that are used to store or retrieve data, while the FDA's definition omits this exclusion. The FDA definition includes software that is a component of a medical device or software that is an accessory to a medical device.

The main philosophy that the EU applies to the CE marking process is primarily to ensure safety and performance complying with the necessities of the Europe 2020 Strategy for the Innovation Union. If, however, a manufacturer wishes to obtain the FDA mark then it has to consider the additional constraint of evaluating efficacy, which is indirectly but ultimately linked to healthcare reimbursements. From the above, it seems that the European approach holds a clear advantage over the US approach: this is the speed of approval, a process that does not ensure the highest level of health protection but secures effective innovation. In this case, the EU market seems more appropriate for manufacturers who wish to score a global advantage and launch their mobile health applications quickly: this is because these apps are mainly classified as Class I or II medical devices and obtain CE mark certification easier and rapidly. Contrarily, if the manufacturer decides to market its product in more than one EU Member State, then it has to consider the language requirements for the countries in which it intends to sell its products.

The paper indicates that, when developing mobile health applications for the EU, the manufacturers must obtain an overview of the directives that concern medical devices and decide on the classification of the apps which are mainly Class I or Class II. For the mobile apps of Class II, medical devices, the manufacturer's technical files/design dossiers must be examined by an accredited notified body to determine compliance with the essential requirements and plan the EU trials. If the manufacturer has a global business strategy for mobile health apps, it has to adopt a more global approach for designing the clinical studies for the health apps.

In addition to these factors, mobile health application manufacturers engaged in the EU market, and those seeking to enter the EU market in the near future, need to be aware of upcoming, large-scale changes to the European medical device regulatory framework and the CE regulatory process. More specifically, GSMA[57] comments on the upcoming revisions in the regulation framework on which the EU needs to focus, consideration mainly of mobile medical device definitions and classification, the 'intended use' and boundaries between wellness and medical solutions, the risk assessment of mobile health apps, the standards and the clarity on regulatory status, post-market surveillance, and last but not least traceability.

## 6. References

Fox, S. & Duggan, M. (2012). Mobile Health 2012 , retrieved April 10, 2013 from http://pewinternet.org/Reports/2012/Mobile-Health/Key-Findings.aspx.

James, C., Crowe, J., Magill, E., Brailsford, S. C, Amor, J., Prociow, P., Blum, J. & Mohiuddin, S. (2008). Personalised Ambient Monitoring (PAM) of the mentally ill, 4th European Conference of the International Federation for Medical and Biological Engineering, Berlin/Heidelberg: Springer 2008, 1010-1013.

[57] http://www.gsma.com/connectedliving/wp-content/uploads/2012/03/mHealth_Regulatory_medicaldevices_10_12.pdf

Merrill, M. (2010). HealthcareITNews Report: 500M to use mHealth apps by 2015, retrieved April 10, 2012 from http://www.healthcareitnews.com/print/20396.

Prigerson, H. G. (2003). Costs to society of family caregiving for patients with end-stage Alzheimer's disease. New England Journal of Medicine, 349, 1891-1892.

Stroetmann, V. (2007). eHealth for safety: Impact of ICT on patient safety and risk management, report prepared for ICT for Health Unit, DG Information Society and Media, European Commission, October.

World Health Organization (2011). New Horizons for health through mobile technologies: Based on the findings of the second global survey on ehealth. Global Observatory for eHealth Series, 3.

## Authors

**Homer Papadopoulos**
Demokritos Research Centre, Greece
homerpap@dat.demokritos.gr
http://epractice.eu/en/people/146210

**Vaidehi B.Sheth**
eClinicalWorks, USA
vaidehisheth@yahoo.com
http://www.epractice.eu/en/people/359103

**Michael Wurst**
InvisionHeart, USA
mwurst5962@gmail.com
http://www.epractice.eu/en/people/358020

# eHealth to mHealth – A Journey Precariously Dependent Upon Apps?

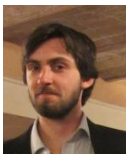
mHealth describes a particular formulation of eHealth, which allows new methods of patient treatment that are not rooted to traditional locations such as hospitals or doctors' clinics. An ever more important key tool in such efforts is the 'medical app', which utilises generic smartphone platforms to deliver patient care and management on a truly mobile basis. Whilst such methods are beginning to open up new frontiers in healthcare delivery, there are a number of concerns as to the suitability of apps, as they currently exist, for such sensitive uses. The recent Warsaw declaration on 'apps' highlights many currently unresolved problems, especially in the area of data protection. Given the sensitive nature of such medical data this poses important problems. Further question marks arise over the safety of such apps and their use as de facto medical devices. This de facto nature arises from the failure of European authorities to enforce the requirements of the Medical Device Framework, even where the app in question clearly meets the definition of a device. This paper explores these problems and their implications for the development of mHealth. In conclusion, the authors suggest potential approaches that may be able to resolve such problems.

Eugenio Mantovani

Vrije Universiteit Brussel, Belgium

Paul Quinn

Vrije Universiteit Brussel, Belgium



Barry Guihen

Centre for Society Science and Citizenship (CSSC), Marie Curie IAPP action VALUE AGEING, Belgium

Ann-Katrin Habbig

Vrije Universiteit Brussel, Belgium

Paul De Hert

Vrije Universiteit Brussel, Belgium

Keywords

App, medical device, mHealth, privacy and data protection, Warsaw Declaration

> “Incorporating privacy and safety in the world of mHealth apps.”

# 1. Introduction

Health is a matter of fundamental importance for European societies, both as a fundamental right to health care and as an element in terms of a productive workforce and economy. The right to health care (Article 35 of the Charter of Fundamental Rights of the European Union[1]) does not only cover basic health services but also extends to the use of modern technologies to arrange patient consultations, facilitate electronic patient health records and allow the possibilities of treatment delivery (eHealth). In recent times, excitement and interest have focused on the term mobile health technology (or mHealth), a particular vision and implementation of eHealth. The utilisation of information mobile health technologies could represent a tool towards achieving 'a state of complete physical, mental, and social well-being and not merely the absence of disease or infirmity', which is what the World Health Organization (WHO) considers to be good health (WHO, 1946). However, to attain these goals, mobile health solutions rely heavily on the processing of personal data and on medical devices. These circumstances do not come devoid of risk factors and threats to users and patients' privacy and security.

Starting from this premise, this paper addresses a technology for medical mobile devices that has gained importance in the last five years, mobile applications or mobile 'apps'. Apps are the primary means by which we interact with both smartphones and tablets. They can be accessed and downloaded through online stores, and are defined by the FDA (2011) as 'a software application that can be executed (run) on a mobile platform, or a web-based software application that is tailored to a mobile platform but is executed on a server.'

This research paper broaches the implications of apps in the mobile health care domain from the standpoint of European Union (EU) data protection law and EU medical device regulation.

As far as apps and data protection are concerned, this research paper reports on the privacy challenges posed by the 'appification of society' as discussed in the homonymous Warsaw declaration issued during the 35th meeting of Data Protection and Privacy Commissioners in Poland in September 2013. The roles and responsibilities of actors in the apps ecosystem are mapped out. In particular the main research question asks whether the data protection rules on user consent are apt to navigate the privacy challenges that apps pose. To this end, the research rehearses the legal framework on the processing of sensitive medical data and assesses its implications for patients using mobile health devices.

With regard to apps and medical device regulations, this research paper places apps in the EU legal medical device framework (MDF). Taking note of the failure of European authorities to engage apps in the MDF, the research question is posed in the following way: What are the safety implications that may originate from the decision not to regulate apps as medical devices even when they are used to attain medical aims?

The paper is structured as follows. The first subsection introduces apps. The following section brings apps under the EU legal framework on data protection. The third section discusses the data protection implications for apps processing medical data. Fourthly, the article describes the MDF and its relevance for software such as apps. The fifth section highlights the implications of the failure to engage the MDF on apps. The final section draws some conclusions and recommendations for future action.

[1] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

# 2. What is an app and why should we care?

This section describes the massive uptake of apps for mobile device in Europe in the past few years, explains how this technology works and provides an mHealth app example.

## 2.1 The huge uptake of apps in Europe

In Europe, we are growing increasingly used to being online continuously. Between 2008 and 2012, the percentage of people in the EU accessing the Internet from a mobile device (either a portable computer or a mobile device) rose from 7 % to 27 % (Eurostat, 2012). During this period the manner in which we access information online has also changed considerably. The original iPhone was released in 2007, with the online application, or 'App Store', opened to third party developers in July 2008. Google's Android Operating System (OS) arrived in September 2008, with its own app marketplace. In the years that followed, other companies including Microsoft and Blackberry (then known as RIM) also introduced their own online stores for customers to purchase and download applications onto their phones. Though some systems are more open than others, these systems are closed to each other so that, for example, an Apple device cannot access the Microsoft store or run software designed for a Google Android device. This new avenue for software has had a profound impact on the information and communication technologies (ICT) industry, sparking the growth of new companies and the decline of some older ones. Smart devices are changing not only how we use technology, but also how we do business, have fun, interact with others, and, indeed, the way we take care of our health.

Apps have become a mainstay of mobile technology. In January 2013, Apple announced that customers had downloaded more than 40 billion apps from their online store (Apple, 2013). Tellingly, more than half of those downloads were in 2012 alone, a figure that displays both a more dramatic rise in usage than suggested by Eurostat figures, and also highlights the increasing pervasiveness of apps in our daily lives. As recently as 22 October 2013, the Cupertino-based company announced there are now 1 million apps in its store (TheVerge.com, 2013). Apple is not alone in operating a booming online market. In July 2013, Google announced that users of devices running its 'Android' OS had downloaded more than 50 billion apps from its online store (Welch, 2013).

## 2.2 How apps work

The capabilities of apps largely depend on the hardware (device) on which they are installed. Most modern smartphones are embedded with a variety of sensors, including, but not limited to, a multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS and cameras. New devices also feature fingerprint sensors. Biometrics is a field that is becoming increasingly prominent in the area of smart devices. Some Android-based phones include basic facial recognition software, which can be used to 'unlock' the device, in lieu of or in conjunction with a pin number. Finally apps can be augmented with additional specialised hardware[2]. It is this wide suite of sensors that allow apps to be remarkably flexible: for example, they allow users to play touchscreen-based games on their devices, and then switch to a map app and receive directions from their current location to their intended destination. Map apps are illustrative of the other key feature of smart devices: they are built to be connected to the Internet at all times. Persistent connectivity allows apps installed on a mobile device to be aware of the user's location at all times, potentially building a profile over time, or set location-based reminders (for example, setting a reminder to trigger as the device

[2] For example, the US company 'Square' allows mobile credit card-based transactions through an app that works in conjunction with a hardware attachment that reads credit cards. This system is primarily designed for mobile and market sellers, effectively turning their smartphone into a teller machine.

registers that the user has entered a defined space such as an office). The flexibility offered by smart device hardware to app developers allows software for an astonishing range of purposes to be developed. There is a wide variety of categories apps can fall into, from business-oriented apps to apps designed for entertainment, navigation, or health care and well-being. As it will be shown shortly, the ability to augment smart devices with hardware attachments has also led to a rise in the number of attachments turning them into ad hoc medical devices, from otoscopes to portable EKGs.

Technically, apps depend on a continuous and smooth data flow between apps (software) and the operating system (OS) of the device (hardware). The data flow is possible through an interface called an Application Programming Interface (API). The API interface that is built into devices enables apps to access data collected by or stored in the device. For instance, apps that require access to geolocation will use the location services of the OS. The app developer will be able to access data that the OS and device manufacturers make available through the API.

Much like the hardware they run on, apps are not static. Many receive constant updates, usually in the form of big fixes or slight alterations based on customer feedback. The hardware they are installed on is also constantly shifting and evolving, with many models receiving yearly updates that increase the power of the device or tune the sensitivity of the sensors. Sometimes new hardware opens up new opportunities for apps to develop and grow, as could be the case with the introduction of fingerprint sensors. Apps-on-mobiles are powerful hardware and software that we carry in our pocket, capable of tracking our location, ‘learning’ from our daily routines and anticipating our needs. They also connect us to other people, and to other devices, becoming an extension of our desktop and personal assistant rolled into a single slab of metal, plastic and glass. We are becoming truly ubiquitous, as we are being surrounded by an increasingly ‘intelligent’ environment (Wright et al., 2008).

## 2.3 An example of an app for mHealth

This world of ubiquitous computing and communication offers us innumerable opportunities. Not only does it allow us to stay in contact with everything from online leader boards for our favourite game, bank records, brands, authors and friends.

mHealth opens up new avenues for patients’ treatment delivery and management of medical dossiers. One area in which apps are rapidly developing is health care. The following example offers an idea of the functionalities apps can offer. A team at the biomedical engineering faculty at Worcester Polytechnic Institute (WPI) in the United States developed a smartphone app that can measure heart rate, heart rhythm, respiration rate and blood oxygen saturation using the phone’s built-in video camera (Scully et al., 2012). When the user places his or her finger over the smartphone camera, the app detects the changes in the intensity of light passing through the finger which changes as blood pulses through the veins (Scully et al., 2012). The app developers contend that ‘a mobile phone can serve as an accurate monitor for several physiological variables, based on its ability to record and analyse the varying colour signals of a fingertip placed in contact with its optical sensor’ (Scully et al., 2012). The team confirms that the app yields measurements of breathing rate, cardiac R wave to R wave (R-R) intervals, and blood oxygen saturation, as accurate as standard medical monitors now in clinical use. This example provides a clear illustration of the ubiquitous computing and communication that apps enable, and of the possibilities they open up in the area of health care.

It is important to point out that the app at hand simply uses data collected by the smartphone's built-in camera. As developers of this app have disclosed, originally the app could work by way of 'an (at the time) unauthorised 'hack' of the device manufacturer's code for the camera' (Gizmag, 2010). The hacking of the smartphone means that apps can harness to the data (visual data) collected by the camera and use it for purposes (medical monitoring) which were presumably not intended by the device manufacturer.

# 3. The 'appification' of society and data protection implications of apps

Drawing from the Warsaw declaration on the appification of society, this section of the paper broaches the privacy challenges wrought on mobile device users by the spectacular rise in the adoption of apps. Subsequently, it describes data protection roles and responsibilities of the manufacturers of the operating system (OS) and device, apps developers and users. Finally, attention is drawn to users rights and requirements under data protection law, in particular on the innovative notion of 'granular consent.'

## 3.1 The privacy challenges posed by apps and mobile technologies

The ubiquitous interaction between apps and mobile technology presents distinctive privacy challenges. The first challenge derives from the fact that mobile devices are almost always turned on and that they often accompany the user wherever he or she goes. This means that the amount of data collected and processed is huge: search queries about health conditions, political interests, highly personal information such as communications with contacts, let alone the biometric data that latest devices are able to record. This amount of data can be processed for personal or domestic use but can also be communicated and shared with third parties. For instance, cheap apps can be used to send consumers behaviourally targeted advertisements.

The second challenge is related to the ubiquitous communication that mobile technology makes possible, as opposed to desktop computers. There are multiple channels of communication within the 'mobile ecosystem'. Imagine wireless providers, mobile operating system providers, handset manufacturers, application developers, analytics companies, advertisers, app owners, app stores, OS and device manufacturers, as well as other third parties, which can all be involved in the collection and processing of personal data from smart devices.

The third challenge concerns the ability of mobile devices and apps to reveal precise information, notably about a user's location. Crossing geolocation data with other data enables rather detailed profiles of consumer to be built. A recent study comparing 43 medical apps from the biggest app stores showed that many medical apps for mobile phones send data, connect to third-party sites, perform behaviour tracking, use unencrypted connections, and allow for data collection by third parties and store data externally. Most of the time this happened without notifying the user or without the user's prior consent (Lie Nije, 2013). It is not only a matter of consent, regardless of the quintessential role that informed consent plays in medical relationships (see below). It is also a matter of discretion and confidentiality on the part of those who manage personal health data. The same 2013 study indicates that privacy policies were only present in 74 % of the free apps and 60 % of the paid apps, either included in the app or externally on the developer's website (Lie Nije, 2013). This means that up to 40 % of the medical apps were not liable to privacy policies. To have or not to have privacy policy seems to be a matter of low importance for many apps providers.

## 3.2 The Warsaw Declaration on the appification of society

The privacy challenges posed by the mushrooming usage of apps were at the centre of the September 2013 Warsaw Declaration on the 'appification' of society. The two-page declaration was initiated by the Data Protection and Privacy Commissioners meeting in Warsaw, Poland, at their 35th annual International Conference (Warsaw, 23-26 September 2013). The declaration urges legal systems to take seriously the aforementioned privacy challenges. It requires that the 'essentials of data protection' are respected and implemented by the actors of the apps and mobile device 'ecosystem'. Accordingly, the declaration invites the competent authorities to clarify the roles and responsibilities of providers of operating systems and devices, app developers, app stores, as well as to make users aware of their rights as data subjects.

In what follows we heed the invitation of the Warsaw declaration. Drawing on the recent opinion of the Article 29 Working Party on apps (2013), an independent advisory body on data protection and privacy that was set up under Article 29 of the Data Protection Directive 95/46/EC, the following paragraphs describe data protection roles and responsibilities of the manufacturers of the operating system (OS) and device, apps developers and users. This section starts by examining users' responsibilities[3]. Subsequently, the article highlights some specific problems and questions posed by apps and mobile devices for data protection in the provision of health care services.

## 3.3 Users' awareness and control

According to consideration no. 17 of the preamble to Directive 2000/31/EC (the eCommerce Directive), apps are considered to be information society services. Information society services are 'any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data, and at the individual request of a recipient of a service.' The 'processing (including digital compression) and storage of data must comply with the data protection framework (Directive 95/46/EC and Directive 2002/58/EC)', which are 'fully applicable to information society services'.

Apps users are endowed with data subjects' rights flowing from the EU data protection legal framework, in particular Directive 95/46/EC, currently under revision (European Commission, 2012a). In addition, the framework comprises Directive 2002/58/EC, also known as the ePrivacy directive, as revised by Directive 2009/136/EC, which sets specific rules for all parties that wish to store or access information stored in the devices of users in the European Economic Area (EEA) (Article 29 Working Party, 2013:7).

For apps to be installed in smart devices, users must give their consent in an informed, specific, truly free fashion. Consent must, first, be obtained before an app places information on, and reads information from, the mobile device. Second, consent must be obtained before information relating to a person, which is stored in the device or accessible by the apps through the device, (e.g., via an online platform) is processed (Article 7 and Article 8 for sensitive data). In regard to consent, the declaration introduces an interesting notion, albeit hardly original, which is that of 'granular consent'. The notion of granular consent is related to the right of users to receive information (Article 10, 95/46/EC). The right to information is particularly important. As mentioned earlier, apps multiply the access points to data. Third parties can place apps on a person's mobile effortlessly for free or in exchange for personal data. For this reason, information must be carefully provided so as to ensure that individuals are aware of the purpose for which apps are being installed, and the kind of data that are accessed and processed. Article 5.3 of the ePrivacy Directive 2002/58/EC

[3] The responsibility of app stores also needs to be considered. App stores are not considered in this article.

is relevant, as it stipulates that any access to information 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, in accordance with Directive 95/46/EC, inter alia about the purposes of the processing. (…)'.

As mentioned, the use of apps entails a multiplication of points of access to personal information. This means that risks of data breaches or leaks increase. Accordingly, pursuant to Article 4 of the ePrivacy Directive 2002/58/EC, providers of publicly available electronic communications services must inform users promptly if a data breach occurs. The EU proposal for data protection regulation, mentioned earlier, makes data breach duty notification compulsory. This would likely also apply to app developers experiencing personal data breaches or in the event an app leaks personal data itself.

Furthermore, according to Articles 12 and 13 of Directive 95/46/EC, app users must be put in a position to exercise their rights of access, rectification, erasure and their right to object to data processing. Importantly, users should always be provided with the possibility to withdraw their consent in a manner which is simple and not burdensome. Users de facto withdraw their consent when they un-install apps. In this case, all personal data stored by the app developer and in the servers of the third party data controller(s) should be removed.

As pointed out earlier, apps are information society services. Accordingly, Directive 2006/24/EC, the data retention directive, does not apply. This means that data controllers, such as app developers, cannot continue the processing of data (Article 29 Working Party, 2013:25, footnote 46). In this connection, the right to be forgotten, introduced in Article 17 of the proposed Data Protection Regulation, would, if the proposal becomes law, strengthen data subjects' rights to obtain erasure of their information.

## 3.4 Granular consent

Let us now turn to the terminological innovation concerning consent. As anticipated earlier, the Warsaw declaration suggests that consent to apps' different processing activities and purposes should be granular. According to the Article 29 Working Party, granular consent means that 'individuals can finely (specifically) control which personal data processing functions [are] offered by the app they want to activate.' Granular consent echoes the notion that consent to data processing ought to be 'specific', that is, users must give consent for each type of data the app intends to access. The expression 'granular' derives from a report of the US Federal Trade Commission (FTC), the US consumers' protection agency. According to a recent staff report '(…) platforms should consider providing just-in-time disclosures and obtaining affirmative express consent for collection of other content that many consumers would find sensitive in many contexts, such as photos, contacts, calendar entries, or the recording of audio or video content' (FTC, 2013). The expressions 'just-in-time disclosures' and 'affirmative express consent' reveal what granular consent is about. It reflects the importance that consumers are and remain aware of what they are consenting to. In practice, granular consent is about or would entail drawing up two separate consent forms: one consent form for the general provisions regarding the apps and its functions, and another separate consent clause for the purpose and means of the processing (FTC, 2013).

Later in this paper, we will discuss user requirements and granular consent in relation to apps and mHealth technology. Before that, we will briefly look at the responsibilities and roles of app developers and of the manufacturer of the device's operating systems. These actors have specific obligations that flow from data protection law. Another group of actors that should not be neglected, but are not directly addressed in this contribution, are the app stores. These online platforms offer mostly paid and unpaid apps. Even though app stores are currently reported to exercise control over the apps they provide, their responsibility for data protection or privacy policies for apps, including the source of the medical information included in the apps, needs to be assessed (Article 29 Working Party, 2013; Lewis, 2013).

## 3.5 Operating system, device manufacturers and app developers

The continuous data flow between apps and device is possible through an interface called the application programming interface (API), described above. The operating system (OS) and device manufacturers are the entities responsible for installing the API. The API should allow users to exercise granular consent. To this end, an API should:

- Determine the means (and extent) of access to personal data;
- Allow app users and the apps developers to have sufficient level of control on access, so that only data that are necessary for the functioning of the app are accessed (granularity);
- Include the possibility of revoking access in a simple and effective manner.

The responsibility of the operating system cannot be separated from other actors in the apps ecology, namely app developers and app stores. The app developer is the person or the company, including the vast array of private and public sector organisations that outsource the app development, which creates apps and/or makes them available to end-users. In other words, app developers design and/or create the software which will run on the smartphone. This means that this group of actors also has, together with the device and OS manufacturers, a say about the extent to which the app will access and process different categories of personal data in the device and/or through remote computing resources (such as cloud services). To the extent that it is the app developer which determines the purpose and the means of the processing of personal data, it must be considered the data controller (Article 2(d) of the 95/46/EC) and it is responsible for:

- Ensuring the proportionality of the data collection by apps;
- Customising information about data subjects rights (granularity), including the providing of up-to-date and adequate information to prospective app users;
- Notifying any breach of personal data or security problems.

The opinion of the Article 29 Working Party is that, given the continuous flow of data between apps and device, it may not be always clear who is the data processor and the data controller, the OS manufacturer or the app developer. This can create uncertainty among users about where they should turn if they have questions about their privacy. For this reason, and in order to dissipate the confusion in responsibilities, the Article 29 Working Party (2013) makes an interesting reference to the notion of privacy by design. The attention that the Working Party draws to ‘privacy by design’ seems to us particularly appropriate for apps that process sensitive medical data, and it will be discussed in the next section of the paper.

# 4. Data protection implications for apps processing medical data

The Warsaw declaration and the Article 29 Working Party reveal a palpable preoccupation about the trend towards data maximisation and the relaxing of conditions concerning secondary uses of data. The deluge of apps possibly adds to this trend. The concern is that people will grow more and more careless about their data privacy. This is alarming, bearing in mind the vast number of apps that process sensitive personal information such as data about the health status. Starting from this premise, the following sub-sections highlight a number of specific problems that medical apps and mobile devices create for data protection law.

## 4.1 Apps and medical data

As long as apps process medical data, they will have to adhere to data protection rules on the processing of sensitive data. In case the data processing involves data relating to the health status of a person, the general rule is that the processing of such data is prohibited (Article 8.2 and 8.3, Directive 95/46/EC).

The prohibition can, however, be lifted in a limited number of instances. Three exceptions in particular can be considered:

- The data subject has given explicit consent to the processing of those data;
- Processing is necessary to protect the vital interests of the data subject or to another person if the data subject is physically or legally incapable of giving their consent;
- Processing occurs for the purposes of preventive medicine, medical diagnosis and the provision of care or treatment of the management of health-care services, if the data are processed by a health professional under national law or rules to the obligation of professional secrecy or by another person also subject to an equivalent obligation of confidentiality.

The second exception relates to a situation in which the person concerned cannot acquiesce or refuse the use of his or her information. The third exception relates to a situation where an app, such as the Pulse Phone, is used by medical doctors to measure biometrics. In this case, medical doctors will be responsible for the processing of medical data.

In addition to these cases, individual consent is likely to be the most used legal basis for processing personal medical data in apps (Directive 95/46/EC, Article 8.2,a). Consent is subject to a number of further requirements that are important for mHealth and need to be pointed out. First, consent must be explicit, meaning that only schemes that utilise consent in an opt in, and not opt out (‘silence or inactivity’), manner are deemed lawful. Second, there is lack of clarity about the form of consent. In some European countries, such as Belgium, explicit consent must be written (Article 29 Data Protection Working Party, 2011); in other countries, the requirement of written consent is not mandatory. Recital 32 and Article 7.1 of the 2012 proposed regulation on data protection requires that ‘where processing is based on the data subject’s consent, the controller should have the burden of proving that the data subject has given the consent to the processing operation.’ Thus, logically, a record must be kept, arguably in written form. The specification that consent to medical data processing must be written is a positive innovation of the proposed regulation. Yet, it is unclear how the requirement of written consent can be implemented in apps (a similar question is presented with regards to medical device rules, below). Third, data should be processed only for the purposes specified when data were originally elicited.

Reflecting the FTC's insistence on 'just-in-time disclosures' and 'affirmative express consent', this may require new thinking about how to ensure that patients or users remain aware of the transmission of their health data, whereby the purpose and modalities of treatment change over time.

## 4.2 Is consent enough?

Is consent enough to ensure that apps for mobile health applications respect the privacy of patients or users? Individuals may well be able to offer their consent technically by pressing a button on a screen. But how can one make sure that patients understand what it is to which they are consenting? Only if apps are integrated in the doctor–patient relationship can one hope that the patient truly understands that to which he or she was consenting. It is questionable if apps processing data for medical purposes can be used without any supervision. Portuguese data protection legislation, for instance, allows a user to have only indirect access to medical data through a physician. Similarly, the Belgian Commission for the Protection of Privacy has stated that personal data in general should be processed under the supervision of a physician whenever possible (Privacy Commission, 2007). In addition, it must be pointed out that apps mobile devices are not used by abstract individuals, but by people with flesh and bones, different levels of understanding and even different capacities for the exercise of individual autonomy. The ability of an individual to be able to gauge truly the exact nature of his/her situation in an mHealth environment will vary enormously between people such as a teenager or an elderly patient. In a real-life environment (in a hospital, for example) a healthcare provider would be able to guide users/patients through the process of consent, explain the consent form that needs to be signed and to answer possible questions. Current medical apps often leave the user alone and even require him/her to open up additional links to find information on external sites (Lie Nije, 2013).

The Warsaw declaration on the 'appification' of society, the Article 29 Working Party, and the FTC report discussed earlier, encourage app developers and device manufacturers to make effective the conditions for granular consent. While we share the accent placed on individual awareness and participation, we are concerned that apps go in the opposite direction towards the depletion of the fundamental function of informed consent.

As it was argued by some of the authors of this paper in a previous publication (Mantovani & Quinn, 2013), two scenarios are likely to play out when apps are put in the picture. The first is a scenario where the satisfaction of consent requirements will lead to a multiplication of informed consent requests to users/patients with the result that such requests will be frequent, irritating, not conducive to convenience and likely to be easily dismissed by users or patients. In the second contrasting scenario, the boundaries of treatment relationship, the third exception mentioned above, are stretched so that the role of consent as a basis for the processing is reduced in practice, thus leaving the individual with the opportunity to opt out. This would mean, however, that apps performing medical measurements could be used only under the supervision of medical professionals.

## 4.3 Proposal for a third way

Perhaps a third way can be found, which possibly involves a mix of education and technological regulatory measures. On the one hand, education, including real-time and physically present contact and consultations with app users, use of dashboards, icons and tailored information, would avert the risk of reducing consent to a consumer-protection tool used to spoon feed seemingly hapless, abstract end-users/patients with 'mind the gap'-like alerts. The role of consent in the medical context is arguably much more important than that of consumer transactions. On the other hand, techno-regulatory initiatives could be envisaged along the lines suggested in the Article 29 Working Party opinion on apps. The Working Party opines that, in order to control the continuous flow of data between apps and devices, apps and devices should incorporate the principles of privacy by design.

In a nutshell, privacy by design means that the conditions for the lawful processing should be incorporated in the design of the device and the apps. There are substantial legal arguments that depose in favour of encouraging the enforcement of privacy by design settings in the apps ecology. According to Article 17 of Directive 95/46/EE and Article 14.3 of the ePrivacy Directive 2002/58/EC, the manufacturer of a device should embed data protection from the very beginning of the design phase of the device. Furthermore, Article 3.3.c of Directive 1999/5/EC on radio equipment and telecommunications terminal equipment stipulates that the European Commission may decide that 'end user devices shall be so constructed that they incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected.' It is worth adding that Article 23 of the Proposal for a Regulation on data protection, not yet in force, also states that 'the controller shall implement appropriate technical and organisational measures and procedures in such a way that the processing will [...] ensure the protection of the rights of the data subject.' These technical and organisational measures should be implemented, according to Article 23, 'both at the time of the determination of the means for processing' and 'at the time of the processing itself'.

In the concluding section, we present a proposal for technical and organisational measures.

# 5. Medical devices and apps

This section begins with an illustration of the EU medical device legal framework and then discusses the reasons why European authorities have been hesitant to impose the requirements of the medical device framework on the manufacturers of apps.

## 5.1 The app as a 'shadow' medical device

A core plus point for apps and their use in mHealth is their potentially unlimited mobility. This is based on the potential use of apps with readily available technology such as smartphones 'to offer information, diagnostic tools, possibilities to 'self quantify' and 'new modalities of care' (European Commission, 2012b). The potentially unlimited technical horizons will however be narrowed by the need for smartphones and apps to conform to varying regulatory requirements in order to be marketed and used (Quinn et al., 2013).

The Medical Device Framework (MDF) can be considered as one of the most important ones. Medical device regulation has been one of the EU's most notable initiatives, promoting the establishment and running of a European single market for medical devices. The primary purpose of the MDF has been to provide common rules for the free movement of goods throughout the EU, and, at the same time, to ensure the same level of safety to all EU citizens using medical devices (Directive 93/42/EEC). In order to achieve these objectives, the EU adopted a series of basic safety requirements achieved by a combination of means of harmonisation and mutual recognition measures. The MDF is at present composed of three different directives. These three are the Council Directive 90/385/EEC on active implantable medical devices (AIMDD), the Council Directive 93/42/EEC on medical devices (MDD), and the Directive 98/79/EC of the European Parliament and of the Council on in vitro diagnostic medical devices (IVDD). This framework is currently undergoing revision, with the Commission having recently completed a consultation process and released a proposed new regulation (European Commission, 2012c).

The directives of the MDF harmonise basic safety requirements and specify a number of documentary procedures that must be conducted in order to demonstrate that these requirements have been respected. In doing so, they ensure a basic level of protection for the users of medical devices in Europe (Quinn et al., 2013). This process is verified by bodies under the control of the Member States. Once a medical device has been approved as meeting the requirements by one of these bodies it must be permitted circulation in all Member States. This general framework not only applies to physical devices but also to software (Directive 93/42, Article 1:2,a). Given that most mHealth scenarios are likely to employ medical programmers or software, this framework is of extreme importance. The basic idea behind the MDD framework for software is that all computer programmes that meet the definition of a medical device must comply with the MDF's requirements. A medical device is:

*'any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application. Such a device should be intended by the manufacturer for one of a number of defined purposes, one of which is, diagnosis, prevention, monitoring, treatment or alleviation of disease'* (Directive 93/42/EEC Article 1:2).

All software that meets this definition, including software that works in combination with a physical device, for instance a smartphone, will be categorised as a medical device (Quinn et al., 2013).

## 5.2 A failure of European authorities to embrace apps as the MDF would expect

Despite the obvious engagement of the MDF with medical apps, little effort has been made on behalf of European authorities to impose the requirements of the framework on the manufacturers of apps (Quinn et al., 2013). This lack of effort is worrying, given that one of the principal aims of the MDF is to ensure patient safety in Europe. It seems likely that this lack of enforcement can be attributed to two causes:

- The first is the fact that the MDF was created in the 1990s. This means that its requirements predate the emergence and subsequent explosion in the use of apps. More explicitly, the MDF and the requirements that all medical devices had to incorporate, were conceived while having in mind traditional, corporeal, 'heavy' medical devices, such as a bedside monitor. As a result it is a challenge, if not an impossibility, to see how such requirements can be applied to the world of apps. Some of these problems, i.e. those related to the CE marking, instructional requirements and labelling, are briefly discussed later in the section of the paper.
- The second reason relates to the innovative image of apps. Such products, and particularly those involved in novel medical uses, are often seen as leading a new wave of innovation that is likely to lead to economic and other benefits. As a result of this, it seems that regulators have been hesitant to take action that they fear may stifle an area of obvious on-going innovation (European Commission, 2012a). Given the costs involved with MDF compliance, which are estimated at up to €10m (EFPIA, 2010; DI Masia, 2007; European Commission, 2012c), a more severe application of the MDF's requirements would likely mean that large numbers of apps (that are currently described as existing for the purposes of well-being, but which could in fact be said to have a quasi or pseudo-

medical purpose, such as a pedometer for self-monitoring), would disappear. Other apps that have a clear medical purpose would, under a system of stricter enforcement, have no choice but to comply with the demands of the MDF. This would be likely to entail an increase in the cost of such applications beyond a level which may be feasible for a low-cost business model. If, at some point in the future, a strict application of the medical device directive were to occur, it would prevent the marketing of many ‘apps’ that have a pseudo-medical function. Enforcement would likely confront medical app producers with a choice of either producing their apps in line with the MDF or ceasing their creation.

## 6. Implications of a failure to engage the MDD on apps and consumers

This section addresses four possible implications stemming from the uneven approach taken to apps in the medical device framework.

### 6.1 The availability of ‘medical devices’ that are not required to meet the basic requirements

In its essential requirements, the MDF does not spell out the precise technical requirements that are needed for a device to be considered as safe. Rather, the directives that form the framework make reference to very broad standards. These standards are framed in a sufficiently broad manner so as to be applicable to all medical devices. Despite their broad nature, such requirements represent important standards that must be met in order to ensure a potentially high level of safety for users. The essential requirements include, for example, requirements that electrical components should be constructed in a safe manner that limits risks for users (Annex I s9.2, Directive 93/42) and that the product in question be designed in such a manner so as to minimise the risks of fire (Annex I s9.3, Directive 93/42). More importantly for apps, the essential requirements require that any software used in medical devices be designed so as to alleviate safety concerns (Annex I s12, Directive 93/42). Given that medical apps essentially consist entirely of software, this requirement is extremely important for apps that are software programmes created in order to carry out a medical function. Such a requirement can be met, for example, by adherence to an internationally recognised software standard that has been shown to be safe.

A serious negative consequence of the European authorities’ failure thus far to apply the requirements of the MDD to apps is that the medical apps that are appearing on the market have not been checked for compliance with the essential requirements of the MDD. This effectively means that manufacturers of medical apps that may incidentally be medical devices do not have to create them to the same standards required for conventional medical devices. Given that the regulation of medical devices is deemed necessary to protect those who use such devices, it is alarming that medical apps that are in reality medical devices are not subject to the same level of scrutiny as is the case with conventional medical devices. Whilst apps may represent an exciting area of innovation, it is difficult to see why they should be subject to a lower level of safety requirements than other more conventional requirements.

## 6.2 Ensured safety testing with possible components

Conventional medical devices may be designed to operate with one or more accessory components. This may also be the case where the medical device in question principally consists of software. An accessory component may be a module that is added to the medical device in question to give it extra functionality. This may be a particular sensor, for example, a blood pressure sensor, or a piece of networking equipment allowing data from the medical device to be transmitted to a remote location for further processing. The medical device directive requires that the testing of a medical device be performed with all the accessories with which it is to be used. The essential requirements of the directive must be met by the combination of the medical device and the accessory. Medical apps are somewhat different from conventional medical devices in so far as they are not designed to work with one or a few select accessories but a potentially enormous range of generic devices. This is because most apps are not designed to operate on one particular device but can run on any smartphone or tablet that functions using a given operating system. In order to be truly tested with all potential accessories, such programmes would have to be tested on every smartphone on the market that is capable of running it. In addition, given the versatility of operating systems such as Android, such apps may well be capable of being run on phones that did not even exist when the app in question was created.

This apparent impossibility to test the medical device with all available accessories poses significant safety issues. It will be extremely difficult for manufacturers to foresee or avoid problems that arise due to the idiosyncratic nature of each smartphone. Consider, for instance, the situation of a creator of an app that uses the speakers of a phone to measure an individual’s heart rate. The creator of that app may well have had in mind the speakers of a certain type of phone when they created the app. Whilst the creator may be able to test the reliability of that individual smartphone’s speakers, it will be time-consuming and expensive to do so for all compatible phones on the market (and impossible for those phones yet to be released). Similarly, the creators of an app that can display medical imagery such as x-rays or an EEG scan may have tailored it for use with the type of smartphone screen found most commonly on the market at that moment. They may have been unaware that a new type of screen technology would be available in the future that did not work so well with their program. These issues mean that even where individual manufacturers wish to attempt to comply with the requirements of the medical device, they will find it difficult to do so unless the app in question is restricted to a few selected, potential accessories.

## 6.3 Instructions, labels and the CE mark

In addition to problems of the type discussed above, it is difficult to see how apps can meet a number of other requirements mandated by the MDF. These essential requirements of the MDF specify requirements in terms of labelling and instructions for all medical devices. Given that an app does not exist as a tangible item with a corporeal form, it is not possible to attach traditional printed instructions and labels to it as is in fact required by the MDF (Annex I s13:1, Directive 93/42; Commission Regulation, 2012d). This risks the creation of an important ‘information gap’ whereby the end-user of the device in question will not have available to him or her information that may be crucial in order to allow the safe operation of the device. Similar issues exist with respect to the CE mark which must be affixed to products that have met the requirements of the MDF in a precisely defined manner (Annex VII, Directive 93/42). It would therefore be an opportune moment for the European Commission to include such requirements in the next version of the MDF so as to accommodate such programs in the upcoming revision of the MDF. However, the European Commission has not indicated that it intends to do so in its representations thus far (European Commission, 2012c, Article 18:3). This appears to ignore the recent conclusions of the EU Council that medical Device legislation needs to be adapted towards  ‘a changing tomorrow’ (Council of the EU, 2011).

### 6.4 Monitoring of problems

The MDF requires that manufacturers monitor problems that may occur on their devices after they have been released onto the market (Annex V s3, Directive 93/42). Where problems occur, the relevant national authorities must be alerted and steps must be taken to remedy the problem in question. The existence of such requirements provides a crucial obligation to provide an important feedback mechanism. Efforts at monitoring may allow problems to be detected early and, where action is taken, further risks to individual safety may be prevented. Given that medical apps have not yet been required to subject themselves to the requirements of the MDF, the motivation or even the awareness of manufacturers to fulfil such an obligation may be reduced. This may have the unfortunate effect of putting the users of medical apps at a higher level of risk than would otherwise have been avoidable.

## 7. Conclusions

Apps and mobile technology may act as the technological turning-point towards a truly ubiquitous information society and a more agile, cost-efficient and patient-centred health care. The journey, is not only laden with opportunities and the creativity that we are just beginning to explore. It could also prove to be a treacherous one. The mushrooming of apps for mobile devices that can perform medical or pseudo-medical operations pose privacy challenges that ought to be addressed now. In this paper we have tried to make a case for greater user control of personal data. Accordingly, the authors of this article suggest that:

1. Responsibilities of the actors in the app ecology should not only be identified and described but also enforced. Fines of 2 to 5 % of global turnover could be an incentive for app developers and mobile device operators to adapt the required data protection measures, such as data breach notification and data minimisation measures.

2. Professional and public education is highly important to avert the risk posed by the societal and technological trends towards data maximisation, which renders individuals increasingly careless about their privacy.

3. Privacy by design principles could be enforced in sensitive areas, such as health care. Privacy by design in the health care domain should embed the following settings and functionalities in apps and mobile devices:

   a. provide for multiple disclosures about which data are being processed and for what purpose at different points in time.

   b. allow users to revisit the choices initially made about the app.

   c. insert dashboards or icons to help users determine which apps have access to which data. More specifically, these tools should help users to determine: what kind of information is stored; what kind of information is transmitted between system components; and what kind of information is presented by the system.

In addition to posing privacy challenges, the explosion in the number of apps available as mobile devices that can perform medical or pseudo-medical operations can also represent concerns for patient/consumer safety. Given the sensitive nature of their use, and the potential risks in case of malfunction, it is not sufficient to simply wait and see how the situation develops before taking firm and transparent regulatory action. Failure to take action increases the risk of injury or even death for the users of medical apps. If such events occur, the public reaction is likely to be strong given that the problems of oversight and regulation of medical devices were not a hidden issue of which no-one had knowledge, but rather were known by many parties, including the European Commission (2012e).

Luckily the revision of the data protection and medical device frameworks means that this is an opportune moment to act. The authors of this paper would like to see an open and honest discussion concerning the place of apps in the world of mHealth.

In particular it is necessary to ask the question: What type of mHealth do we want? Two distinct choices appear to be available. At present it appears that, as a society, we are approaching a fork in the road.

One route leads towards a future for mHealth in which new technologies would be regulated according to the same principles as conventional medical devices. Accordingly there might be fewer devices, including apps. Those apps that present themselves might therefore be more expensive than they are currently, due to the need to comply with medical device regulation. They might also not be as flexible as today in terms of their being able to run on all phones and tablets operating a particular operating system. However, in return for such inconveniences users would be able to have more confidence in the safety of any product they choose in terms of the risks for both themselves and their loved ones.

The other possibility is to continue as the European Commission has done so far and allow medical apps to avoid the need to comply with medical device regulation. This would result in a world where inexpensive, unregulated medical apps were available to all, many simply by download from an online app store. In such a world, however, accidents would be more frequent and could have occasional devastating consequences for the users of such devices. As a result confidence in the industry would be harmed, since consumers would not know which apps they could or could not trust.

The authors of this paper would submit that there is little reason to allow apps to avoid the usual regime of medical device regulation. If apps are medical devices they should be regulated accordingly, whether or not they represent a cluster of innovation. When the safety of patients and consumers of mHealth is at stake, such economic considerations should not be able to ride roughshod over normal safety requirements.

The authors point to the recent declaration of the American Food and Drug Administration with regard to its approach to medical apps that provides both transparency and a firm level of regulatory control as an example (FDA, 2013). This is an example which it is hoped the European Commission will follow as a matter of urgency.

## 8. References

Apple Inc. (2013). App store tops 40 billion downloads with almost half in 2012, retrieved October 2, 2013 from http://www.apple.com/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html.

Article 29 Data Protection Working Party (2013). Opinion 02/2013 on apps on smart devices, retrieved October 10, 2013 from http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

Article 29 Data Protection Working Party (2013). Opinion 02/2013 on apps on smart devices, retrieved October 10, 2013 from http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

Belgian Privacy Commission (2007). Sectoraal comité van de Sociale Zekerheid en van de Gezondheid. Beraadslaging N° 07/031 van 4 september 2007 m.b.t. de mededeling van persoonsgegevens aan het Federaal Kenniscentrum voor de Gezondheidszorg in het kader van de studie PF2006-14-HSR, retrieved September 15, 2013 from http://www.privacycommission.be/sites/privacycommission/files/documents/beraadslaging_SZ_031_2007_0.pdf.

Council of the EU (1993). Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, retrieved September 20, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31993L0042:en:NOT.

Council of the EU (2011). Council conclusions on innovation in the medical device sector, O.J. 2011 C202/7, retrieved September 10, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:202:0007:0009:EN:PDF.

DiMasia, J., & Grabowski, H. (2007). The cost of biopharmaceutical R&D: Is biotech different?. Managerial and Decision Economics, 28, 469–479.

EFPIA (2010). The pharmaceuticals industry in figures, retrieved October 2, 2013 from http://www.efpia.eu/Content/Default.asp?PageID=559&DocID=9158.

European Commission (2012a). Personal data protection: Processing and free movement of data COM 2012/0011/COD retrieved October 15, 2013 from http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

European Commission (2012b). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'eHealth Action Plan 2012-2020 — Innovative healthcare for the 21st century', retrieved September 12, 2013 from http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1252.

European Commission (2012c). Proposal for a Regulation of the European Parliament and of the Council on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No. 178/2002 and Regulation (EC) No. 1223/2009, retrieved October 15, 2013 from http://ec.europa.eu/health/medical-devices/files/revision_docs/proposal_2012_542_en.pdf.

European Commission (2012d), Commission Regulation No 207/2012 of 9 March 2012 on electronic instructions for use of medical devices retrieved July 15, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:072:0028:0031:en:PDF.

European Commission (2012e). Impact Assessment on the Revision of the Regulatory Framework for Medical Devices — Commission Staff Working Document, retrieved October 22, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2012:0274:FIN:EN:PDF.

European Parliament (1995). Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, retrieved July 15, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

European Parliament (1999). Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity, retrieved July 15, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0005:en:NOT.

European Parliament (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), retrieved July 15, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:En:HTML.

European Parliament (2002). 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), retrieved July 15, 2013 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

Eurostat (2012). Information society statistics, retrieved October 22, 2013 from http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics.

Federal Trade Commission (FTC) (2013). Mobile privacy disclosures, building trust through transparency: Staff report, retrieved June 10, 2013 from http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

Food and Drug Administration (FDA) (2011). Mobile medical applications: guidance for industry and Food and Drug Administration staff, retrieved July 15, 2013 from www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

Ingraham, N. (2013). Apple announces 1 million apps in the App Store, more than 1 billion songs played on iTunes radio. The Verge, October 22, 2013, http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store.

Lewis, T. (2013). Exclusive: Apple now asking app developers to provide sources of medical information. iMedical Apps, 18 September 2013, http://www.imedicalapps.com/2013/09/apple-app-developers-sources-medical-information/.

Lie Njie, C. M. (2013). Technical analysis of the data practices and privacy risks of 43 popular mobile health and fitness applications, retrieved September 21, 2013 from http://www.privacyrights.org/mobile-medical-apps-privacy-technologist-research-report.pdf.

Mantovani, E., Quinn, P. (2013). mHealth and data protection? The letter and the spirit of consent legal requirements. International Review of Law, Computers & Technology, 21 (1).

Quick, D. (2010). Pulse phone app has its finger on the pulse. Gizmag.com. November 16 2010, http://www.gizmag.com/pulse-phone-heart-rate-app/16962/.

Quinn, P., Habbig, A., Mantovani, E., De Hert, P. (2013). The data protection and medical device frameworks: Obstacles to the deployment of mHealth across Europe? European Journal of Health Law, 20, 185-204.

Scully, C. G., Lee, J., Meyer, J., Gorbach, A. M., Granquist-Fraser, D., Mendelson, Y., Chon, K. H. (2012). Physiological parameter monitoring from optical recordings with a mobile phone. IEEE Transactions on Biomedical Engineering, 59 (2), 303-6.

Welch, C. (2013). Google: Android app downloads have crossed 50 billion, over 1M apps in Play. The Verge, July 24, 2013, http://www.theverge.com/2013/7/24/4553010/google-50-billion-android-app-downloads-1m-apps-available.

Wiewiórow, W. R. & Kohnstamm, J. (2013). Warsaw declaration on the "appification" of society, retrieved September 24, 2013 from https://privacyconference2013.org/web/pageFiles/kcfinder/files/ATT29312.pdf.

World Health Organization (1946). Constitution of the World Health ORganization, retrieved September 20, 2013 from http://apps.who.in/gb/bd/pdf/bd47/en/constitution-en.pdf.

Wright, D., Gutwirth, S., Friedewald, M., Vildjiounaite, E., Punie, Y. (2008). Safeguards in a world of ambient intelligence. Dodrecht, The Netherlands: Springer.

## Authors

**Eugenio Mantovani**
Vrije Universiteit Brussel, Belgium
Eugenio.Mantovani@vub.ac.be
http://epractice.eu/en/people/359021

**Paul Quinn**
Vrije Universiteit Brussel, Belgium
paul.quinn@vub.ac.be
http://epractice.eu/en/people/359027

**Barry Guihen**
Centre for Society Science and Citizenship (CSSC), Marie Curie IAPP action VALUE AGEING, Belgium
barry.guihen@cssc.eu
http://epractice.eu/en/people/359028

**Ann-Katrin Habbig**
Vrije Universiteit Brussel, Belgium
ahabbig@vub.ac.be
http://epractice.eu/en/people/262421

**Paul De Hert**
Vrije Universiteit Brussel, Belgium
paul.de.hert@vub.ac.be
http://epractice.eu/en/people/359064

# The Regulatory Context of Mobile Health in the United States and a Conceptual Framework for Privacy and Security

The advent of mHealth technologies is changing the patient health information exchange landscape, with patients becoming increasingly involved in the management of their health and health data. However, current United States (US) federal regulations, specifically the Health Insurance Portability and Accountability Act (HIPAA), require only 'covered entities' to comply with privacy and security provisions, leaving patient-generated health information vulnerable to privacy and security threats. Federal policymakers must acknowledge the interconnectedness of the current mHealth landscape to draft global policy protecting patient health information. The work presented in this paper provides a clear conceptual framework with which public and private sector healthcare leaders can develop robust privacy and security policies and procedures. Managed care decision makers should extend their efforts to protect patient data on mobile platforms beyond what is required by HIPAA. Advances in reforming healthcare through the Affordable Care Act will benefit from expanding privacy and security regulations that take account of the principles set forth in this paper.

Robert Furberg

RTI International, US

Alexis M. Kirk

RTI International, US

Douglas S. Johnston

RTI International, US

## Keywords

Health information technology, mobile health, policy, privacy, security.

> “Mobile health technologies are being adopted at rates quickly surpassing regulatory protections, leaving patient health information vulnerable to privacy and security threats.”

## Funding source

RTI International supported the development of this publication with internal funds

## Acknowledgements

The authors would like to acknowledge Kathleen Lohr and Carol Offen for their efforts in editing this paper. The authors would also like to acknowledge Kathleen Mohar and Tayo Jolaoso for their efforts in the original production of the figure used in this text.

## 1. Introduction

The privacy and security of patient health data are critically important; historically, policies and regulations aim to ensure data confidentiality, integrity and availability. With rapid advances in and adoption of mobile health (mHealth) technologies –including smartphones and tablets, health applications (apps), wireless medical devices and personal health records –patient health data traditionally produced and exchanged within the healthcare system is increasingly generated and held by entities that are not subject to conventional regulatory protections. In contrast to past technology advances in healthcare, mHealth technologies are increasingly developed by entities without previous roles in healthcare. Although mHealth technologies afford great opportunities for patient engagement and facilitate health information exchange, they are being adopted at rates quickly surpassing privacy protections, leaving health information vulnerable to unauthorised disclosures and inappropriate use. This paper provides a conceptual framework of the current mHealth landscape, which could serve as the basis for identifying factors that policymakers should consider as they solicit input, develop guidance or draft new policies for mHealth privacy and security.

## 2. Changes in modes of data exchange leave patients vulnerable

Most existing federal policies regulating the privacy and security of health data in the US presume the existence of a controlled network of data exchange, primarily among healthcare organisations, payers, patients and other stakeholders. In this traditional model of health information exchange, sensitive health data is initially generated and governed by providers or payers and data is exchanged via limited, secure methods. Patient health information is initially generated and stored within the provider sphere and the patient is primarily a recipient of data. Conventional regulatory policies for health information reflect this model of information exchange. Landmark federal regulations to address the privacy and security of health information were the Privacy and Security Rules set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 1996). HIPAA's Privacy and Security Rules established national standards for 'covered entities' to secure patients' 'protected health information' (PHI). Since all data exchange occurs between the patient and a 'covered entity', HIPAA regulates all data exchange in traditional networks. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 bolstered HIPAA protected health information protections by extending the complete HIPAA Privacy and Security rules to 'business associates' of covered entities (HITECH, 2009).

The rapidly evolving mHealth landscape poses new issues in information exchange and involves additional organisations not considered at the time that the HIPAA umbrella was created (ONC, 2008). HIPAA rules assume a controlled flow of data generated by healthcare providers and transmitted to patients and payers. Consequently, only protected health information generated, transmitted or held by a covered entity is subject to compliance with HIPAA rules. Advances in mHealth technologies are putting patient data 'at the fingertips' of players not customarily involved in health data management, including technology and app developers and patients themselves. These mHealth technologies, with expanding wireless, remote and patient-owned functionalities, mean technology developers and patients are increasingly active participants in managing health and health information, putting such data outside any 'covered entity' protection. Moreover, the previous notion of one-sided data generation is increasingly being challenged as patients become more engaged in their own healthcare through the adoption of mHealth technologies. Thus, even though HIPAA is one central authority for protecting health information, it is limited in its purview to covered entities, a jurisdiction no longer sufficient to protect health information in the current mHealth landscape.

To conceptualise the mHealth landscape, a framework was developed, in which covered entities are no longer the only parties generating patient health information. Patient-owned mHealth technologies are generating and exchanging data both between the patient and provider spheres and within the patient sphere itself.

## 3. The mHealth framework

This framework is depicted in Figure 1 below. our primary areas of concern were identified in the figure:  (1) access to health information from mobile devices, (2) health apps, (3) personal health records (PHRs), and (4) wireless medical devices. Data flows freely between these areas, for example, a patient may collect data using a health app or wireless medical device and want to aggregate it in a PHR to share with his/her providers. The concerns and the positions of the regulators vis-à-vis each of these domains are dealt with systematically in this section of the paper.

Policies governing this data flow, however, fall under the jurisdiction of various federal agencies, each with a different focus and differing levels of protection. Overarching policies recognising the interrelationship of each area have not been drafted; concerns about the privacy and security of protected health information as it moves between various areas in the mHealth network remain. The primary concerns pertinent to protected health information and existing regulatory policies regarding this information for each of these four areas are sequentially discussed in this section of the paper.

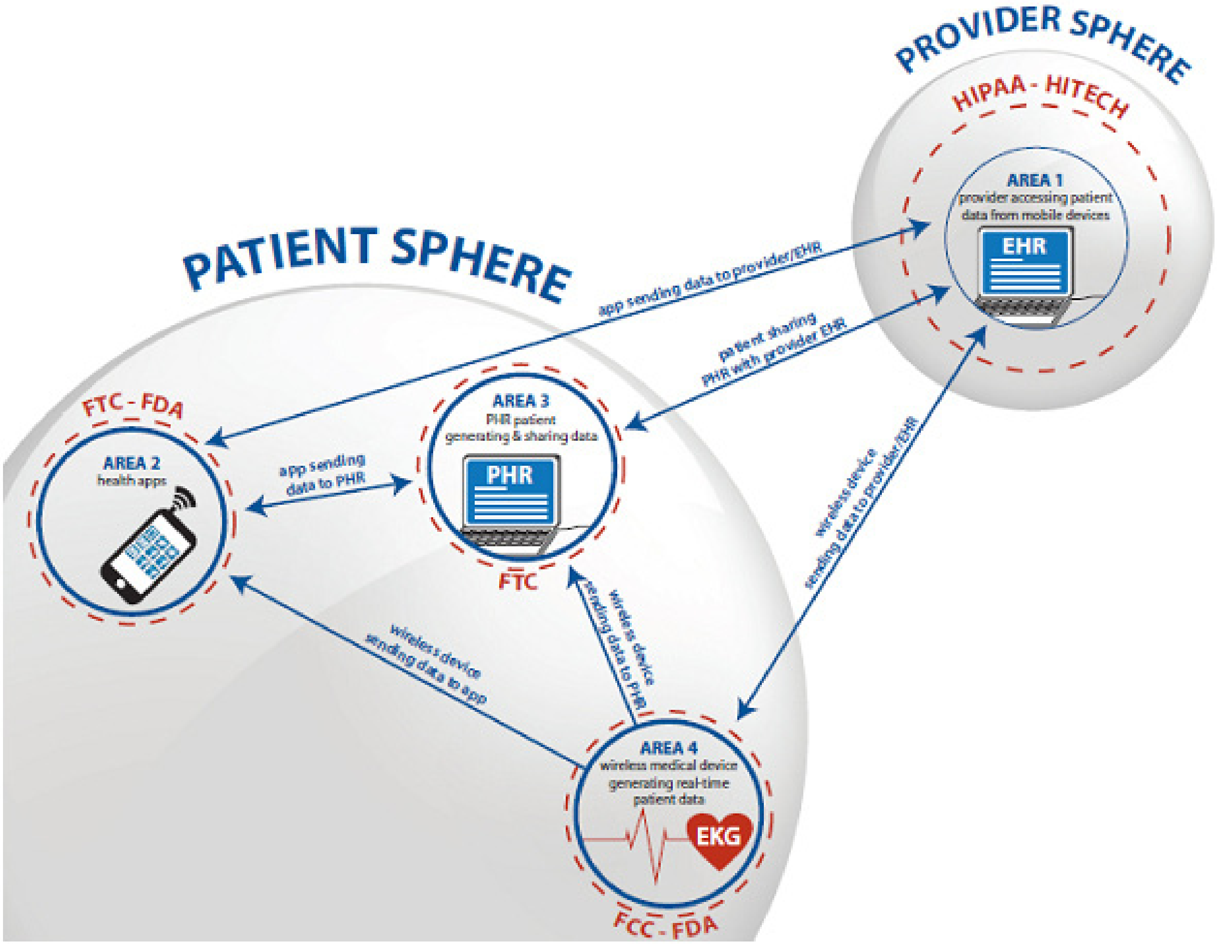

PROVIDER SPHERE
HIPAA - HITECH
AREA 1
provider accessing patient data from mobile devices
EHR
PATIENT SPHERE
app sending data to provider/EHR
patient sharing PHR with provider EHR
FTC - FDA
AREA 2
health apps
app sending data to PHR
AREA 3
PHR patient generating & sharing data
PHR
FTC
wireless device sending data to provider/EHR
wireless device sending data to app
wireless device sending data to PHR
AREA 4
wireless medical device generating real-time patient data
EKG
FCC - FDA

**Figure 1:** The mHealth Network of Health Information Exchange

## 3.1 Area 1 - Access to health information from mobile devices

***Concerns:*** This area represents health information remotely accessed on mobile devices, including smartphones and tablets. Although security protections are well developed for the access, exchange and storage of patient health information on laptops and other enterprise-owned computers, the emerging popularity of smartphones and tablets to access patient health information remotely is of increasing concern in the healthcare system. HIPAA Privacy and Security Rules extend to data on these mobile devices, but the nature of mobile devices presents new data security and compliance issues. Mobile devices travel outside of organisations' perimeter protections (firewalls and other intrusion prevention systems); they are loaded with potential vulnerabilities (via apps); and, because they are small devices, they can be easily lost or stolen, exposing their confidential content to unauthorised users (Juniper, 2012). In contrast with the range and sophistication of security applications available for computers, security provisions for mobile devices may be immature or compatible with only one of the many mobile operating system platforms that smartphones and tablets use (Juniper, 2012). In addition to the less than ideal security protections that are available for mobile devices, the 'bring your own device' philosophy is emerging as a challenge since many providers use their personally-owned devices to access protected health information (Juniper, 2012).

***Regulators:*** Through HIPAA, the Office for Civil Rights (OCR) in the Department of Health and Human Services is the primary regulator in this area. HIPAA establishes the authority for protection of any protected health information used by covered entities, including data on mobile devices. However, the lack of federal guidance has left industry to self-regulate and to establish best practices for the use of smartphones, tablets and other mobile devices to access and exchange protected health information. The popularity of smartphones and mobile devices is not unique to healthcare apps. Many private technology companies have begun, therefore, to develop broader guidelines and best practices for the security of sensitive data in business environments (Juniper, 2012; Kao, 2011)

## 3.2 Area 2 – Health applications

***Concerns:*** Health apps include any application software offering health- or medical-related functions for smartphones and tablets that are used by both patients and clinicians. Examples range from wellness and fitness apps such as calorie counters, to medical apps, such as those for managing chronic conditions or those tied to other wireless medical devices, such as vital sign monitors. More than 23 000 health and medical applications are available in the marketplace for consumer download (Happtique, 2012a). Emerging concerns include content, privacy and security standards of health-related apps.

***Regulators*:** Current federal regulators in the health applications' area include the Food and Drug Administration (FDA), the Federal Trade Commission (FTC), and, potentially, the OCR (through HIPAA). Some private organisations, such as Happtique, have emerged as pioneers of certification standards in the health applications arena.

The FDA's jurisdiction lies in its statutory authority to regulate medical 'devices' (FDA, 2013). To fall under FDA purview, an app must meet the FDA's definition of a medical device and must also be used either as an accessory to an already regulated medical device or transform a mobile communication device into a regulated medical device (FDA, 2012). Although the FDA began to define its role in app regulation through the release of a Draft Guidance in 2011 and congressional hearings in 2013, it has targeted its regulation of medical apps primarily to assuring the safety and effectiveness of the application (FDA, 2011; USHoR, 2013).

On 25 September 2013, the FDA issued its final guidance for medical app developers (FDA, 2013). This guidance, which has been in draft form for over two years (Dolan, 2013) describes how the FDA intends to apply existing regulations to the world of medical apps. The FDA is taking a pragmatic approach to this area: it is trying to balance the need for oversight with the sheer size and scope of the market and by focusing on apps that meet criteria considered to be medical devices and which pose significant risks if they do not work as intended. Given the number of health and wellness apps available to consumers and healthcare providers, the FDA rightly asserts that it simply cannot and should not try to regulate the entire market. According to the final guidance of September 2013, the FDA plans to only regulate those apps that are: 1) an extension of a medical device; 2) transform the mobile platform into a regulated medical device, or 3) perform patient-specific analysis by providing diagnosis/treatment recommendations. While programmes like in-depth app certification may become available, the sheer size of the market as well as the speed of development make it unlikely that such programmes will be able to cover more than a small fraction of the apps released.

A mobile application comes under the FTC's purview through the FTC Act's truth-in-advertising principles (Section 5) and the FTC's Fair Information Practice Principles (FTC, 2011a & 2012). The FTC's truth-in-advertising policy would prohibit unfair or deceptive practices in the mobile arena, including unsubstantiated claims by app developers about their products (FTC, 2011b). In contrast to the FDA's near-exclusive focus on regulating content of the app, the FTC also clearly outlines policies and enforcement actions that protect privacy of consumer data in the mobile arena (FTC, 2011b). However, the FTC has taken action against companies failing to protect the privacy and security of consumer information only in instances in which companies make deceptive claims that undermine consumers' privacy choices (FTC, 2011b).

Compliance with HIPAA for a health app depends on the app's user and the type of information contained in the app. An app used by a covered entity and containing protected health information would be subject to compliance with HIPAA privacy and security standards; an app used solely by a patient would not, regardless of whether the patient had health information stored in the app (Greene, 2011). When patients share data with a covered entity via an app, the application itself would not be subject to HIPAA, but the patient's health information would become subject to HIPAA regulations once received by the covered entity (Greene, 2011).

Private sector organisations, such as Happtique, are developing standards for health apps and supporting their dissemination via online app stores (Happtique, 2012b). Happtique's voluntary certification standards encompass a range of areas including operability, privacy, security and content (Happtique, 2012c). These standards integrate an array of federal agency rules and policies, including HIPAA Privacy and Security Rules, and various FTC and FDA rules and policies

## 3.3 Area 3 – Personal health records

***Concerns:*** A PHR is defined as 'an electronic record of an individual's health information by which the individual controls access to the information and may have the ability to manage, track and participate in his or her own healthcare' (OCR, 2012). PHRs may pose challenges to privacy and security of patient data. For instance, third party vendors of PHR systems may not be covered entities under HIPAA and therefore not subject to the same privacy and security rules as providers and health plans offering PHRs. Moreover, vendor privacy and security policies may differ significantly.

***Regulators:*** Similar to the regulation of health apps, regulation of PHRs varies based on the entity offering the PHR to the patient; any PHR offered by providers or insurers is subject to HIPAA regulations and must abide by HIPAA Privacy and Security Rules (OCR, 2012). Although privacy and security are concerns for any PHR, PHRs not offered by organisations such as providers or insurers are not subject to HIPAA regulations. They are, however, subject to the privacy policies of the vendor or other pertinent regulations, such as the FTC Act.

In September 2011, the Office of the National Coordinator for Health Information Technology (ONC) released a PHR Model Privacy Notice Implementation Guide: it outlined a uniform approach that any PHR vendor could use to be transparent about key privacy and security issues (OCR, 2012). The Model Notice is 'intended to enable PHR vendors to represent complex information that is accessible, consistent and conducive to informed choice' (ONC, 2011a). Using the ONC guide is voluntary, but any PHR companies that do not adhere to the privacy and security commitments stated in their PHR Notice may be violating the FTC Act.

## 3.4 Area 4 - Wireless medical devices

**Concern:** This area encompasses wireless-enabled medical devices; it includes technologies such as Concern:  This area encompasses wireless-enabled medical devices; it includes technologies such as low-cost sensors attached to a patient's body that collect and transmit patient vital signs to a nearby 'hub' device. Transmitting data to the hub allows doctors to access real-time patient data remotely (Linebaugh, 2012). Potential issues pertinent to mobile medical devices include maintaining reliable connectivity, ensuring interoperability between different devices and preventing interference.

Regulators: Regulators in this arena include the FDA, the Federal Communications Commission (FCC), and, potentially, the OCR. Given the fact that wireless-enabled medical devices are medical devices, the FDA regulates or approves them for use in the diagnosis and treatment of disease. Given that a defining feature of wireless-enabled medical devices is their ability to transmit real-time data wirelessly, the FCC also regulates the functionality of data transmission through a medical device. Thus far, FCC and FDA regulation of wireless devices has focused on safety, efficacy and operability of the devices; these agencies have given little attention to the privacy and security concerns related to wireless medical devices (FCC, 2012).

Wireless medical devices could fall under HIPAA purview if any covered entity uses such a device. In this circumstance, the wireless medical device needs to comply with HIPAA privacy and security standards.

# 4. Conclusions

Although several federal agencies in the US regulate each mHealth area to one degree or another, policy makers have yet to define rules that encompass health information generally. As depicted in our framework (see figure 1 and section 3 of this paper), the introduction of patient-owned mHealth technologies falls outside the reach of HIPAA. In 2008, the ONC published the Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information. This framework, however, focuses on organisations and entities, such as health information exchanges, and not individual patients as data generators and sharers (ONC, 2008).

Technologies in all four of these mHealth areas are being used in ways that integrate each component into an interrelated whole. This evolution in patient health information creation and exchange demands the development of comprehensive policies that span these areas. Health information privacy and security issues are a primary concern at the federal level (e.g. the detailed privacy and security objectives found in ONC publications) (ONC, 2008; 2011b). What is lacking – and what is depicted in the conceptual framework – is an integrated model that shows the interconnectedness of the mHealth landscape. Developing and rendering operational the necessary mHealth privacy and security policies requires such a framework as a precursor to these efforts.

Collaboration and information exchange, building on this framework, will be crucial for developing a sound policy to protect health information. In addition to collaboration across federal agencies, public-private partnerships can play a role in policy development. Private technology firms and boutique certification programmes are already outpacing federal policy in the development of standards and regulations for mHealth technologies. Moreover, many private sector guidelines already reflect existing multi-agency federal policy. To avoid duplication of efforts, federal efforts should build on this work.

As a result, with a conceptual framework outlined and relevant stakeholders identified, the last key component for drafting comprehensive mHealth privacy and security policy is a commitment to action by policymakers. Section 618 of the recently passed Food and Drug Administration Safety and Innovation Act (2013) calls for the development of a draft report that, with input from the FDA, ONC, FCC, and other stakeholders, outlines an 'appropriate, risk-based regulatory framework pertaining to health information technology, including mobile medical applications, that promotes innovation, protects patient safety and avoids regulatory duplication'. This mandate could serve as the final catalyst that policymakers need in order to engage in high-level discussions about mHealth privacy and security concerns. The call for such a report clearly demonstrates federal interest and dedication to mHealth. It also recognises the need for multi-agency and private-public collaboration. Using our conceptual framework as a foundation could foster development of a flexible, yet exhaustive, policy that would address privacy and security concerns in the context of the modern mHealth landscape.

## 5. References

Dolan, B. (2013). Republicans, EHR vendors want ONC to take over medical app regulation, retrieved May 9, 2013 from http://mobihealthnews.com/20839/republicans-ehr-vendors-want-onc-to-take-over-medical-app-regulation/.

Federal Trade Commission Act (1994). 15 USC § 45(a), retrieved May 1, 2013 from http://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap2-subchapI-sec45.pdf.

Food and Drug Administration (2011). Draft guidance for industry and Food and Drug Administration staff: mobile medical applications, retrieved March 13, 2013 from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

Food and Drug Administration (2012). 21 CFR 801.4, retrieved May 8, 2013 from http://www.gpo.gov/fdsys/pkg/CFR-2012-title21-vol8/pdf/CFR-2012-title21-vol8-sec801-4.pdf.

Food and Drug Administration (2012). Food and Drug Administration Safety and Innovation Act, Section 618, S 3187, 112th Cong, 2nd Sess, retrieved January 8, 2013 from http://www.gpo.gov/fdsys/pkg/BILLS-112s3187enr/pdf/BILLS-112s3187enr.pdf.

Food and Drug Administration (2013). Guidance for industry and Food and Drug Administration staff: mobile medical applications, retrieved October 11, 2013 from http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

Greene, A. H. (2011). When HIPAA applies to mobile applications, retrieved May 3, 2013 from http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/.

Happtique, Inc. (2012a). Happtique "eBook", retrieved May 3, 2013 from http://www.happtique.com/wp-content/uploads/HAPP_booklet010212hi.pdf.

Happtique, Inc. (2012b). Happtique Overview, retrieved May 3, 2013 from http://www.happtique.com/aboutus/overview.

Happtique, Inc. ( 2012c). Happtique app certification program: draft app certification standards, retrieved January 8, 2013 from http://www.happtique.com/wp-content/uploads/App-Certification-Standards-final.pdf .

Health Insurance Portability and Accountability Act (HIPAA) (1996). 42 USC 201, retrieved May 1, 2013 from http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm.

Health Information Technology for Economic and Clinical Health Act (HITECH) (2009). Title XIII of the American Recovery and Reinvestment Act of 2009, retrieved May 3, 2013 from http://www.gpo.gov/fdsys/pkg/BILLS-111hr1enr/pdf/BILLS-111hr1enr.pdf.

Juniper Networks (2012). Security best practices for mobility in healthcare, retrieved August 16, 2012 from http://whitepapers.medtechmedia.com/sites/default/files/Security%20Best%20Practices%20for%20Mobility%20in%20Healthcare.pdf.

Kao, (2011). Securing mobile devices in the business environment, retrieved August 16, 2012 from http://www-935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_business_environment.pdf.

Linebaugh, K.(2012). More hospital devices to go wireless. Wall Street Journal, May 23, 2012.

Office for Civil Rights (2012). Personal health records and the HIPAA privacy rule, retrieved September 4, 2013 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

Office of the National Coordinator for Health Information Technology (2008). Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, retrieved January 28, 2013 from http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf.

Office of the National Coordinator for Health Information Technology (2011a). About the PHR model privacy notice: background, development process, key points, retrieved September 4, 2013 from http://www.healthit.gov/sites/default/files/phr-model-privacy-notice-backgrounder-final.pdf.

Office of the National Coordinator for Health Information Technology (2011b). Federal Health Information Technology Strategic Plan 2011–2015, retrieved January 8, 2013 from http://www.healthit.gov/sites/default/files/utility/final-federal-health-it-strategic-plan-0911.pdf.

US Department of Health and Human Services, Food and Drug Administration (2012). Federal Food, Drug, and Cosmetic Act, 21 USC Section 201(h), retrieved May 8, 2013 from http://www.gpo.gov/fdsys/pkg/USCODE-2010-title21/pdf/USCODE-2010-title21-chap9-subchapII-sec321.pdf.

US Federal Communications Commission (2012). FCC dedicates spectrum enabling medical body area networks to transform patient care, lower healthcare costs, and spur wireless medical innovation. Federal Communications Commission, retrieved May 1, 2013 from http://www.fcc.gov/document/fcc-dedicates-spectrum-enabling-medical-body-area-networks.

US Federal Trade Commission (2011). Prepared statement of the Federal Trade Commission on protecting mobile privacy: your smartphones, tablets, cell phones, and your privacy before the United States Senate Committee on the Judiciary Subcommittee for Privacy, Technology, and the Law, retrieved May 8, 2013 from http://www.ftc.gov/os/testimony/110510mobileprivacysenate.pdf.

US Federal Trade Commission (2012). Fair information practice principles, retrieved May 1, 2013 from http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

US House of Representatives (2013). Committee kicks off three day hearing series on potential regulations and taxes on smartphones, tablets, and mobile apps [news release], retrieved May 9, 2013 from http://energycommerce.house.gov/press-release/committee-kicks-off-three-day-hearing-series-potential-regulations-taxes-smartphones-tablets-mobile-apps.

## Authors

**Robert Furberg**
RTI International, US
rfurberg@rti.org
http://www.epractice.eu/en/people/robertfurberg

**Alexis M. Kirk**
RTI International, US
mkirk@rti.org
http://www.epractice.eu/en/people/359048

**Douglas S. Johnston**
RTI International, US
djohnston@rti.org
http://epractice.eu/en/people/354937

European Journal of ePractice

A publication of epractice.eu

# Organising Information Connections for Mobile Healthcare

Humankind, organisations and technology are increasingly intertwining into new hybrid combinations. Such combinations exist on the basis of connections established between humans, organisations and technology, and between organisations, based on technology and technological applications (for instance in the field of mobile healthcare). These connections facilitate an ever greater stream of information and lead to a situation where hybrid systems are increasingly linked horizontally. Individuals collect and process their own information within their own environment and communicate this information to others: this potentially leads to the representation of a more accurate picture than is available in the status quo. Deviations from this everyday situation can then be registered more effectively and more efficiently. Professional care givers can give better and quicker advice tailored to an individual's needs either during a regular consultation (medical appointment) or at a distance. Technology and technological applications are clearly demarcating what can and what cannot be done. This brings up new questions about the organisation and governance of these connections, about the way information can be exchanged and shared within and between organisations, between people and machines, and by machines amongst themselves. We also have to ask what impact this shift has on the structure and responsibilities within organisations: for instance, within the healthcare sector.

Ben van Lier

Centric World of Innovation, Netherlands

Keywords

Electronic medical records, healthcare information technology, human resources, international comparative studies, public health

> “For mobile healthcare, the success lies in the software, which makes the connection between the different devices possible and which combines personal information with information made available by others.”

# 1. Introduction

Humankind, organisation and technology are increasingly intertwining into new hybrid combinations. Take, for example, the combination of a laptop, (wireless) networks and the Internet that makes people able to receive, edit and send (company) information anytime and anywhere.

Cyber Physical Systems, for instance, are combinations of information and communication technologies (ICT) applications that are integrated into physical objects and procedures. This combination makes it possible to exchange information from the object with regard to its location, status and context and to share it with people and machines. Such new combinations make it possible to monitor the relevant objects (and subjects) regardless of their location and time, and to monitor and control their current status.

Medical Cyber Physical Systems developed specifically for healthcare, are 'safety-critical, interconnected intelligent systems of medical devices', as stated by Lee & Sokolsky (2012). According to Lee & Sokolsky (2010), these medical cyber physical systems (mCPS) have in common that they are based on the possibilities that software offers and can be connected in networks. Therefore, they provide place- and time-independent, autonomous control: 'to provide continuous monitoring of the patient state and handling of routine situations' (2010). According to Lee & Sokolsky (2010), such a 'closed loop' monitoring of patients' current situation may help to reduce the workload of healthcare providers, because they only need to respond to exceptions to previously established health patterns. The use of such possibilities for place- and time-independent monitoring and control of patients not only increases the safety of the patients, but can also ensure that their treatment is performed more efficiently and effectively. Examples of such applications can be found in glucose meters, insulin pumps and heart monitors; a particularly noteworthy example is a blood laboratory of only 14 millimetres length, that is inserted under the skin and provides doctors with live data through a mobile telephone (Prigg, 2013).

New and hybrid combinations exist on the basis of connections established between humans, organisations and technology, and between organisations, based on technology and technological applications. These connections facilitate an ever greater stream of information exchange and sharing between organisations. Exchanging and sharing information enables organisations to be part of various different coalitions and networks. Such developments are also reflected within the emerging Internet of Things or the development of medical cyber physical systems. By their ubiquitous and networked nature, these kinds of mobile technology and technological applications are increasingly determining what can and what cannot be done within healthcare processes. This brings up new questions about the organisation and governance of these networked devices, the connections they have and the information they are exchanging and sharing between people, between machines and between, people and machines. Finally the question will be what impact these new combinations will have on the structure and responsibilities within organisations.

In an attempt to gain greater insight into the issues raised by these new questions, extensive research has been conducted over the past few years focusing on the following: whether the development of interoperability of information between organisations in for instance the public or the healthcare sector can be improved and made transparent using Niklas Luhmann's systems theory. This article will examine some of the results of this study, and first focus on the process of hybridisation followed by Luhmann's systems theory which will serve as a basis for the analysis and description of the concept of connection. Exchanging and sharing information between hybrid systems, i.e. the realisation of information interoperability, will subsequently be systemised into a theoretical model using systems theory. The interoperability principles ensuing from that theory will then be used to build a case for its use in the realm of mobile healthcare. The article will conclude by exploring new possibilities, such as self-organisation and a more ecological or horizontal approach to the set-up and management of organisations, based on insights into the development of networks.

## 2. Hybridisation

Technology, for example in the form of IT, mobile telephony, and networks such as the Internet, has triggered some fundamental changes in society over the past few decades. Technology and ensuing technological applications are reducing in size and offering ever greater functionality and increasing opportunities. In addition, they are becoming ever more independent in terms of time and place. Radio-frequency identification (RFID) chips, for example, are capable of emitting a signal and storing information. These tiny chips are already being attached to or incorporated into products or goods in order to make these products or goods identifiable and traceable anytime and anywhere. RFID chips are already being used in passports, rail passes, books or food packaging. The next step will see nanotechnology on an atomic or molecular scale deployed to create new possibilities through the production of minuscule new applications that are invisible to the human eye and can even reproduce unaided.

Nanotechnology is one of the latest and perhaps most compelling developments to come out of technoscience, the merger of technology and science. Many people classify such new applications as science fiction instead of proper science, but that is not doing them justice. As early as 1959, Richard Feynman, who would go on to win the Nobel Prize for Physics in 1965, predicted ways of manipulating and controlling things on a very small scale. By small scale he meant at the level of atoms and molecules. New forces, possibilities and effects are conceivable and possible on that level. The past few decades have shown enormous progress in the development of products and applications in this area. There are already hundreds of products incorporating nanotechnology, from sun cream to different kinds of coatings, and from tennis rackets to bandages or new kind of medicines. What these new products have in common is that they are, or are becoming, part of people’s everyday lives, and produced through the interdisciplinary use of technologies such as IT and nanotechnology, to name but two.

The development towards technology and technological applications on an ever smaller scale, enabling their incorporation into virtually everything, will increasingly capture humankind’s attention in coming decades. This unstoppable and irreversible trend in technology and technological applications will lead to humankind as well as the organisations it is part of and the society they live in, unwittingly merging with technology to an increasing degree. This paper refers to this merger of humankind, organisation and technology as a process of hybridisation. Any new and hybrid combinations of man, organisation and technology, as well as their interconnections, emerging from this process will have to become the starting point for all people’s thinking about organising and shaping organisations.

Information and the possibility of exchanging and sharing parts of information is then an essential basis for these new hybrid combinations. Within the care sector an example of these new and hybrid combinations could be, according to McCullagh and Augusto (2011), sensors worn on the body which work together with other sensors in their environment, thereby contributing to the collection, processing and exchange of information between the individual patient and the care giver.

## 3. Systems

The biologist Ludwig von Bertalanffy (1969) claimed in the mid-twentieth century that the combination of technology and society (such as nuclear bombs and the space programme) had become too complex for traditional scientific approaches and interpretative systems to grasp. In his opinion, a need had arisen for more holistic or 'system-oriented', and more generic and interdisciplinary, approaches. He formulated a general systems theory to that effect: a doctrine or a collection of accepted and well-founded general principles and methods which can be applied to all kinds of systems that are the object of scientific research in different fields. He defined a system as a complex of mutually interacting components, with interaction, meaning that these components are in a mutual relationship and that they all have an effect on each other. According to Von Bertalanffy, the approach that results from general systems theory is not limited to material entities, but rather intended for entities that are partly immaterial and largely heterogeneous in their make-up, such as organisations. When it comes to organisations, he states:

'System analysis, for example, of a business enterprise encompasses men, machines, buildings, inflow of raw material, outflow of products, monetary values, good will and other imponderables; it may give definite answers and practical advice' (1969:196).

Organisational theorist Russell L. Ackoff (1971) also denoted organisations as systems, because he considered them to be a constellation of interrelated and interacting components. He branded organisations as 'purposeful systems', i.e. systems that under steady circumstances have the capacity to define their own objective and direction. Following on from Von Bertalanffy and Ackoff, the new combinations of humankind, organisation and technology referred to above can be designated as hybrid systems. These hybrid systems connect humankind, organisation and technology and see them interact with each other and with other hybrid systems. The connections that arise within and between these new and hybrid systems define, as philosopher Martin Heidegger (1998/1927) observed, the way in which reality, as created by the joint efforts of man, organisation and technology, is approached. Such a new and specific combination will also appear within the development of mobile healthcare. The new and hybrid mobile healthcare system determines a new reality for healthcare and the features of the new healthcare products or healthcare services that are or will be produced and used. Heidegger's focus was increasingly on unearthing new phenomena produced by the relation between humankind, organisation and technology (e.g., nuclear energy or hydro-electric power stations). Heidegger discouraged people from considering technology as something mythical or unreal, urging us to look for the essence of applied technology, the relation with that technology and the underlying objective of technology usage. He found that technology and technological applications are increasingly becoming a framework around the actions of individual people or groups of people.

Following on from Heidegger, philosopher Don Ihde (2002; 2009) posited that modern humans should start devising an inter-relational ontology of entities that applies to new and hybrid combinations of humankind, organisation and technology. Inter-relational ontology refers to the inextricable link between human experience and the environment or world in which humans live. In that world, humankind and organisation are subject to continuous changes in their experiences and perception of reality. This is driven by the extremely high pace at which technology and technological applications are developed and applied, and have started to play a fundamental role in people's environment. Ihde argued for research into and analysis of the new embodiment of these relations, and to analyse them as relations of men, technology and world (IT digimedia). Embodiment is Ihde's concept that mainly signified the way in which humans approach their environment or world, connect with it, and the role of artefacts or technology in that. In this context, man-IT-man and organisation-IT-organisation relations in any shape or form can be taken as the embodiment of relations between hybrid systems that Ihde had in mind.

During the more than eighty years that passed between the ideas of Heidegger and those of Ihde, technology not only saw sweeping changes, but also became a more integral and invisible part of people's daily existence. That has not only changed people's relation with technology and technological applications and turned both into a given in their lives, but also increasingly the changes that are produced using this technology. Technology and technological applications are increasingly turning into the framework within which we live and work. Slowly but surely, man, organisation and technology are intertwining. Without even realising it, they are creating new systems of mutually interacting elements, as posited by Von Bertalanffy. The interaction between the different components in a system is enabled and shaped by technology and technological applications. Connections between the different components come about as a result of and are shaped by the available possibilities for information exchange and sharing between these components.

## 4. Information interoperability and systems theory

Owing to the fact that there are so many technologies and technological applications available (such as the Internet and mobile telephony), hybrid systems (comprising humankind, organisation and technology) are developing an ever greater need to exchange and share the information they have, independent of the where and the when. This development is, according to literary theorist Katherine Hayles (2006a; 2006b), in keeping with humankind's development into what she refers to as 'posthumans'. Posthumans are, in her view, subjects of mixed composition, a collection of heterogeneous components, entities made up of material and information with continuously shifting boundaries. This evolution is typified by the information processing that pervades every aspect of biological, social, economic and political reality, as well as the construction of reality itself. Furthermore this information can, in turn, be exchanged and shared between networks such as the Internet, which is the linking factor between these information-producing hybrid systems.

The possibility and ability of exchanging and sharing information between random hybrid systems can also be referred to as information interoperability. Interoperability is a linguistic compound that can mean several things. 'Inter' stands for applying mutual links between entities that have been or will be designated. The 'operability' part comes from the verb 'to operate', i.e. the ability to act, work or produce. Interoperability hence creates a basis for the development of a new form or a new system of communication between hybrid systems. Landsbergen & Wolken (2001) considered interoperability no more and no less than the problem of exchanging and sharing information between people and organisations in an information-technological environment. When one departs from the combination of man and technology, or organisation and technology, it becomes irrelevant whether information is exchanged and shared between people, between people and machines, or between two or more machines. In this context, interoperability can, in principle, be equated with the concept of people exchanging and sharing information simply by talking to each other when elements such as semantics and context are taking into account (van Lier, 2013a). Information interoperability basically enables the exchange and sharing of information between random hybrid systems. In order to partake in this new form or system of communication, the different participating systems will have to come to some agreement on what technology (protocols – standards) and semantics (language) to use, and in what context they want to re-use the information.

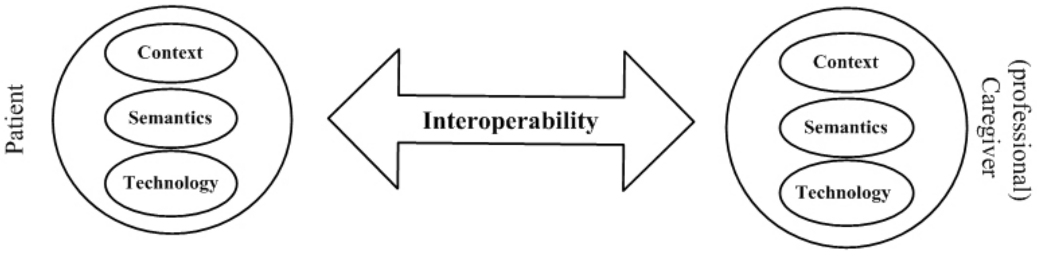


**Figure 1:** Interoperability

Whenever individual hybrid systems (comprising of humankind, organisation and technology), such as within the development of mobile healthcare, have the potential to exchange and share information, a process of communication between these systems can be started. In order to be able to explain and further ground this new and still developing system of communication between random systems, and therefore better understand and shape its further development, this paper draws on the five principles from Luhmann's (1995) general systems theory, as described by van Lier (2009; 2010). These five principles are: self-reference and autopoiesis, double contingency, system and environment, communication and action, and interpenetration. Using these five principles, a model has been devised for the analysis and design of the further development of communication between random hybrid systems and entities. The section below briefly outlines the five principles which will then be used as the basis to explain the proposed interoperability model.

## 4.1 Self-reference and autopoiesis

The interoperability model departs from the assumption that each separate system that wants to be part of this communication process has an independent ability for observation and an ability to use observations to make connections with itself and the outside world. Hybrid systems wanting to enter this communication process will be denoted by the symbol of a circular arrow pointing back to itself.

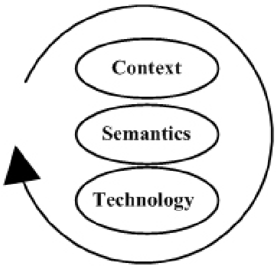


**Figure 2:** Self-reference and autopoiesis

Communication between these separate systems consists of elements that are created by and from the system and produced specifically for this process of communication. Luhmann refers to this process of creation as autopoiesis. ‘Auto’ stands for self, and ‘poiesis’ for creation. Luhmann, in turn, founds his general systems theory on the basic principle that every form of communication is in fact a differentiation of a system, including society as a whole as the sum of all these communications. Systems that self-create in this way should be considered as independent and autonomous systems. In this paper we can assume for instance, that within the development of mobile healthcare the patient, his or her smartphone and the sensors that the patient is wearing, is a new combination of this sort that could be considered as an self-referential and autopoietic system.

## 4.2 Double contingency

Being able to direct the components of communication, or determine the action between the systems, first requires a solution to the double contingency problem. Double contingency can be considered as a confrontation between two or more autonomous systems that each make their own selections in relation to each other. Solving the double contingency problem requires us to shift our focus from the single and autonomous system to two or more autonomous systems, i.e. to the interaction between two or more interacting systems. This shift in perspective is reflected in the model by a circular connection between two or more systems. Figure 3 shows such an interaction between a patient and a professional caregiver.

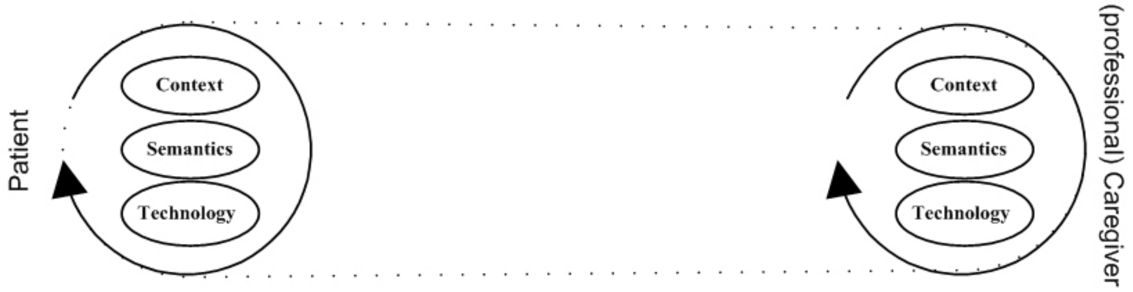


**Figure 3:** Double contingency

In this context, highly complex systems that provide and use information, such as humans, organisations or complex IT systems, are taken as a given. In addition, it is also assumed that these systems are ungraspable and unpredictable to each other. However, in the solution of double contingency, a single system focuses precisely on the question of whether the other system will accept or reject the offered communicative element. Within the developing vision on mobile healthcare the new combination of patient, smartphone and sensors is considered as a system which will try to be into contact with another system: for instance, the combination might consist of a professional caregiver and the technological devices that will be used to receive and interpret the received data.

## 4.3 System and environment

On the one hand, the communicative element generated by the system is captured in a difference that comes about as a consequence of the creation process by and from the system. On the other hand, it is also captured as a difference in the process of observation from the other system. This double difference is reflected in the model as two right-angled symbols (see figure 4).

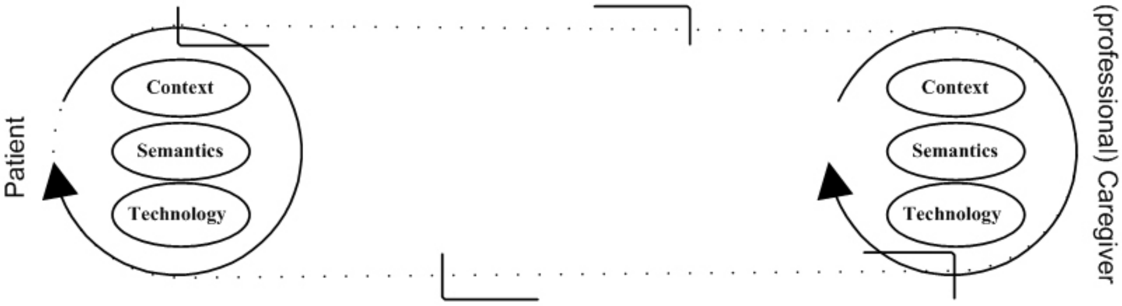


**Figure 4:** System and environment

Information, referred to here as a new selection by and from the system, can be considered an initiative to implement a change in another system. Every system has to take into account other systems in its environment, depending on the depth of the system's observation ability. The system's own environment thus also defines the system's identity.

## 4.4 Communication and action

According to Luhmann, it is a common misconception that communication only consists of sending and receiving information as stated by Claude E. Shannon (1948). People send or express information and hope that the beneficiary will be able to receive and accept this information, and will then know what to do with it. In this model, work is based on the foundation that a communicative element is a three-piece entity, consisting of the information selected by and from the system, the way in which selected information is expressed, and finally the way in which the selected information should be understood by the receiving system. This trinity is reflected in the model by the aforementioned right-angled symbols positioning the entity between selection and observation (see both figures 4 and 5).

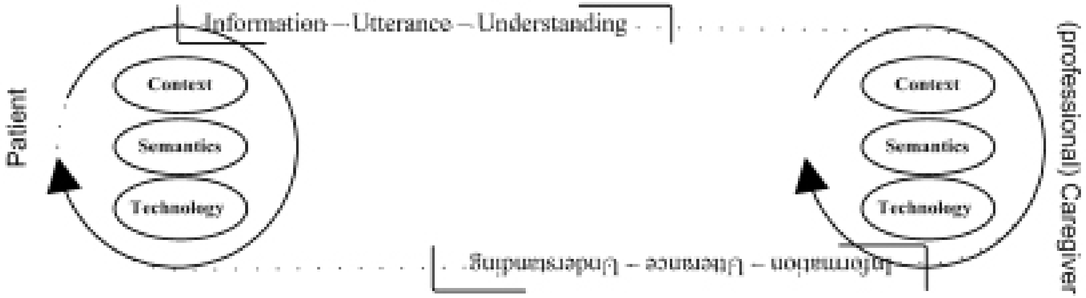


**Figure 5:** Communication and Action

This process brings about a unit of communication that can be communicated: a unit that is constructed and generated from and by the system; i.e., a unit that is not isolated or based on the perspective of an observer. The system reproduces itself in the unit of communication.

## 4.5 Interpenetration

The communicative unit can be rejected or received by the receiving system. When systems possess a reciprocal willingness and ability to accept the communicative unit, and are willing to allow communicative units from each other into their own system, a form of interpenetration comes about. The model presents interpenetration in the form of an arrow attached to the unit of communication, which is cleared to enter the receiving system. Systems thus allow communicative meaning from the outside to enter their own complexity. Systems proceed to incorporate this communicative unit into their own system and their sense-making process. The interpenetration of a communicative element from the environment and its incorporation, causes the sense-making process of the receiving system to change and evolve. Within the case of mobile healthcare, professional caregivers will accept or reject the receiving information within their own systems, allowing the information to become part of their own system. The caregiver will then interpret the receiving information, and assign meaning to it on which the caregiver can or will act.

To fully understand the combination of interpenetration and the act of assigning meaning, a link needs to be established between Luhmann's interpenetration concept and Karl E. Weick's sensemaking concept, as described by van Lier (2013b). Luhmann stated during a lecture on the 'Informationsgesellschaft' (information society) in 1996 that information should crystallise 'Sinn' or meaning in order to enable or continue further realisation. In Luhmann:

'und damit die Ambivalenz von Wissen und Nichtwissen in nächste Situationen zu übertragen'. Luhmann goes on to state that the English language would in this context denote this with the new word 'sensemaking' (1996:2).

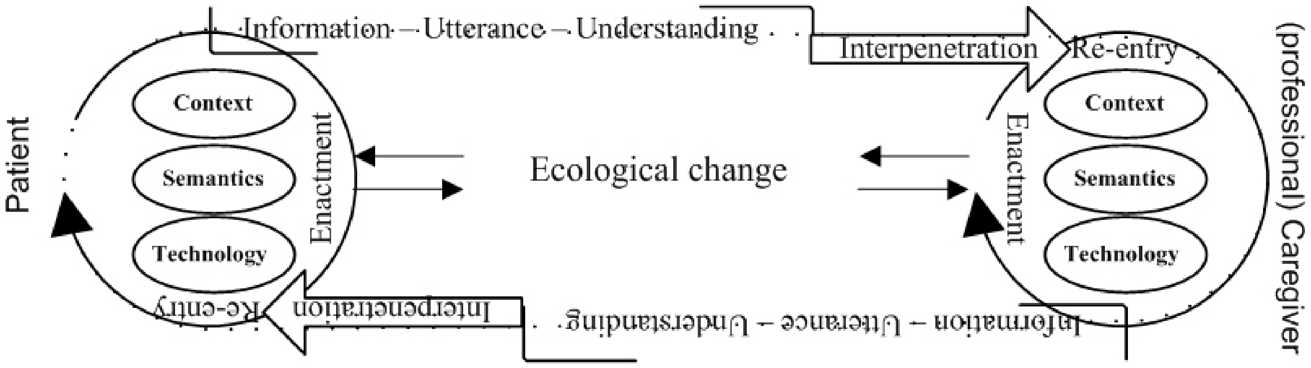


**Figure 6:** Interpenetration and sensemaking

The concept of sense-making, developed by Weick (1995), starts with a system that assigns meaning (grounded in identity constructions). The sensemaker will give meaning on the basis of knowledge and experiences accumulated in the past (retrospective). The receiving system will take action on the basis of the meaning assigned (enactment). Assigning meaning is, according to Weick (1995), the result of a social process based on a shared language and day-to-day social interaction. He considers the sense-making process to be a continuous one that cannot be detached from the context in which meaning is assigned, claiming that it can be of particular importance in organisations. That Weick considers the link to technology a crucial one in the sense-making process becomes clear from his following claim:

'Because technology is a crucial part of organisations, it is important to incorporate it into any discussions of sensemaking' (1995: 114).

According to van Lier (2010), the interoperability model outlined here leads to the following definition of interoperability between hybrid systems:

'the realization of mutual connections between two or more systems or entities to enable systems and entities to exchange and share information in order to further act, function or produce on the principles of that information.' (2010: 69).

## 5. Case: smart shoes and mobile healthcare

Free et al. (2013) note that the features of mobile technologies which can be connected to different kinds of networks:

'may make them particularly appropriate for providing individual level support to healthcare consumers related to their popularity, their mobility, and their technological capabilities' (2013:2).

For Free and colleagues the popularity of mobile technologies has led to high and increasing ownership of these technologies, which means interventions can be delivered to large numbers of people. This popularity of the technology can be observed, for example, when one goes jogging on a Sunday morning. A growing number of runners can be seen with devices attached to their arm. Often it is an iPod connected to sensors in their shoes, which register the amount of time the shoe is in contact with the ground. The information derived from this is then combined with an individual training schedule. A virtual coach will indicate how the performance compares against the personal training schedule. The advice given by the coach is based on information that is stored - via an Internet connection – after the run is completed in the training schedule made available on the Internet by Nike. This individual training schedule is based on information from runners all over the world, which is received, processed and analysed by Nike. This information is then combined with information from top athletes and top trainers. Using this data, Nike creates an individualised training schedule.

In a Wired magazine article in 2009, journalist Mark McCluskey (2009) described the essence of this Nike model: 'People change their behaviour – often for the better – when they are being observed'. Nike's success is not related to the device itself – similar pieces of equipment are already freely available. The success lies in the software, which makes the connection between the devices possible, and which combines the personal information with information made available by others.

According to Peterson et al. (2012), new developments that are based on hardware and software that are connected to each other may play an important role in the future in assisting individual elderly people living at home, for example, who suffer from dementia, for example. This is certainly the case when a combination of applications can support the individual elderly person in a specific and dynamic context (place, time and goal). For instance, this development towards interconnected hardware and software has also been envisaged by Jara et al. (2011), who specifically focus their attention on patients with diabetes.

According to the approach of McCullagh (2011), the exchange and sharing of information can contribute to direct action being taken when exceptional circumstances occur in the living situation of the relevant individual. One collects and processes one's own information within their environment and communicates this information to others, which leads to a more accurate picture than the normal every day one. Deviations from this everyday situation can then be registered more effectively and more efficiently. Professional care givers are enabled to give better advice, and more quickly, tailored to the individual during a regular consultation or from a distance. According to McCullagh et al., technology can provide a reliable filter: 'enabling the doctor to attend to urgent cases'. (2011: 62). Technological applications that are connected together in networks, that exchange and share information, can provide not only an important contribution to improving personal performances, but will in the future also contribute to the care and support of an increasing number of elderly persons in Europe.

In 2012, the European Commission (EC) published an eHealth Action Plan 2012-2020 (Com(2012) 736 final) which declared that: "We know from a wide range of other services that information technology applications can radically revolutionise and improve the way we do things". In this plan, the EC states that a significant barrier to using these possibilities is formed by a lack of vision of the interoperability of information within the care sector. It concludes that "the important issue of the lack of health data exchange can only be tackled by addressing in a coordinated way fragmented legal frameworks, lack of clarity and lack of interoperability". The EC therefore proposes the development of a specific interoperability framework for eHealth. This framework would operate alongside the existing eGovernment framework in Europe and other specific frameworks that are or will be developed for the exchange and sharing of information. This eHealth European Interoperability Framework (EIF) has been published in 2013. The eHealth EIF is a generic EIF for the domain of eHealth which builds on the European Interoperability Framework for eGovernment. In the systems theoretical approach to interoperability of information described in this paper, the specific eHealth related components of the eHealth EIF can be fitted into the components technical, semantics and context.

The conclusion can be drawn that the exchange and sharing of information between a range of human and non-human actors in random networks will become increasingly important and complex. Any solution for a specific sector will thereby no longer be adequate. The question of whether more investments should be made in a more fundamental and holistic approach to this challenge, including in the EU context, is then a topical one. The problem of the interoperability of information will eventually spread, slowly but surely, from the smallest level on a nanoscale to the effects on a macro scale of the exchange and sharing of information in the form of a society based on networks and the exchange and sharing of information within them. Certainly from the perspective of good and affordable care for the rapidly growing elderly population in Europe, collaboration in this area between sectors and above them is of crucial importance.

## 6. Networks

Modern organisations are generally still structured and shaped based on vertical principles, with information flowing from the top down. The process of hybridisation, the use and application of more and more connections, and the exchange and sharing of information through these connections, is increasingly undermining this verticality.

American researchers such as Shapiro et al. (2006) found that such a development towards better access to and better exchangeability of medical information actually leads to changes in the set-up of urgent care. They argue that doctors will as a result need greater involvement in the preparation of the exchange and sharing of information from different sources. However, they also point out that a lot of work still needs to be done to make this information exchange a reality, and they look into its impact on medical treatment. Establishing new connections within the healthcare sector based on technology and technological applications leads to a situation where hybrid systems, on an executive level, are increasingly linked horizontally.

There are, in the opinion of sociologist Dirk Baecker (2006), hardly any phenomena, events or activities in today's world that are not in some way interconnected or that do not co-produce as part of networks. In many situations it will be, or will become, unclear or imperceptible whether communication and interaction actually takes place between two or more persons, two or more machines, or a random combination of both (as can be seen in the development of mobile healthcare). As a result, organisations will turn into hybrid systems that will increasingly merge with other hybrid systems connected through networks that exchange and share information with each other. This unit of networked, interacting and communicating hybrid systems is sustained by information from other organisations and society as the whole of all communications.

In this context, organisations are increasingly showing a metaphorical resemblance to the human brain, as first suggested by Gareth Morgan (1986). Morgan based this metaphor on the idea that every aspect of an organisation's functioning depends on some kind of information processing. That makes an organisation a more or less closed system of information processing, where information is interlinked and converted into new links back to the organisation's environment based on the exchange and sharing of information and corresponding actions. An organisation's thinking and operations within these information interoperability-based networks does, however, require new insight into establishing and maintaining such connections. Based on these ideas, it can be concluded that the development of organisations as hybrid systems will in the future depend hugely on the connections and communication between different entities within the organisation as a system.

The development of organisations as systems will become dependent on connections and communication between an organisation as a system and its environment as argued by Ben van Lier and Teun Hardjono (2011). The extent to which an organisation will be able to assume the role of a hub and organise connections with other nodes in its part of the network will be decisive in the development and success of the organisation in its environment.

Dirk Baecker (2001) claims that people's thinking on organising and structuring organisations is changing, leading to drastic changes in both existing organisations and their management. People's thinking is changing from a hierarchical and functional approach to a more horizontal and connection-driven approach. This new approach mainly involves developing and maintaining relations as van Lier argues (2011) between the hybrid system's interior and its exterior world. As a hybrid system, an organisation will increasingly be incorporated into the networks in its environment on a social, technological and economic level.

The ability and willingness to operate in these networks will pose a growing challenge for the existing organisational structures as they are today. However, the organisation as a social system, which is based on traditional principles such as hierarchy, will not quickly or easily accept a different form or allow itself to transform, or be transformed, into a new structure. New theoretical insights are needed to channel such developments and support organisations in developing a new basis for themselves. Furthermore, new insights are also needed to be able to further develop new connections between organisations as hybrid systems and the environment they exchange and share information with.

According to Dirk Baecker (2006), this will not add up to hierarchical or organisational layers being wiped out by these developments, but rather to new functions being added to them to absorb the insecurities that are part and parcel of operating in networks. This changing environment with a horizontal rather than a vertical information flow requires the development and implementation of new and more ecological ways of managing and controlling organisations. These new forms of control and management must veer away from exclusively focusing on direct management of the execution or controlling of available information, and move towards self-organisation and self-management of and by small and self-organising hybrid systems. Organising thus becomes focused on creating small hybrid sub-systems that, within the greater whole, independently organise their connections, and exchange and share information with their environment within the boundaries of predefined frameworks. That will not only contribute to the development and growth of each sub-system, but also to the development of the system as a whole. Organisations arrange themselves as networks, and can therefore be included in networks around them without any problem. This is increasingly creating a likeness between organisations and living organisms in a living body with other organisms.

## 7. Conclusions

The hybridisation of humankind, organisation and technology is on-going and inevitable. This process of hybridisation forces organisations to conform to working in networks. Establishing and maintaining connections within these networks will be a crucial aspect for the organisation and execution of processes within these networks. In turn, exchanging and sharing information within these networks requires a horizontal rather than a vertical approach to organising. In the case of the development of mobile healthcare, patients and caregivers will also merge with technology into hybrid systems. Within this process of hybridisation the development of interoperability of information between these hybrid systems will be crucial to enable the exchange and sharing of information between humankind, between machines and between humans and machines within different networks. Patients, professional caregivers or other caregivers, healthcare organisations and technological devices will be integrated within these networks in which the exchange and sharing of information is self-evident. The exchange and sharing of information makes new types of organising healthcare and self-organisation of patients possible based on place and time independent availability of information. Organising information connections will be necessary to make optimal use of new technological developments such as mobile healthcare for patients, professional or other caregivers and healthcare organisations.

## 8. References

Ackoff, R.L. (1971). Towards a system of systems concept. Management Science 17 (11), 661- 671.

Baecker, D. (2001). Managing corporations in networks. Thesis eleven, 66, 80-98.

Baecker, D. (2006). The form of the firm. Organization, 13(1), 109-142.

Bertalanffy, van, L. (1969). General System theory. Foundations, Development, Applications. New York: George Braziller.

European Commission (2012).eHealth Action Plan 2012-2020 – Innovative healthcare for the 21st century. Brussels 6-12-2012

European Commission (2013). eHealth European Interoperability Framework, European Commission – ISA Programme

Feynman, R. (1959). There’s plenty of room at the bottom.

Free, C., Phillips G., Galli L., Watson L., Felix L., Edwards P., Patel V., & Haines A. (2013). PLOS Medicine. January 2013, 10 (1), 1-45.

Hayles, K.N. (2006a). Traumas of code. Critical inquiry, autumn 2006, 136-157.

Hayles, K.N. (2006b). Unfinished work: From cyborg to cognisphere. Theory, Culture & Society, 23 (7-8), 159-166.

Heidegger, M. (1927). Being and Time. Dutch edition (1998). Nijmegen: Zijn en Tijd.

Ihde, D. (2002). Bodies in technology. Minneapolis: University of Minnesota Press.

Ihde, D. (2009). Postphenomenology and technoscience, The Peking University Lectures. New York.

Jara, J., Zamora, A. & Skarmeta, A.F.G., (2011). An internet of things – based personal device for diabetes therapy management in ambient assisted living. Personal and Ubiquitous Computing. 15 (4), 431-440.

Landsbergen Jr., D. & Wolken, G. (2001). Realizing the promise: Government information systems and the fourth generation of information technology. Public Administration Review, 61 (2), 206-220.

Lee, I., Sokolsky, O., Sanjian, Ch., Hatcliff, J. & Jee, F. (2012). Challenges and Research Directions in Medical Cyber Physical Systems. Proceedings of the IEEE, Special Issue on Cyber Physical Systems, 100 (1), 75-90.

Lee, I. & Sokolsky, O. (2010). Medical Cyber Physical Systems. Dac'10 June 13-18 2010.

Lier, v. B. (2009) Luhmannontmoet 'The Matrix'. Uitwisselen en delen van informatie in netcentrische omgevingen. Delft: Eburon.

Lier, van B. and Hardjono T.W., (2010). Luhmann meets the matrix. Exchanging and sharing information in network-centric environments. Journal of Systemics, Cybernetics and Informatics, 9 (3), 68-72.

Lier, van B. & Hardjono T.W., (2011). A systems theoretical approach of interoperability of information. Journal of Systemic Practice and Action Research. 24 (5), 479-497.

Lier, van B., (2011). Connections, Information and reality. Thinking about the 'Internet of things'. Journal of Systemics, Cybernetics and Informatics. Special Issue on Collaborative Enterprises. 9 (5), 91-97.

Lier, van B. (2013a). Can Machines Communicate? - The Internet of Things and Interoperability of Information. Engineering Management Research. 2 (1), 55-66.

Lier, van B. (2013b). Luhmann meets Weick: Information Interoperability and Situational Awareness. (Emergence: Complexity & Organization (E:CO) 15 (1), 71-95.

Luhmann, N. (1995). Social Systems, Stanford: Stanford University Press.

Luhmann, N. (1996). On the scientific context of the concept of communication. Social Science Information, 35 (257), 257-267.

Luhmann, N. (2006) Systems as difference. Organization, 13 (1), 37-57.

McClusky, M., (2009). The Nike experiment: How the Shoe giant unleashed the power of personal metrics. Wired. http://www.wired.com/medtech/health/magazine/17-07/lbnp_nike?currentPage=all

McCullagh, P.J. & Augusto J.C., (2011). The internet of Things: The potential to facilitate health and wellness. CEPIS Upgrade XII (1), 59-68.

Morgan, G. (1986) Images of Organization, Sage Publications.

Peterson, C.B., Prasad N.R. & Prasad R., (2012). The future of assistive technologies for dementia. Workshop ISG-ISARC 27 June 2012.

Prigg, M. (2013). The medical lab implanted under the skin that can automatically phone a doctor BEFORE you fall ill. Retrieved from http://www.dailymail.co.uk/sciencetech/article-2296347/The-medical-lab-skin-automatically-phone-doctor-fall-ill.html#ixzz2fASUlfnO.

Shannon, C.E., (1948). A mathematical theory of communication. The Bell System Technical Journal 27, 379-423.

Shapiro, J.S., Kanry, J., Lipton, M., Goldberg, E., Conocenti, P., Stuard, S., Wyatt, B.M. & Kuperman, G. (2006). Approaches to patient health information exchange and their impact on emergency medicine Annals of emergency medicine, 48, 426-432.

Weick, K. E. (1995). Sensemaking In organizations. Thousand Oaks: Sage Publications.

## Author

**Ben van Lier**
Centric World of Innovation, Netherlands
Ben.van.Lier@centric.eu
http://epractice.eu/en/people/359025

# European Journal of ePractice

The European Journal of ePractice (EjeP) is a peer-reviewed online publication on eTransformation, launched in November 2007. The Journal belongs to the ePractice.eu community, is sponsored by the European Commission as part of its good practice exchange activity and is run by an independent Editorial Board.

The aim of EjeP is to reinforce the visibility of articles as well as that of professionals in eTransformation building an author's community which will strengthen the overall ePractice.eu activity. The publication will promote the diffusion and exchange of good practice in eGovernment, eHealth and eInclusion and will be open access, free of charge to all readers. We have a target audience of 50 000 professionals in Europe and beyond, and build on a community of some 25 000 members.

The scope of the European Journal of ePractice reflects the three domains of ePractice.eu: eGovernment, eHealth and eInclusion. We invite professionals, practitioners and academics to submit position papers on research findings, case experiences, challenges and factors contributing to a successful implementation of eGovernment, eHealth or eInclusion services in Europe and beyond.

You are kindly invited to read the current calls at www.epracticejournal.eu.

## Editorial guidelines

- Authors: Researchers and eGovernment practitioners at every level are invited to submit their work to Journal
- Type of material: Articles, case studies and interviews
- Peer-review: The articles are always evaluated by experts in the subject, usually peer-reviewer(s) and member(s) of the portal's Editorial Board
- Length: Full texts of 2 000-6 000 words (the word limit may be extended in exceptional cases)
- Language: English

## Article structure

- Title (no longer than 15 words)
- Executive summary of 200-300 words
- Keywords (3-6 descriptive keywords)
- Key sentence (single sentence which stands out)
- Tables, pictures and figures (attached in separate file)
- References according to the guidelines
- Author profile must be made public on http://www.ePractice.eu/people

For the full instructions please visit the submission guidelines at the web page of the European Journal of ePractice.