HealthManagement
Promoting Management and Leadership

Volume 14 - Issue 3, 2014 - Matrix

Medical Apps – A View From Medical Device And Data Protection Law

Authors

Eugenio Mantovani

PhD Researcher

Vrije Universiteit Brussel (VUB)

interdisciplinary Research Group on

Law, Science, Technology and Society (LSTS)

www.vub.ac.be/LSTS/

Eugenio.Mantovani@vub.ac.be

Efrain Castañeda-Mogollon

PhD Researcher

Vrije Universiteit Brussel (VUB)

Interdisciplinary Research Group on Law, Science, Technology and Society (LSTS)

www.vub.ac.be/LSTS/

This research was in part supported by the Brussels Institute for Research and Innovation (INNOVIRIS) under the framework of the project Interoperable platform for Remote monitoring and Integrated e-Solutions (IRIS). The authors also acknowledge the support of the European Commission-FP7 Marie Curie Industry-Academia Partnerships and Pathways Action 'VALUE AGEING' (GA 251686).

Key Points

• Medical devices and non-medical apps
• Medical apps in the context of data protection
• Processing sensitive data
• Recommendations for developers

The growth in the mobile devices market (smartphones and tablets) has been accompanied by a rapid increase in the number of software applications for mobile devices ('apps'). One of the fields propelling this market growth is the healthcare and life sciences sector and industry (Greenspun and Coughlin 2012). Modern smartphones and tablets are embedded with a variety of sensors, such as multi-touch touchscreen, accelerometers or gyroscopes, ambient light sensors, GPS, cameras, fingerprint sensors, facial recognition etc. These sensors are able to collect and store large amounts of data. Through an interface called Application Programming Interface (API), collected data can be accessed and processed by software programs or accessories, or a combination of accessories and software, that run on smartphones: what we call 'applications' or 'apps'.

Thanks to wireless communication networks – allowing continuous, real-time, exchange and 'crossing' of data, apps can be used for a wide variety of purposes, including the management of personal health, wellness, and wellbeing. For instance, many apps allow users to monitor their caloric intake for healthy weight maintenance: 'MyFitnessPal', 'LoseIt!', and 'DailyBurn' are just a few examples.

Apps can be used by healthcare professionals, nurses, physicians, and informal carers. For instance, the REACTION GlucoTab implements a mobile tablet- based workflow support system for nurses and physicians on the ward; its features include a validated basal/bolus insulin titration protocol. The Radiation Emergency Medical Management (REMM) app gives healthcare providers guidance on diagnosing and treating radiation injuries. Other apps allow for the monitoring of heart rhythm abnormalities, to carry out consultations on dermatology cases, etc.; and the list goes on.

As for most technological developments, e-health and mobile health technologies are laden with risks and uncertainties. Participants in studies highlight "clinical risks (misdiagnosis), social and interpersonal (interactional), personal and professional (overload of information, liability and role change), technical (failure) and organisational (poor integration)" (Finch et al, 2006). Two diffuse concerns relate specifically to the use of medical apps for medical purposes.

The first concern relates to the safety of the patient. Under EU law, safety requirements vary depending on whether apps are intended to be used for medical purposes or are instead intended to be used for 'wellbeing'. The second concern relates to the protection of personal data. Given the choice of the EU regulators to give leeway to the market in medical and pseudo-medical apps, a massive number of them are available in the market. Data protection law is summoned as 'second best' to regulate not the presence and the use of medical apps, but the personal data processing performed by those apps. In order to mitigate safety and privacy risks, technologically mediated healthcare provision must be compliant with the relevant legislative frameworks and requirements1. The relevant legal frameworks are the EU medical device framework and the EU data protection framework2.

Medical Apps In The Medical Device Framework

The primary purpose of the EU Medical Device Framework (MDF) is to ensure the same level of safety to all EU citizens using medical devices (Directive 93/42/ EEC)3. Article 1 of the Medical Device Directive (MDD) defines medical device as "software[…] intended by the manufacturer to be used for human beings for the purpose of: diagnosis, prevention, monitoring, treatment or alleviation of disease; diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap; investigation, replacement or modification of the anatomy or of a physiological process; control of conception […]". This means that software such as a medical app that works in combination with a device (a smartphone) is a medical device. Before being put into free circulation and used in medical practice, mobile technology and medical apps must satisfy the legal requirements detailed in Directive 93/42/EC. Once the requirements are fulfilled and validated by the competent national office (this can also occur by adherence to an internationall recognised software standard shown to be safe), the CE certification is granted. The CE certification guarantees that a medical device has been approved as meeting the requirements of the MDF and, being safe, must therefore be permitted circulation in all Member States.

Despite the obvious engagement of the MDF framework with medical apps, the EU regulator has been hesitant to take action in an area of obvious ongoing innovation and market growth (Mantovani et al. 2013). At present, there are apps being advertised or readily available which perform activities that fall within the aforementioned definition of a medical device, but which do not carry a CE stamp, and are not described by its manufacturer as intended for medical purposes. Arguably the main reason for this relaxed approach is economic. The costs involved with MDF compliance are estimated at up to €10m (EFPIA 2010; DiMasia 2007; European Commission 2012). Under a literal interpretation of the regulation, apps that have a clear medical purpose would have no choice but to comply with the demands of the MDF, regardless of the intention of the manufacturer. This means that under a literal interpretation of the MDF a large numbers of apps that have a quasi or pseudo-medical purpose, such as ECG for self-monitoring, would disappear (Mantovani et al 2013).

Do apps that have a clear medical purpose have the obligation to comply with the demands of the MDF? In 2012 this question came under the scrutiny of the highest Court of the European Union: the European Court of Justice (ECJ). The case Brain Products GmbH v. BioSemi VOF, which was referred by the Federal Court of Justice in Germany, concerned an application called 'ActiveTwo' which enabled human brain activity to be recorded. The plaintiff (a company competing with Active Two) argued that 'ActiveTwo' was not marketed as a medical device, though what it did (record brain activity) very clearly fit into the literal description of medical. The Court disagreed, espousing not a literal, but a teleological interpretation of the MDF. The teleological (from ancient Greek telos= purpose, aim) interpretation gives decisive weight to the purpose intended

by the manufacturer of the device or app. On the one hand, a medical device or app intended to perform an activity that falls within the definition (literal interpretation), must obtain the CE certification or satisfy the legal essential requirements, if its manufacturer expressly marketed it as a medical device. On the other hand, a device that de facto performs an activity that squarely falls within the letter of the definition, but is not intended to be used for medical purposes by its manufacturer, is not a medical device. Accordingly, in situations in which a product is not conceived by its manufacturer to be used for medical purposes, its certification as a medical device cannot be required (§ 30), says the Court (European Court of Justice 2012).

This 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. As a consequence, many medical apps that are appearing on the market have not been checked for compliance with the essential requirements of the MDF. They are not as safe.

Medical Apps In The EU Data Protection Framework

The vision of mhealth elicts concerns about the security and confidentiality of medical records. In the pre-digital era, the duty of medical confidentiality required doctors and nurses to keep drawers closed and avoid sensitive talk in hospital cafeterias and elevators. In the digital era, a growing problem is the increased number of personnel who have access to patient data, who may not always be, or feel, subject to the duty of confidentiality. Another drawback is that data can be easily lost: news reported the NHS North Central London Trust losing a laptop containing an estimated 8.3 million patient records. The same source reported that thousands of notes belonging to cancer patients have gone missing from the abandoned Belvoir Park hospital in Belfast, which closed in 2006 (The Independent 2011; The Daily Mail 2014). Many healthcare operators are careless in storing and exchanging medical information records, e.g. they carry diagnoses or x-rays in memory sticks without a password. With the advent of apps, the doctor's obligation of confidentiality becomes more complex to navigate. A recent study indicated that privacy policies were only present in 74% of the free apps, and in 60% of the paid apps. Such privacy policies were either included in the app, or externally available on the developer's website (Lie Nije 2013).

In addition, apps are generally not bound to a precise purpose. Data can be used for secondary goals, and there is little transparency about the duration of data storage, processing and the rights of app users. Apps often leave the user alone and even require him/her to open additional links to find information on external sites (Lie Nije 2013).

Apps that process sensitive data collected in any of the EU Member States must adhere to the EU data protection rules. The rules for processing and storing of medical data are found in Directive 95/46/EC, currently under revision (European Commission 2012) and in the so-called e-privacy directive (2002/58/EC). Because of their sensitivity, medical data can be processed only in a restricted series of circumstances. Aside from cases of emergency, or when the vital interests of the patient or others are at stake, two relevant conditions for the processing of medical data are: a) explicit informed – written – consent of the 'data subject'; and, b) when data are processed by a health professional subject to the obligation of confidentiality (Article 8 Directive 95/46/EC)4.

However, it is crucial to point out that being the principal carer or having received consent does not legitimise any use of the data not originally foreseen. Under the circumstances in which the processing is lawful, the data protection principle of data minimisation applies. As enshrined in the fundamental right to data protection (Article 8 EU Charter of Fundamental Rights; Article 6, Directive 95/46/EC) "… data must be processed fairly for specified purposes". Data minimisation mandates that all processing is both adequate for and limited to a specific purpose.

In addition, the EU data protection framework lists a series of rights of data subjects and obligations of data controllers and processors (the entities, like a hospital or a doctor or app developer controlling the purpose and the means through which personal data are processed). Data subjects have the right to receive information (Article 10, 95/46/EC). Pursuant to articles 12 and 13 of Directive 95/46/EC, app users must be put in a position to exercise their rights to access, rectification, erasure and object to their data being processed. Data controllers are under the obligation to keep the data secure, accurate, and to act promptly in case of data breach or leakages (adapted from Article 4 Directive 2002/58/EC). In a string of cases – Z v. Finland (1997), I v. Finland (2008) and, more recently, L.H v. Latvia (2014)5 - the European Court of Human Rights (ECHR) penalised states that failed to take appropriate steps to secure medical data, so that it cannot be accessed improperly. According to the Court, "what is required […] is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place" (I v. Finland, § 46).

The implications of the data protection regime for medical apps are as manifold as the risks, which are created by processing medical data through mobile health technologies. Some basic recommendations based on the legal framework can, however, be put forth.

1. Incorporate the Principle of Data Minimisation in Apps. – *Whoever controls or owns medical data should not process more personal data than necessary, and must not do so for purposes not defined and for indeterminate or excessive periods of time. As the case law of the European Court of Human Rights indicates, doctors and hospitals should not disclose patients' data to third parties, including law enforcement agencies and health or social security departments.*

2. Improve Security Measures. – *The use of mobile health technologies means that more people have access to personal sensitive information. As the case law of the ECHR suggests, the conditions for the lawful processing should be incorporated in the design of the device and of the apps. The controller should 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.*

3. Increase Transparency of Apps. – *Users of medical apps have the right to receive information, exercise their rights to access, rectification, erasure and object to data processing. It is important to provide users with instructions that clearly state whether apps are certified (the CE stamp) for medical purposes, and ensuring awareness of the kind of data that are being accessed and processed. Ideally apps developers should ensure 'by design' the proportionality of the data collection; customise information about data subjects' rights, including the provision of updates and adequate information; and notify any breach of personal data or security problems.*

4. Make Room for 'Granular' Consent. – *This recommendation is closely linked to transparency. Patients must understand what an app does before they can give valid consent in an informed, specific, truly free fashion. Consent must be obtained before information is gathered, but also before the information stored in the device – or accessible by the app, is processed. It should also be noted that patients withdraw de facto 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.*

5. Include Different Capacities. – *The ability of an individual to truly gauge the exact nature of his/her situation in an mhealth environment will vary enormously between a teenager and an elderly patient. It is questionable if apps processing data for medical purposes can be used without any supervision at all. In this regard, Portuguese data protection legislation allows users to have only indirect access to medical data through a physician. Similarly, the Belgian Commission for the Protection of Privacy advises patients to access their medical dossier under the supervision of a physician whenever possible.*

Conclusion

Many apps performing medical activities are not considered medical devices in a strict legal sense. Developers can get their way out of the requirements mandated by the MDF simply by not stating that the app has a medical purpose. The difference between considering an app to be a medical device or not is relevant for the safety of the patient, for doctors' liability, as well as for the relationship between patient and doctors. As a rule of thumb, it is advisable to read carefully the instructions that come with the app and verify the presence of the CE mark. Patients and doctors should avoid taking decisions relying on measurements provided by the hundreds of apps that are not certified medical devices. In any case, app developers and users are bound by data protection principles, rights and obligations. A safe medical app with a CE mark and software compliant with data protection rules will grant developers a solid competitive advantage.

Note

1 The law is one of the tools through which risks can be mitigated and arguably not the most important one. In medical practice, audit of services and clinical evaluation (trials) are the most widespread ways to stem perceived risks.

2 The EU Medical Device Framework (MDF) is one the most important EU 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). Similarly, the EU Data Protection framework is one the most important EU initiatives promoting the establishment and running of a European single market in which personal data can flow freely while the fundamental rights of individuals, in particular the fundamental right to privacy, are safeguarded (Preamble (3) and article 1, Directive 95/46/EC)

3 The MDF is at present composed of three different directives: Council Directive 90/385/EEC on active implantable medical devices (AIMDD), 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). In 2012 the Commission released a proposed new regulation.

4 Other exceptions include the protection of the vital interests of a subject unable to consent; when and for public health purposes, law enforcement or emergency. Under these circumstances data processing is allowed, but this does not mean that any kind of processing is legal (Article 8 Directive 95/46/EC).

5 These cases are retrievable from the Court search engine
http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx#{%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22]}

Published on : Sun, 31 Aug 2014