Getting a Clean Bill of Health for Privacy in Your Mobile App

By Emily Hay and Jan Dhont, Data Privacy Department, Lorenz Brussels.

I. Introduction to the legal regime and risks

As the marketplace floods with all kinds of medical apps for mobile devices, doctors and patients are yet to realise their full scope and potential. These apps are also creating new relationships, bringing patients directly in contact with app developers who may not be accustomed to handling sensitive health information. It may seem that change is happening too fast for the law to keep up. In reality, however, many relevant laws are already in place and users and regulators alike are waking up to how they apply. Apart from the thorny issue of when a smart device becomes a medical device, there are data protection and privacy obligations to take into account.[1] Recent guidance papers issued by regulators in Europe and the US flag many privacy concerns, highlighting that regulators are alert to privacy and data protection issues and want them prioritised when developing and operating apps.[2] This is of particular importance for medical apps which make use of sensitive health information. With growing interest in privacy from app users and authorities, now is the moment to ensure that your mobile app is in line with data protection best practice.

This article focuses on some of the key data privacy challenges for those involved in developing medical apps. It is aimed primarily at app developers, but it should be borne in mind that device manufacturers, app stores and others will often have overlapping concerns. While privacy laws in Europe and the US are very different, regulators show strikingly similar concerns when it comes to apps. Some of those concerns include:

- defining the responsibilities of different actors in the app market;
- ensuring that apps do not abuse individual privacy by accessing and using more information than is really necessary;
- making sure appropriate measures are in place reflecting the sensitivity of information;
- ensuring that individuals are meaningfully informed of how their information is used; and
- getting valid user consent at the right moment.

[1] This article deals exclusively with the privacy and data protection aspects of mobile app development, and does not address the question of when a smart device becomes a medical device.

[2] Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices' (adopted 27 February 2013) (hereinafter: 'Working Party Opinion'); Kamala D. Harris, Attorney General, California Department of Justice, 'Privacy on the Go: Recommendations for the Mobile Ecosystem' (January 2013) (hereinafter: 'Privacy on the Go'); FTC Staff Report, 'Mobile Privacy Disclosures: Building Trust Through Transparency' (February 2013) (hereinafter: 'FTC Staff Report'); Atle Årnes and Catharina Nes, 'What does your app know about you?' (15 September 2011), Datatilsynet; Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, Düsseldorfer Kreis, (4/5 May 2011).

In Europe there are binding privacy laws in place and data protection authorities in each country ready to enforce them. In February 2013 a group representing these data protection authorities, the Article 29 Data Protection Working Party, adopted an opinion on apps on smart devices.[3] While the opinion itself is not binding law, it is a strong indication of how EEA regulators see privacy obligations in the app market and therefore could be used as the basis of future enforcement action.

Even if a business is not established in the European Economic Area (EEA) or specifically targeting EEA citizens, it could be obliged to comply with EEA law. This is because the law not only applies based on the country of establishment of a business, but also by virtue of the fact that the business may use 'equipment' such as computers and smart devices located in the EEA. If an app on a smart device (located in the EEA) generates traffic of personal information back to the app developer, then the Data Protection Directive is considered to apply to the app developer regardless of their location.[4] In the EEA a broad interpretation of 'personal information' is taken, meaning that any information linking to an identifiable individual triggers the application of the legal regime.[5] This includes data such as location information, contacts, unique device identifiers, credit card details, and pictures. Another important law to consider is the ePrivacy Directive, which has even broader provisions.[6] If an entity places information on, or reads information from, a smart device of a user in the EEA, the entity is required to provide clear and comprehensive information to the user about it and obtain their consent.[7] This obligation applies not just to personal information but to any information, meaning that installing an app on a smart device is sufficient to activate the law. Another provision specifies that user information and consent is required for any processing of location data.[8]

These European laws are important to take into account because their operation cannot be excluded by declaration or contract. This contribution puts some of the key legal obligations into context for those thinking of developing, or already operating, medical apps for smart devices.

[3] Working Party Opinion.
[4] 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.
[5] Article 2, Data Protection Directive.
[6] 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.
[7] Article 5(3), ePrivacy Directive.
[8] Article 9, ePrivacy Directive.

II. From provisions to practice: key challenges

One significant aspect of the proliferation of medical apps is that it brings app developers into direct contact with patients. Previously medical diagnosis, advice and treatment were the exclusive domain of health care professionals. There are many apps now stepping into this field, for example apps to track illnesses such as asthma or diabetes, or apps to manage medications.

These apps may be monitoring health symptoms and indicators, recording health incidents, receiving laboratory results, providing reminders to take medication or renew prescriptions, and communicating information to a doctor. This new role played by app developers brings new privacy obligations.

(a) Who is responsible?

Part of the challenge when it comes to mobile apps is determining who is responsible for what, especially when legal obligations are at stake. If a pharmaceutical company develops an app, or outsources the development of an app, it will be considered a 'data controller' under EEA law because it decides what information will be collected and what it will be used for. Data controllers have fairly heavy obligations to ensure amongst other things that information is used fairly and lawfully, that unnecessary or irrelevant information is not collected, that information is kept up-to-date, and that it is deleted or irreversibly de-identified when the purposes for using it expire. If there is a risk that you will be considered a data controller under EEA law, you should verify that you are complying with all your relevant obligations.

A 'data processor', on the other hand, only deals with personal information under the instructions of the data controller. This includes for example cloud storage providers storing personal information generated by an app, internet service providers hosting content on their websites, and call centres to which a particular function of a company has been outsourced. The key is that the data processor only acts on behalf of the controller. As soon as they use personal information for their own purposes, they become a data controller. There is not always a data processor, as the controller might do any 'processing' of the information themselves. It is also possible to have 'joint controllers' of the information in which case all companies are held liable for compliance with the applicable data privacy laws.

As new technology allows actors to use personal information in innovative ways, it can be difficult to pinpoint the different roles of controller and processor and the related liabilities. This does not mean, however, that the legal obligations do not exist. A careful assessment is necessary to determine the legal responsibilities you have based on the way you use personal information. Ignoring those responsibilities or taking a careless approach could backfire if an EEA regulator later takes a different view.

The Working Party Opinion goes through the different parties that may be involved in the app market and explains how they may be responsible under EEA law. Those with obligations include app developers, OS and device manufacturers, app stores, analytics providers and communications service providers. Each of these may be considered a data controller or processor of certain information and will therefore have responsibilities under EEA law. For example, app developers who choose the purposes for which an app collects information, and the means it uses to do so, will be the data controller of that information. App stores on the other hand are data controllers in relation to the information they collect for user registration along with any financial information, data about purchase and usage behaviour, etc. Even analytics providers are data controllers if they use information from different apps to create profiles for personalised recommendations. If they only provide analytics for an app without using the information for their own purposes, they are a data processor.

(b) *A case of TMI*

While the initial instinct may be to use your app to gather as much information as possible from users, collecting Too Much Information may be more trouble than it is worth. European laws prohibit the collection or use of data which is not necessary for the app to function.[9] US best practice guidelines also recommend that developers avoid or minimise the collection of personal information which is not related to the app's basic functionality.[10] This advice especially applies to sensitive information like health information as well as to geolocation data.

An important principle to keep in mind when developing an app is proportionality. If your app is collecting or using excessive data you will be in breach of the European Data Protection Directive, even if you obtain consent from the app user.[11] To avoid this, it is recommended to start the app development project with an assessment of what data your app will need to function and how it will be used. This way, you can make decisions which build privacy into the functioning of the app ('privacy-by-design'). For example, if the app has a feature making use of geolocation data, avoid continuously collecting that location information unless it is really necessary for the app to function. Similarly, if your app contains a feature to sync with a calendar or address book, make sure it does not access or retrieve personal information of the app user or their contacts and use it for other purposes. Doing so would generally be a disproportionate use of personal information because retrieving information is not necessary for the syncing to be carried out.

[9] Working Party Opinion, p. 17, 27.
[10] Privacy on the Go, p. 9.
[11] Working Party Opinion, pp. 16, 27.

US guidance frames this issue as 'surprise minimization'.[12] This is a useful measure when planning the way your app will use personal information – if you can see that an average app user may be unpleasantly surprised that the app collects and uses particular information, verify that it is really needed for the app to function.

(c) *Dealing with sensitive information*

The new situation of app developers directly handling patient information brings with it the obligation to treat that information with appropriate care. Health information is classified as sensitive information in both the EEA and the US, and is subject to special protections. If your app collects or uses health information, you should be sure that you have obtained consent for those practices from the app user.

You will also need to consider what information security measures you have in place to protect the sensitive information. Is the data stored in encrypted form? Could other apps on the smart device also access the sensitive information? Does the app interact with other apps that may have a lower level of security, e.g. an email app? These issues should all be worked through as part of your privacy-by-design approach.

Another matter requiring attention which is relevant for any kind of personal information but even more so for sensitive information, is your contractual safeguards. Rigorously examine your contractual relationships with any vendors, cloud service providers, or other service providers, to make sure that robust contractual arrangements are in place to protect the information. Under EEA law, as a data controller you are obliged to choose service providers (parties which will 'process' personal information on your behalf) providing sufficient guarantees in terms of technical security measures and organizational measures governing the processing. This relationship must be governed by a written contract.

(d) Small screen, big task

After having engaged in privacy-by-design to decide on how your app collects and uses information, the next challenge is to ensure that app users are informed about those practices and that you obtain their valid consent. The consent you obtain must be free, informed and specific. Transparency is key to a privacy-friendly approach, because obtaining valid consent is only possible if you have already informed app users of your privacy practices. Further, the app may not begin installation on the smart device before that consent is obtained.

[12] Privacy on the Go, p. 5.

In the EEA, there are certain specific requirements to satisfy transparency and ensure that consent is valid. The information that you must tell app users is (i) the name and contact details of your organisation, (ii) the type of personal information the app will collect and process, (iii) the exact purposes for which the information will be used, (iv) whether the information will be disclosed to third parties, and (v) how app users can get in touch with you about your privacy practices or to correct or update any information you hold about them.

Providing all this information in detail can prove to be a challenge on a small smart device screen. For this reason EEA regulators have endorsed the use of multi-layered notices, where the essential information is presented directly on the screen but users can follow a link to more comprehensive explanations, for example in a privacy policy. The crucial information to include on the screen will depend on your app – it should certainly include your identity as the app developer, but also information about the kind of data you collect or have access to, and the purposes you use it for. 'Surprise minimization' is a good guide again here – make sure you inform individuals of any use of their information that may not be obvious. The rest of the required information can be explained in full detail via a link to the privacy policy.

Only if app users are fully informed in line with the above can they validly consent to the use of their personal information. The Working Party Opinion refers to the need for consent to be 'granular', i.e. specifically provided in relation to each purpose of processing.

The EEA regulators insist that simply clicking an install button, or having app users accept a lengthy privacy policy, is not specific enough to give valid consent.[13] The purposes of processing need to be actually laid out on the screen so that users know what they are specifically consenting to, and can freely choose to use the app.

If EEA law applies to you (see I, II(a)), you will be obliged to obtain consent under the ePrivacy and Data Protection Directives for (i) placing the app on the smart device,[14] (ii) any collection or use of location data,[15] (iii) any collection or use of sensitive information such as health information,[16] and possibly also (iv) any intended international transfer of the information outside the EEA.[17] Where relevant, consent would also need to be obtained if personal information will be used for direct marketing. Not all of these consents can be combined, for example consent to the use of location data and sensitive information should be expressed separately. To ensure that separate consent is obtained, some app platforms use "just-in-time disclosures" to alert app users that this kind of data is being shared, and asking for their specific consent at that moment.[18] Collaboration with app platforms is therefore useful to ensure that separate consent is obtained, but also that it is not doubled up, causing unwelcome interference in the user's app experience.

To take the most privacy-friendly approach, app developers should give app users as much control as possible by allowing them to choose which features of the app they wish to activate, and which they do not consent to.

---

[13] Working Party Opinion, p. 15.
[14] Article 5(3), ePrivacy Directive.
[15] Article 9, ePrivacy Directive.
[16] Article 8, Data Protection Directive.
[17] Articles 26 and 26, Data Protection Directive.
[18] FTC Staff Paper, pp. 15-16.

This approach is suitable for apps with a variety of independent features or functions. If the app cannot function without using information for certain purposes, however, giving users such a choice would be misleading. Instead, it should always be clear that users can choose not to install the app, for example by pressing a cancel button.

While there is no easy answer to getting the notice and consent right, EEA regulators have called upon app developers to apply their creative skills to this challenge.[19] App developers manage to find innovative ways to design many app features in a way that makes sense for a small screen, and the notice and consent could benefit from equal attention. Both US and EEA regulators point to the potential for icons and images to communicate important privacy-related information. They call for collaboration with other actors like app platforms who could standardise such icons, as well as consumer testing to make sure the information is clear and understandable to potential users.[20]

III. Conclusion

App developers, users, and regulators alike are all grappling with the possibilities and implications of app technology. Medical apps have huge potential to influence the way medical diagnosis and treatment are undertaken, and more broadly health-related apps are already having an impact on everyday lives. As use of these apps grows, increasing attention is also being paid to privacy issues where those apps involve the collection and use of personal information. While up to now apps have often been developed with scant regard for individual privacy, moving forward this will not be a viable approach. This article has highlighted some of the privacy fundamentals to consider when developing a medical app. By adopting a privacy-by-design approach, you can ensure that as privacy standards are clarified and enforced in the app realm, you will be one step ahead.

[19] Working Party Opinion, p. 24.
[20] Ibid.; FTC Staff Report, pp. 16-19.