Mobile privacy – A better practice guide for mobile app developers

April 2013

Medical Technology
ASSOCIATION OF AUSTRALIA

www.mtaa.org.au

Level 12, 54 Miller St, North Sydney
NSW 2060 Australia
PO Box 2016 North Sydney
NSW 2059 Australia
P (+612) 9900 0650
F (+612) 9900 0655
E reception@mtaa.org.au

Executive summary

This submission is in response to the release in April 2013 by the Australian Government Office of the Australian Information Commissioner (OAIC) of a consultation draft paper: *Mobile Privacy – A better practice guide for mobile app developers.* The Medical Technology Association of Australia (MTAA) welcomes the opportunity to comment on the consultation draft and make specific recommendations. MTAA would like to see the consultation paper address privacy issues that may arise in the case where mobile apps are promoted for health or medical purposes. In some cases medical applications (apps) on smartphones may be marketed as medical devices. This area is currently unregulated in the Australian market.

MTAA **recommends**:

- Specific guidelines covering privacy for mobile medical apps and apps for health and wellbeing.

1. About the Medical Technology Association of Australia (MTAA)

The Medical Technology Association of Australia (MTAA) is the national association representing companies in the medical technology industry. MTAA aims to ensure the benefits of modern, innovative and reliable medical technology are delivered effectively to provide better health outcomes to the Australian community.

MTAA represents manufacturers and suppliers of medical technology used in the diagnosis, prevention, treatment and management of disease and disability. The range of medical technology is diverse with products ranging from consumable items such as syringes and wound dressings, through to high-technology implanted devices such as cardiac pacemakers. MTAA members distribute the majority of the non-pharmaceutical products used in the diagnosis and treatment of disease and disability in Australia. The medical technology industry had sales in Australia of more than $10.02 billion in 2010-11 and employs more than 19,000 people.

In response to the looming demand for healthcare we see the rapid adaptation of existing medical devices, and development of new applications for monitoring and treating health conditions in the home, that can respond to this demand. There has recently been an explosion of smart phone health and medical apps launch onto the market. These provide an innovative solution for self-management of a range of health conditions, however such apps are unregulated and in some cases a smart phone app may claim to function as a medical device with potentially detrimental consequences.

2. Features of the app market of concern

2.1. Consumerisation of medical devices

A wide range of health and medical applications (apps) can be downloaded for use on smartphones. MobiHealthNews made the prediction that by August 2012 there would be 6,000 smartphone apps available to medical professionals and 13,000 health apps available to consumers on the iPhone alone. Many apps are misclassified and it is hard to determine how many real (i.e., validated and reliable), medical apps actually exist. To date, only 75 mobile apps have received regulatory clearance from the Food and Drug Administration (FDA) in the US.

Medical apps for smartphones can be purchased by both medical professionals and consumers. There is concern about the use of unregulated medical apps by clinicians as a large number of mobile health apps are targeted at doctors to facilitate and improve patient health care, for example to perform calculations. A separate concern is the purchase of apps by patients who are less likely to have the ability to assess whether an app is able to do what it claims or a clear understanding as to how their data may be used. Consumers may prefer to monitor medical conditions using an app. For example, a diabetic person may prefer to track glucose levels on a smartphone as it is less conspicuous than using a glucometer (glucose monitor). However, in terms of risk, a smartphone app for monitoring glucose is no different from a glucometer in terms of the seriousness of complications should the app fail to work as intended.

2.2. Safety of medical apps for smartphones

The Apple apps store for iPhone has thousands of "symptom checkers" and medical apps available to download (some at no cost). In many cases these apps require user input of confidential health-related data. Smartphone health apps fall broadly into the categories of "medical" or "wellness"; an important distinction when determining whether an app needs to be regulated. In late 2011 the FDA stated that it would assess the safety of *"a small subset of mobile medical applications that present a potential risk to patients if they do not work as intended"*. These are mobile applications which have an intended use similar to that of a medical device. The UK followed suit and the first smart phone app has been approved by the Medications and Healthcare Products Regulatory Agency (MHRA). Likewise, in Australia, the Therapeutic Goods Administration (TGA) has stated that it will act to regulate certain smartphone medical applications (none have been regulated to date).

Mobile medical apps are different from wellness apps (e.g., calorie counters). Medical apps are intended for *"curing, treating, seeking treatment for, mitigating, or diagnosing a specific disease, disorder, patient state or any specific, identifiable health condition"*[1]. The distinction between wellness and medical apps can at times be unclear and medical apps designed to assist with prevention or monitoring can fall into a grey area. They may have a significant impact on health but are not intended to "cure". In some cases an app may be marketed to function as a medical device but may not actually fulfill this function. In the case of both wellness and medical apps, input of confidential patient data may be required.

Medical apps can be used to help patients monitor their own health conditions at home (e.g., tracking heart rate). More sophisticated apps may replace visits to

[1] www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm263280.htm.

doctors and may be connected to devices (e.g., a glucometer). Some smartphones even contain sensors to measure physiological signals, for example, cardiovascular disease detectors that can detect disease in real time (Oresko et al., 2010).

It is hard to know which medical apps live up to their claims or are of any use given that only a small number have received FDA clearance. For example, the accuracy of smartphone apps for diagnosing melanoma is highly variable. A recent study found that 30% of melanomas were incorrectly classified as benign by smartphone apps (Wolf et al., 2013). Likewise, it is difficult to ascertain whether apps are based on scientific evidence, are reliable and have been developed without conflict of interest (e.g., an app developed by a pharmaceutical company recommending a specific drug treatment).

It is only a matter of time before medical errors caused by incorrect use of medical apps gain major media attention. In 2011 Pfizer recalled a rheumatology calculator app because it gave erroneous scores for specific markers of disease activity[2]. The Federal Trade Commission (FTC) has removed two fraudulent apps from market in the US. The mobile apps "AcneApp" and "AcnePwer" both claimed to be able to treat acne using coloured lights emitted from the smartphone. The charges brought by the FTC barred the developers from making unsubstantiated claims and misrepresenting scientific data. Both companies were fined.

Anybody can create an app and it can be very lucrative to do so. A study assessing microbiology-themed apps found that only 34% had been developed with the guidance of a medical expert (Visvanathan et al., 2012). In most cases there are no clinical trials and no process of academic peer review in the development of a medical app. Many apps have lengthy disclaimers and claim to diagnose or monitor various health conditions; however in most cases the apps are not subject to any validation. It is often unclear where patient data will be stored, how this data may be used and who has access to it.

3. Regulation of medical apps

3.1. Food and Drug Administration (FDA)

In June 2012 Congress passed a bill that allows the FDA to regulate medical applications on smart phones (FDA Safety and Innovation Act). The previous year the FDA issued "Draft Guidance for Industry and Food and Drug Administration Staff; Mobile Medical Applications", which address how the FDA intends to apply its regulatory authority to a subset of apps that the agency has termed "mobile medical apps" (see Appendix A for the definition of a mobile medical app).

3.2. Therapeutic Goods Administration (TGA)

Medical devices are regulated by the TGA in Australia and must be included on the Australian Register of Therapeutic Goods (ARTG). The TGA has stated that it will regulate health apps for smartphones as the need arises. The TGA's current medical device regulatory framework provides for regulation of software for therapeutic purposes. There are some medical software tools listed including physician management and sleep assessment software. There are no current listings for

[2] Pfizer Ltd. Pfizer rheumatology calculator. Iphone/Android application. Important information. 14 October 2011. http://www.mhra.gov.uk/home/groups/fsn/documents/fieldsafetynotice/con137658.pdf.

medical apps for smartphones. TGA has stated that it will undertake an independent investigation if a complaint is lodged about a medical app or an add-on.

Medical devices have the potential to present a hazard, in particular if they are used incorrectly. Regulations are based on the principle of mitigating, to an acceptable level, the potential of a device to cause harm. Devices are classified according to the risk they present to the human body. Risk determines the level of regulatory oversight, including the level of evidence required before the device can be approved for supply. The manufacturer's intended use of a medical app for a smartphone will determine its risk level and regulatory requirements. Manufacturers of all medical devices have to undertake risk analyses to determine the residual risk when the device is used. Clinical evidence has to be developed if any residual risk cannot be eliminated so that the manufacturer can demonstrate that the benefit of using the device outweighs any residual risk. For Class I items, clinical evidence may therefore not be needed if it is possible to determine that benefit outweighs risk.

All medical device manufacturers and sponsors have to comply with post-market vigilance and monitoring requirements. Currently there is no process to review medical apps before they are released. There are a wide variety of medical apps, meaning that there is a wide variety of risks, for example medication names and doses may be uploaded incorrectly, glucose levels may be recorded incorrectly or patient data may be accessible to third parties. The TGA's role is limited to regulation of devices and clinical software. In many cases medical apps represent a grey area and it is recommended that app developers consult regulatory authorities to determine whether medical device regulations apply.

A recent article in the Medical Journal of Australia highlights concerns about the need for regulation of clinical software on personal mobile devices. The article focuses on apps used by health professionals and notes that *"In the absence of regulatory guidelines, physicians and health organisation need to be cautious about their use of this software, which, when linked to error, may lead to medicolegal consequences"* (Fernando, 2012, p. 437).

3.3. Privacy/data security concerns

Any smartphone app that interfaces with patient data should be regulated. There are concerns that software developers may create apps in order to access medical information. Juanita Fernando, from the Faculty of Medicine at Monash University in Melbourne notes that medical information theft is the fastest growing area of cybercrime in Australia[3]. When a consumer makes a purchase of a health or medical app they are likely to enter their names, addresses and phone numbers. Short message service (SMS) information is not difficult to intercept and medical apps can contain large amounts of confidential information. In many cases consumers do not read the fine print that states how their information can be used. In some cases apps can access the content of SMS messages and address books. Apps may be developed internationally by individuals not operating within the confines of Australian privacy laws.

The lack of legal certainty on the use of clinical software (e.g., MedCalc or iSthethoscope) on personal mobile devices such as smart phones and tablets exposes healthcare professionals to risk (e.g., ensuring data security). Legislation in

[3] See: http://www.theage.com.au/digital-life/smartphone-apps/an-app-a-day-keeps-the-doctor-away-20121220-2bp9s.html#ixzz2GyJaPStZ.

Australia does not address security risks such as monitoring activity on smartphones or security and transmission of user logins.

All 3G, 4G and tablet devices have the potential to harvest private information. A 2010 study by the Wall Street Journal reported that 64% of smartphone apps transmitted the unique device ID of the phone to other companies without user consent or knowledge, 47% transmitted the phone's location and 5% sent personal details such as gender and age[4]. Australian doctors load medical apps that may enable information to be collected by third parties. In many cases it is up to the user to change their settings and "opt out" in order to control what information can be sent by their devices. Many apps require users to click to agree to (lengthy) terms and conditions prior to download.

One of the greatest concerns over the use of smartphone apps in clinical care is the risk of breaching patients' confidentiality. Current regulations protecting health information stored electronically do not specifically address health information in medical apps.

Given the dramatic growth in medical apps, consideration should be given to developing guidelines for the collection and utilisation of this information.

[4] http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

References

Barton, A.J. (2012). The regulation of mobile health applications. *BMC Medicine, 10,* 1-4.

FDA Guidance Document: Draft Guidance for Industry and Food and Drug Administration Staff. Mobile Medical Applications. Document issued July 21, 2011.

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

Oresko, J.J., Duschl, H. & Cheng, A.C. (2010). A wearable smartphone-based platform for real-time cardiovascular disease detection via electrocardiogram processing. *IEE Transactions on Information Technology in Biomedicine, 14(3),* 743-740.

Visvanathan, A., Hamilton, A. & Brady, R.R. (2012). Smartphone apps in microbiology-is better regulation required? *Clinical Microbiology and Infection, 18(7):*E218-20.

Wolf, J. A., Moreau, J., Akilov, O., Patton, T., English, J.C., Ho, J., Ferris, L.K. (2013). Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection. *JAMA Dermatology, in press.*

Appendix A – FDA definition of a mobile medical app[5]

The FDA defines a "mobile medical app" as a mobile app that meets the definition of "device" in section 201 (h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act); and either:

- is used as an accessory to a regulated medical device that is regulated by the FDA (i.e. an app that enables a doctor to view medical images and make a diagnosis); or
- transforms a mobile platform into a regulated medical device (i.e. an application that turns a smartphone into an electrocardiography machine that detects abnormal heart beat or whether a patient is having a heart attack).

The FDA is concerned about those apps that pose identical or similar risk to public health as currently regulated medical devices if they fail to operate as intended. The components in a smartphone medical app may include a mobile phone, sensors, software and an associated network infrastructure, each of which could be classified as a device, component or accessory. The characteristic of a smartphone platform may pose a risk if, for example, a clinician is unable to clearly read an X-ray.

Apps that are *not* considered medical devices include[6]:

- Medical text and reference books such as teaching aids or materials
- Mobile apps that are used only to record, track, evaluate, or make decisions or suggestions in regard to general health and wellness. This is in the case where those decisions, suggestions, recommendations are NOT intended for disease treatment or any identifiable health condition. These types of apps include calorie counters, or decision tools relating to general health and wellness
- Mobile apps that automate general office functions such as billing, appointments, collecting patient history, and apps that replace paper-based entry
- Mobile apps that are generic aids to assist users (i.e. a magnifying glass) but are not marketed for a specific medical purpose
- Mobile apps for personal or electronic health record systems.

Examples of the types of applications for which the FDA will provide oversight are shown in Table 1.

Table 1: Mobile Medical Applications for which FDA will apply regulatory oversight[7].

Description	Examples
Mobile applications that are an extension of one or more medical device(s) or displaying, storing, analyzing, or transmitting patient-specific medical device data	- Remote display of data from bedside monitors - Display of previously stored EEG waveforms - Display of medical images directly from a Picture Archiving and Communication System (PACS) server - Control of inflation/deflation of a blood

[5] From FDA Draft Guidance for Industry and Food and Drug Administration Staff.
[6] FDA Guidance Document: Draft Guidance for Industry and Food and Drug Administration Staff. Mobile Medical Applications. Document issued on July 21, 2011.
[7] from Barton, 2012.

	pressure cuff - Control of the delivery of insulin from an insulin pump.
Mobile applications that transform the mobile platform into a medical device by using attachment, display screens, or sensors, or by including functionalities similar to those of currently regulated medical devices	- Attachment of a transducer to a mobile platform to function as a stethoscope - Attachment of a blood glucose strip reader to a mobile platform to function as a glucose meter - Attachment of electrocardiograph (ECG) electrodes to a mobile platform to measure, store and display ECG signals - App that uses the built-in accelerometer on a mobile platform to collect motion information to collect motion information for monitoring sleep apnea.
Mobile applications that allow the user to input patient-specific information and through the use of formulae or processing algorithms, output a patient-specific result, diagnosis, or treatment recommendation to be used in clinical practice or to assist in clinical decisions	- Mobile applications that provide a questionnaire for collecting patient-specific lab results and either: (1) compute the prognosis of a particular condition or disease; (2) perform calculations that result in an index or score; (3) calculate dosage for a specific medication or radiation treatment; or (4) provide recommendations that aid a clinician in making a diagnosis of selecting a specific treatment for a patient.

The FDA will address separately those medical apps intended to analyze, process or interpret data from more than one medical device. For example, analysis of Class I device information in conjunction with demographic information may result in interpretation of an acute patient condition which presents higher risk than the connected Class I device.