Group Briefing
February 2017

European Commission Draft Code of Conduct on Privacy for Mobile Health Applications

KEY CONTACTS

For further information, please speak to your usual Arthur Cox contact or one of the following lawyers:

PEARSE RYAN
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0518
pearse.ryan@arthurcox.com

COLIN ROONEY
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0543
colin.rooney@arthurcox.com

HUGH MCCARTHY
ASSOCIATE, TECHNOLOGY & INNOVATION
+353 1 779 4237
hugh.mccarthy@arthurcox.com

This document contains a general summary of developments and is not a complete or definitive statement of the law. Specific legal advice should be obtained where appropriate.

The Internet of Things is fast becoming a familiar feature of everyday life. Nowhere is this more apparent than in the health sector. The ubiquity of smart phones, tablets, sensors, wearables, personal trackers and similar wireless smart devices means that huge volumes of data concerning health, fitness, life-style, stress and sleep are being harvested and processed. This demand for services and products is feeding an enormous growth in mobile health apps ("**mHealth apps**"). A 2015 report commissioned by iMedicalApps[1] estimated that 165,000 mHealth apps were then available. A separate report estimates that the Mobile Health ("**mHealth**") sector will become a USD$59 billion market by 2020.[2] This new marketplace is certain to offer commercial opportunities for app developers, healthcare providers and health insurers, but also presents several challenges. In particular, there are important data privacy implications where personal data relating to individual's health and well-being is collected and processed on such a large scale. At present there is little harmonisation, whether by accident or design, across EU member states in terms of the data protection legislation governing this sector. The European Commission has acknowledged this legal fragmentation and in July 2016 proposed a 'Code of Conduct on privacy for mHealth apps' (the "**Code**").[3] This article provides an overview of the key features of the Code.

ADOPTING THE CODE OF CONDUCT

The European Commission submitted the draft Code to the Article 29 Working Party (the "**WP29**")[4] for approval in July 2016, which is required before the Code can have effect.[5] The WP29 has not yet approved the Code, or given any indication of when approval might be granted. If the WP29 does approve the Code, it will then be possible for eHealth app developers to adopt the Code. The Code is a voluntary framework and is thus not automatically binding on app developers. Those who wish to be certified under the Code are required to: (i) conduct a Privacy Impact Assessment

1 http://www.imedicalapps.com/2015/09/ims-health-apps-report/#

2 http://www.marketsandmarkets.com/Market-Reports/mhealth-apps-and-solutions-market-1232.html

3 https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised

4 The Article 29 Working Party is established under the EU Directive 95/46/EC and is made up of a representative from the data protection authority of each EU Member State, the European Data Protection Supervisor and the EU Commission. The Working Party acts in an independent advisory capacity and seeks to harmonise the application of data protection rules throughout the EU, and publishes opinions and recommendations on various data protection topics.

5 After entry into force of the General Data Protection Regulation ("GDPR") on 25 May 2018, the Code will then also have to be submitted for approval to the European Data Protection Board in accordance with Articles 40 and 41 of the GDPR.

("**PIA**"), together with submitting the results to the Code's Monitoring Body (the "**Monitoring Body**") (discussed below): and (ii) self-certify compliance with the Code.[6] If accepted by the Monitoring Body, the app developer and the mHealth app will be placed on a public register.[7] Continued adherence to the Code is necessary in order to remain on the register and the app developer can be subject to further investigations by the Monitoring Body, either by random selection by the Monitoring Body or following a complaint.

The Code has its origins in the Commission's Green Paper on mHealth (2014)[8], which revealed that 45% of consumers were concerned with unwanted use of their data when using mobile devices for health related activities.[9] The stated aim of the Code is therefore to "*foster trust among users of mobile applications which process personal data that includes data concerning health*". By certifying compliance with and following the guidance in the Code, app developers will not only go a long way towards ensuring full compliance with EU data protection legislation, but also potentially gain a competitive advantage by assuring consumer trust. Before submitting the current draft of the Code to the WP29, the Commission had earlier requested clarification from the WP29 on the scope of the definition of health data in the context of wellbeing and lifestyle apps. The WP29 identified three distinct situations whereby the processing of personal data by mHealth apps would be considered "*health data*":

» Data processed by an app that is inherently medical data;

» Raw sensor data that can be used to draw conclusions about the status of one's health; and

» Data where conclusions are drawn about a person's health status or health risk

SCOPE OF CODE

Differing slightly from the definition of "*health data*" given by WP29, the Code defines "*data concerning health*" as "*any personal data related to the physical or mental health of an individual, including the provision of health care services, which reveal information about his or her health status*". The Code makes it clear that it covers only apps dealing with data concerning health, and apps that deal only with users' lifestyles are excluded from the Code. For example, a lifestyle app that monitors the amount of steps someone takes in a day for the sole purpose of measuring the user's activity, but without processing that data to draw conclusions about that person's physical condition or health status, would not be considered a lifestyle app and would fall outside the scope of the Code. It would be bound by data protection law generally. It will be necessary to assess potential application of the Code to mHealth apps on a case by case basis.

The Code is currently governed by the Data Protection Directive 95/46/EC (the "**Directive**")[10], but it provides targeted guidance on how mHealth app developers can ensure compliance with the General Data Protection Regulation 2016/679 ("**GDPR**")[11], which will replace the Directive when it takes effect in May 2018. The Code is not intended to replace or add to existing data protection obligations (whether under the Directive or GDPR), but rather is intended to provide guidance to assist app developers in ensuring that their mHealth apps are in compliance with EU data protection law.

The Code addresses a broad range of problematic issues and sets out a number of guidelines for app developers, the most important of which are:

» ***User Consent:*** mHealth app developers must obtain the user's free, specific, informed and explicit consent for their health data to be processed for the purposes indicated by the mHealth app prior to or as soon as users install the app;

» ***Data Protection Principles:*** the principles outlined and defined in the Code include purpose limitation, data minimisation, transparency, privacy by design and privacy by default and data subject rights that are of the utmost relevance to mHealth apps;

» ***User Information:*** the user must be informed of the purpose(s) and lawful basis for which their personal data is collected and processed, the identity of the app developer, where their data will be processed and stored, including whether their data will be stored in other locations, such as back-up servers. Users must also be informed of their rights to access, correct or delete their data, as well as the right to data portability. A layered approach is recommended, whereby users are provided with a condensed notice which contains the vital information in accessible language with the possibility of clicking through to a full privacy policy containing all other relevant information. The information should be available before app installation and should be easily accessible again after installation should the user so wish;

» ***Data Retention:*** personal data may not be stored any longer than is necessary for the functionalities of the app. Criteria must be set out and communicated to the user for either the deletion or the anonymisation of data. As an alternative to deleting data, apps providers may also irreversibly anonymise personal data, such that there is no risk of individuals being subsequently identified from the data;

» ***Security:*** the Code requires the carrying out of a Data Privacy Impact Assessment and adoption of

6 The PIA under the Code is separate to the obligation contained in Article 35 of the GDPR to conduct a data protection impact assessment in instances of high-risk data processing. This is beyond the scope of this article.

7 http://www.lexology.com/library/detail.aspx?g=0ba6f737-556f-4427-86d0-ba3aef4a5d65

8 https://ec.europa.eu/digital-single-market/en/news/green-paper-mobile-health-mhealth

9 The Annual Report of the Irish Data Protection Commissioner for 2015 similarly raised general concerns about the data protection issues across a range of apps. https://www.dataprotection.ie/docimages/documents/DPC%20AR2015_FINAL-WEB.pdf

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

11 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

security measures which have been recommended by the European Union Agency for Network and Information Security (**ENISA**), which is a centre of expertise for cyber-security in Europe.[12] Provisions in both areas are outlined in annexes to the Code. It might be noted that mHealth app developers, as well as being within the scope of data protection legislation, including the Code (which is a voluntary arrangement), could also potentially be within the scope of the Directive on Network and Information Security (the "**NIS Directive**"), whether as an '*Operator of Essential Services*' or '*Digital Service Provider*'[13]. Further discussion of the NIS Directive is outside the scope of this article;

» ***Advertising:*** any advertising within the mHealth app must have been given prior authorisation by the content user, but this requirement differs depending on whether the advertising involves the processing of personal data. For contextual advertising, which is a form of targeted advertising based on the identity of the user and the content displayed, an opt-out option must be given to the user before any processing of personal data can occur;

» ***Use of Data for Secondary Purposes:*** any further data processing must be compatible with the purposes for which it was originally collected, as communicated to the content users. Processing for scientific or historical research may be considered as compatible with original purposes, provided all relevant national and EU level restrictions are observed. Data anonymisation or pseudonymisation may facilitate secondary processing for the purpose of big data analytics;

» ***Disclosing Data to Third Parties:*** Data may only be made available to a third party for processing after the user has been appropriately informed. A legally binding agreement must be entered into with the third party, which restricts the third party from processing the data for any purpose other than that which the user has been informed of and must contain specific security obligations on the third party;

» ***Data Transfers:*** The Code provides that data can be transferred and stored on the app developer's servers only if proper consent has been obtained from the user. Transferring data to third parties must satisfy conditions mentioned above, and, in the case of data transfers to locations outside the EU/EEA, legal guarantees are required to ensure that the transfer is permitted under EU data protection law (i.e. must ensure that the country to which the data is being transferred has an adequate level of data protection). The European Commission has published a list of countries that it deems to have an adequate standard of data protection. Subject to several exceptions,[14] the Directive states that transfers of personal data should not be made to countries not on this list;

» ***Data Breaches:*** The Code sets out practical steps to follow in the event of a data breach. These steps could be pro-actively implemented by app developers to compile a data breach "play-book" before a data breach occurs. The Code outlines the notification process that accompanies breaches of personal data. Note that, where applicable to a developer, the NIS Directive contains a (separate) notification and post-notification investigation, including potential sanction process; and

» ***Children's Data:*** The Code places specific focus on mHealth apps that are aimed at children. It is recommended that app developers pay attention to the age limit defining minors (which may vary from one EU Member State to another under the GDPR), and apply the most restrictive data processing approach to children's data. Moreover, it is noted that parental involvement is critical for such apps and therefore "*reasonable efforts*" must be taken by app developers to verify consent. The approach adopted in the Code largely mirrors that of the GDPR, particularly as regards the processing of children's data.

CODE OVERSIGHT

A three-tiered governance system has been proposed under the Code to ensure compliance with the Code and that the views of relevant stakeholders are taken into account. The governance of the Code will be financed and supervised by a General Assembly, comprised of representatives of all stakeholders, namely app developers, the "*data protection community*" (which appears to be the collective term for the relevant regulatory bodies), industry associations and end-users. A Governance Board consisting of 6 to 10 members selected from the General Assembly has been proposed to manage the everyday interpretation and maintenance of the Code, as well as any potential code amendments. Furthermore, a Monitoring Body comprised of members chosen by the Governance Board after consultation with the General Assembly will deal with complaints and ensure the adherence to and effective enforcement of the Code by keeping a public registry of all app developers complying with the requirements of the Code and by engaging in reviews of app developers' applications.

IS THE CODE LIKELY TO BE ATTRACTIVE TO APP DEVELOPERS?

While the purpose of the Code is to assist app developers in "*making responsible and informed choices that comply with European data protection law*", it remains to be seen whether the Code will prove attractive to app developers in large numbers. While the Code endeavours to assist mHealth app developers in complying with EU data protection law, there is no guarantee that stating adherence to the Code will lend a competitive advantage to app developers. Further if this were to be the case, it is unclear whether any commercial advantages accrued

12 https://www.enisa.europa.eu/

13 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

14 http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm

would outweigh the administrative and regulatory burden of continued compliance with the Code (such as the necessary completion of a PIA and ongoing checks by the Monitoring Body). For example, in certain circumstances app developers who conduct a PIA may be subject to an obligation to "consult" with the relevant data protection authority on the findings of the PIA.

CONCLUSION

The number and variety of mHealth apps has grown hugely in recent years and it is now clear that a harmonised EU data privacy framework is required to protect users' privacy and to ensure adequate security of data. As the privacy framework develops in this area, the integrity of mHealth data is intended to be ensured and the trust of the public in mHealth apps will grow. The potential for growth in the mHealth area is incalculable and will provide invaluable benefits to users, including empowering them and providing them with independence when it comes to managing medical and health conditions. However, it is important to foster such growth in a regulated environment so as to ensure the privacy and safety of all mHealth app users across the EU. Subject to WP29 approval, the Code is a step in the right direction in terms of consumers' data protection, but mHealth app developers may require a greater incentive to adopt the Code in order for the Code be a success.

Many thanks to Chloe Hawker for assisting in the preparation of this article.