Translating GDPR into the mHealth Practice

Joana Muchagata
CINTESIS - Center for Health Technology and Services Research
FMUP - Faculty of Medicine of the University of Porto
Porto, Portugal
joanamuchagata@med.up.pt

Ana Ferreira
CINTESIS - Center for Health Technology and Services Research
FMUP - Faculty of Medicine of the University of Porto
Porto, Portugal
amlaf@med.up.pt

***Abstract*—The interaction between patients and health providers through mobile apps can potentially improve the efficiency and quality of healthcare. But despite the advantages, the majority of mobile apps provide low or no security protection and there is a lack of security standards and guidelines to support its development with an adequate balance between availability and confidentiality. Since May 2018, this lack of security awareness and measures has to change. With the application of the new General Data Protection Regulation (GDPR), the European residents' personal data processing by third parties will be stricter and more controlled. On the way to understanding how GDPR affects the content and interactions of mHealth apps, this article aims to compare how previous legislation is reflected in the interactions between users and those apps and what key changes must take place now that GDPR is in force. GDPR empowers patients to ask and receive in a simple understandable manner, information about the security measures that are applied to protect their personal data and transparently see how their personal data is processed, by whom and to what purposes. Use-case scenarios are presented to discuss the impact of GDPR key changes in the visual interactions between the user/patient and mHealth apps and how the app content can be adapted to a more objective and uncluttered view. This study provides means to easily and quickly integrate the key privacy and legislation requirements from GDPR into app visualization, improving this way availability, transparency and patients' empowerment.**

Keywords—General Data Protection Regulation (GDPR), EU Data Protection Directive, Privacy and Availability, Visual Interactions, mHealth Apps, Patients' empowerment

I. Introduction

The globalisation, technological advances, rapid innovation and the increase of system's complexity in many fields is translated in profound challenges for privacy and protection of personal data [1] [2]. On May 25 2018, the European Union (EU) General Regulation on Data Protection (GDPR) has come into force to regulate the principles and rules applicable to the processing of personal data [1] [3]. As it is happening in many different areas, also in healthcare, there are several changes regarding personal data protection. In the example of mobile health apps, some studies refer that the interactions between a patient and a health professional, through a mobile app, can significantly improve the efficiency and quality of healthcare [4] [5]. But not all are advantages and often there is a lack of security standards or guidelines to follow and the majority of existing mobile apps provide low or no security protection [4].

Thus, the main goal of this paper is to analyse what changes the new regulation brings and what procedures should be implemented in order to translate that regulation to the interactions between users (patients and health professionals) and mHealth apps. Although GDPR regulation has been decided since 2016, the authors could not find in the research literature works that can provide clear methods to translate the key changes that need to occur between previous and current GDPR legislation regarding users' interactions with mobile apps. This paper also aims to make this clarification and provide interested researchers and developers with sample use-case visualizations to be adapted to their needs. A detailed comparison is made between the look, feel and content of the mHealth app using previous data protection legislation and the key changes introduced by GDPR and how these can impact security and availability.

II. State of the Art

In Europe, the adoption of the Data Protection Directive 95/46/EC [6] was very important in terms of protection and processing of personal data. And even though the key principles remain valid, the world of today is very different and over the years it was difficult for this Directive to keep up with the development of the new technologies and the needs of the current society. This situation eventually made the Directive not ensuring the necessary effectiveness in the protection of personal data, nor the uniformity necessary for the EU [7]. Consequently, and after 20 years, Europe is experiencing a major change in data privacy regulation. The Data Protection Directive 95/46/EC was replaced by the new EU General Data Protection Regulation (GDPR), legally enforceable since the 25th of May 2018 [1] [3].

GDPR is designed to enable individuals to better control their personal data (including a better perception about how their personal data are going to be used on the Internet). Individuals' personal data includes, among others: basic identity information (name, address and ID numbers); web data (location, IP address and cookie data); health and genetic data; biometric data; racial or ethnic data; political opinions and sexual orientation. GDPR intends to protect all EU residents from privacy and data breaches in a gradual data-driven world. Thus, GDPR will allow the modernization and standardization of the legislation throughout the EU [7].

A. GDPR Key Changes

A summary from GDPR [3], the Official Journal of the European Union [1] and the Portuguese National Commission for Data Protection [8] comprises:

- more rigorous requirements for individuals' consent, that should be obtained using a clear and understandable language. Silence and pre-validated options or omissions are not valid forms of consent;
- no longer the use of long and illegible terms and conditions full of legal terminology. More transparency is required and data processing information should be easy to access and understand;
- the extension of special data categories to: biometric data, race, ethnic origin, politics, religion, genetics,

978-1-5386-7931-9/18/$31.00 ©2018 IEEE

health, sex life and sexual orientation. The processing of such types of data is prohibited by default and can only be processed if the data subject gives explicit consent or in a small number of specified situations;

- the right for individuals to be informed if their data are being processed, how, where, and for what purpose;
- the portability of personal data between companies;
- the right to be forgotten when data are no longer needed to the original purposes of processing;
- ensuring Privacy by Design (PbD) which means that data protection should be included since the beginning of the systems' design;
- the obligation to notify supervisory authorities and individuals affected within a maximum of 72 hours when a data breach may result in a risk for the rights and freedoms of people, subject to heavy penalties;

B. User and Mobile Health Applications (mHealth Apps)

Healthcare systems have been following the digital innovation and Mobile Health applications (mHealth apps) are increasingly used. Among many other advantages, mobile apps can improve efficiency and quality of healthcare [4] [5]. They help to improve communication and care coordination among specialists, doctors, nurses, and others, providing access to services independently of time and location. Physicians may access patient records, view test results and prescribe medications [9] [10]. At the same time, different studies have shown that patients who use mobile apps and have access and update their Electronic Health Records (EHRs), play an important role in the maintenance of their own health [11] [12]. Physicians and patients can share information as diagnoses, prescriptions, lab results and even schedule appointments. This can also be beneficial in emergency situations [12].

There are different apps available for different types of needs, many of them full of features and useful functions. But despite all the benefits they may offer, there are legal and security concerns. Some apps, in addition to store and process heath data, they also collect information (including sensitive data) such as username, password, contact information, age, gender, list of contacts, personal photographs, among other data [10]. They can also access the global positioning system (GPS) functionality which allows obtaining the location of the device, and in turn, the user (patient) who carries it. Furthermore, many times users do not know how their data are going to be used and from which type of organizations. There is also a lack of standardization and security measures on the majority of applications, as well as low protection of data transferred through the mobile and wireless networks [4].

III. Methods

After the analysis of GDPR key changes, the authors need to explore how these changes will influence the interactions between the user and a mobile healthcare system. This interaction could be done in different stages (from system's installation until its daily use) so it is important to verify what could be done to both apply the new legislation as well as improving data privacy and availability.

Taking into account certain elements such as: the privacy policy, request for consent, choices, sensitive data, among others (from Data Protection Directive 95/46/EC), and taking into consideration the changes that have to be implemented with the GDPR, the authors identify what could be done to protect users and their data at different levels of interaction between a user and a mobile app. This is expressed within a table where a comparison between the selected elements is described. Further and in order to validate the ideas that were compared, the authors propose use-case scenarios based on how a mobile healthcare app could comply with GDPR. With before and after mock-up visual interfaces, those scenarios are shown where some of the key changes proposed by the GDPR are applied and further discussed.

IV. GDPR and the Impact on Mobile Health Apps

Taking into consideration the rules of the new regulation [1] [3] and the few available studies [7] [13] [14] [15] on the topic, we propose the translation of some key changes of that regulation, which focus on protecting the user at the moment of interaction, into visible scenarios. Table I presents, on the first column, the key topics analysed, on the second column the situation described under the Data Protection Directive 95/46/EC, and on the third column how that situation changes with the new GDPR rules. Within this column, ideas/methods from other studies are also proposed to comply with GDPR. The goals are to provide compliance, improve the interaction between the user and a mobile app and at the same time ensuring the security and privacy throughout users' navigation and interaction experience. All data is supported by references.

V. Use-case

With the help of Table I, the authors present a use-case where they compare a few scenarios of a fictitious mHealth app (named iCare) complying, on one hand, with previous legislation to protect users and their data at different levels of interaction between a user and a mobile app and, on the other, with GDPR requirements. Five different scenarios are presented: privacy policy, consent, choice, customization of permissions and special categories of personal data.

Privacy policy and special data categories: Figs. 1 (before) and 2 (after) represent different scenarios which can influence the security and usability when installing a new application. In Fig. 1, it is possible to install iCare through the button "Agree and Continue" even without reading the privacy policy. If the user intends to read the full privacy policy, usually this is presented as a long document with small lettering and difficult legal terms to understand. In Fig. 2 (left), the user is advised about what kind of features the app needs to work with and to proceed s/he needs to go to the privacy policy page. Instead of a long list of legal information (such as in Fig. 1), the middle picture shows the relevant items which are rendered to the user through icons, with a short and clear explanation below. There is also a link to the full privacy policy, if required. The rightmost picture (Fig. 2) presents more information related to a sensitive data icon identified with a danger sign. The user needs to provide explicit consent for the processing of special categories of data. The visual proposal makes it easier/quicker to both understand and choose options within the same screen.

TABLE I. DIFFERENCES BETWEEN PREVIOUS DATA PROTECTION POLICY AND SOME KEY CHANGES GDPR BRINGS

Key changes	Data Protection Directive 95/46/EC	EU General Regulation on Data Protection (GDPR)
Privacy policy and terms and conditions (1)	Use of long and illegible terms and conditions full of legal expressions, often difficult to understand. This information is available at the EU General Data Protection Regulation Portal [3]	Information should be communicated in a concise, transparent, intelligible and easily accessible form, using clear and plain language. Art 12 - 1; [1] [3] A mobile privacy policy and the information about the terms and conditions can start with an icon, label, image or a link. Then, it can be linked to a short form notice, no longer than a single screen and with the important points. In the short form notice a link to the full privacy policy should be provided. The privacy policy should also be visible (e.g., with an icon) at all times while the user navigates the application [14]
Request (explicit) consent (2)	The request for consent is mentioned in the directive but it is not clear how it is presented to users. Lines (30) (33); [6] With our experience with some digital systems, many times the consent mechanism is just an "I agree" box or a checkbox without enough supporting information	When users need to make a decision about whether to give consent to the collection of their personal information, they must have a button or a ticking box complemented with clear, specific and targeted information. Line (32); Art. 4 (11); Art. 22 - 2 (c); [1] [3] [13]
Making a choice (multiple purposes) (3)	Many times the user's consent is given just for one purpose, once, but information is used for various purposes without any subsequent consent. Line (39); [6]	When information is going to serve multiple purposes, users have the right to consent their information being used for one purpose but not for another. Lines (32), (33); Art. 6 - 1(a); [1] The app must provide a list of unticked checkboxes or yes/no buttons to easily verify that information [13]
Access to user's data (4)	Sometimes data are disclosed to third parties often without being planned at the time of collection. Lines (30), (39); [6] Today companies make use of user's data for the most diverse purposes, such as for personalized advertising, and even selling to other companies without user's consent [7]	Users have to give consent for the collection and use of information either if it is just for one purpose or for several purposes. When the processing has multiple purposes, consent should be given for each one. Lines (32), (33); Art. 6 - 1(a); [1]
Privacy dashboard (5)	Some apps have a privacy dashboard but many times they just have an on/off button without complementary information [14]	Users must have access to a privacy dashboard where they can control their privacy settings. The tools should be easy and straightforward to use with an explanation of the consequences of making certain choices [14]
Permissions customization (6)	Several apps do not have this option and others cannot be modified by the user. Commonly, the description of the apps that have this option is difficult to understand by the user [7] [15]	Permissions must be visible and users should have the right to edit them. Apps should have a list of permissions and each of them must have a description of their privacy implications, specially permissions related with sensitive data associated with privacy leaks (e.g., address book or location) [7] [15]
The right to be forgotten (7)	Usually information is kept even when it is not necessary anymore [14]	Users should have the opportunity to track their profile, edit information and delete it entirely if they wish. Art. 17; [1] [3] [14]
Sensitive data (8)	Although special attention is paid to sensitive data, this directive does not specify all types of data that can be considered as sensitive data. Lines (34) (60); [6]	The new regulation has extended the range of special data categories, including, for instance, biometric data. Art. 9 - 3; [1] Graphics in the app are very useful when sensitive information is about to be transmitted and user consent is required. Icons, forms, colours, and sounds can be used to draw user's attention. The intensity or volume can be scaled depending on the information's sensitivity or the importance of the decision [13] [14]

Request for consent / Making a choice: After login in to iCare, the user can see a new message to read. A message is about a campaign and consent is required from the user in order to participate. In Fig. 3, the options are just "Yes" or "No" without enough information to support the answer. In this case, by choosing "Yes", the user is giving consent without being properly informed. In its turn, Fig. 4 (middle) provides a message with more complementary information which potentially helps the user to take a more informed decision. After reading all the information, the user can go to the next page where a list is presented with several options regarding other institutions that can also use the supplied data (rightmost display in Fig. 4). Users are free to choose several or none [1] [3] [13]. Only at the end, will the user decide if s/he agrees to participate in the campaign.

Privacy policy icon: One other new element is about the privacy policy. Under GDPR, the privacy policy should be on the landing page of any web application and be visible at all times while the user navigates the app. Therefore, in Fig. 4, we propose an icon (in the lower right corner) to provide more information regarding the current privacy policy whenever the user needs to access it, in every display.

Permissions customization: According with our research, permissions should be visible and users should be allowed to edit them (Line 6 in Table I). The blue icon (Fig. 4 - top right corner) is presented in all displays and allows the user to turn on or turn off the permissions according with her/his preferences. Each permission should also have the option "+info" which is linkable to complementary information.

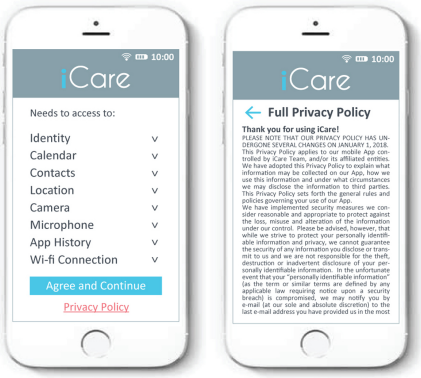

Fig. 1. Common description of privacy policies provided by apps during the installation (Line 1 in Table I).

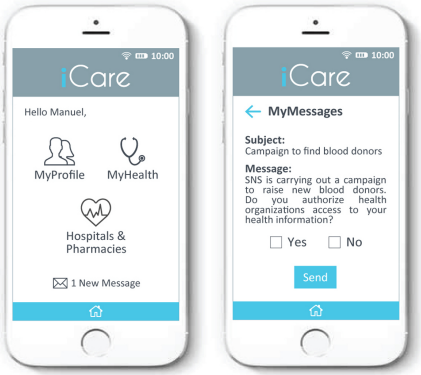

Fig. 3. In this scenario there is not enough information to support an informed answer and the user gives consent of personal data processing just for one purpose, once, but that data can be used for various purposes (Lines 2 and 3 in Table I).

Sensitive data / Biometric data: It is also relevant to notice that biometric data is one of the elements of the extended group of special data categories defined by the new regulation [1]. Attention should be paid when developing an app, specifically the authentication feature, as using biometrics as part of the multi-factor authentication may not be possible in most cases or require special permissions from local data protection authorities. This can be even more complicated if the domain of the app is healthcare. In the use of special/sensitive information, graphics such as forms, colours and sounds can help draw user's attention and raise his/her awareness. The consent to use special data is always required by the patient or acquired in specific authorized situations, as specified in the GDPR (Fig. 4).

VI. Discussion

The advances in mHealth technology and the adoption of medical apps are an important part of the daily medical practice but in some situations, the type of interaction between the user and the system can present a significant risk to the privacy and security of users and the protection of their health data. Sensitive data can be shared through mHealth apps between patients, physicians, family members and researchers but may also be shared with third parties, such as marketing companies and advertisers.

The work presented in this paper helps follow some of the new GDPR requirements in clear/simple steps.

Fig. 2. An app must have clear information regarding collected data and how these are protected, as per GDPR (Line 1 in Table I). Users must give consent for each one of the options regarding sensitive data from what GDPR considers being a special category (right), (Lines 2 and 8 in Table I).

Fig. 4. The user has more information regarding data collection and s/he has the right to specify which organizations can also have access to the data. (Lines 2 and 3 in Table I).

Mobile apps need to comply with all the new security and privacy rules, but being so many can make this hard to achieve and control. The synthesis presented in this paper (Table I) is a succinct but complete guide which reflects the main key changes that apps must integrate to securely

interact with users. Those guidelines are extracted directly from the text legislation and are ready to be applied in practice. To test this concept, several scenarios were designed to verify the impact of the changes into a specific, but fictitious, mHealth app (iCare). To better compare those changes, screenshots show iCare in the selected situations, with previous legislation and with GDPR requirements.

In more detail, the visual impact and amount of information that can be taken from Figs. 1 and 2 are completely different. In Fig. 2, information is more complete and available, easy to understand and grasp, within the same screen size. Special attention is given to special categories of data as they are considered high sensitive data. In the specific situation of an mHealth app, healthcare data will surely be collected and processed. Therefore, this needs to be considered separately from the other user's personal data because health data belongs to a special sensitive data categorisation introduced by GDPR. Due to this criticality, Fig. 2 shows what needs to happen to clearly alert the user about this fact and to ask explicit consent, specifically in this case. Icons are used to simply state the type of information that is going to be collected and, similarly to other examples, the user can select which types of his/her data can be used.

A different scenario is described in Figs. 3 (before) and 4 (after). In this case, in the after version, the user needs to read and process more displays to perform an informed decision. However, the rendered information is important and clear with the goal to make the user more informed and therefore more inclined to trust in the way their data is protected and used. So users will probably be more engaged to participate in similar campaigns, which can have a serious impact on public health. Again, the use of icons is very helpful in conveying the necessary messages in small spaces. Obviously, all used icons are not intended to be final or the ones that should be used in similar situations. They are just examples that can be used as a base to be adapted to specific app needs. Similar scenarios can be studied and defined for the other situations presented in Table I, which are not presented due to space constraints.

In summary, the presented work can be used as a guideline with recommendations to comply with GDPR and moreover improve the interactions user/mobile and ensuring the safety of patients, physicians and healthcare data.

Limitations. The authors could not find research about the impact of the new GDPR on the development of mHealth apps as well as guidelines for implementation and use. Thus, concrete examples are not available to be compared and discussed as well as easily adapted to the app at hand. This work presents such examples with those goals. However, the presented scenarios were not yet tested but will be in the future. Further, those scenarios may not be directly adaptable to languages other than English and there was still no consideration regarding accessibility issues, which also needs to be implemented and tested.

VII. Conclusions

Organizations have to be prepared to comply with GDPR now, to avoid heavy consequences. So they must refer to existing research and developments to be able to adapt to the new reality in the short run. This paper presents a study of different methods that can be used to improve security and privacy in mHealth apps and what measures can be available when applying GDPR in practice. Thus, this work is a necessary step to start dealing with required legal transformations. Future work comprises the development and test of proposed methods and features within real mHealth scenarios, with real users.

Acknowledgments

This article was supported by FCT through the Project TagUBig - Taming Your Big Data (IF/00693/2015) from Researcher FCT Program funded by National Funds through FCT - Fundação para a Ciência e a Tecnologia.

References

[1] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council L 119," Official Journal of the European Union, 2016.

[2] A. Cavoukian, "Privacy by design: the 7 foundational principles," 2009.

[3] GDPR. (2017, 06/11/2017). GDPR key changes. Available: https://www.eugdpr.org/the-regulation.html

[4] J. Mirkovic, H. Bryhni, and C. M. Ruland, "Secure solution for mobile access to patient's health care record," in 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, 2011, pp. 296-303.

[5] C. L. Ventola, "Mobile devices and apps for health care professionals: uses and benefits," Pharmacy and Therapeutics, 2014.

[6] EUR-Lex, "Directive 95/46/EC of the European Parliament and of the Council," Official Journal L 281, 23/11/1995 P. 0031 - 0050, 1995.

[7] R. J. T. R. Pires, "mHealth: o impacto da nova diretiva Europeia de proteção de dados, caso de uso e avaliação," Mestrado em informática médica, FCUP - University of Porto, 2016.

[8] CNPD. (2017, 08/01/2018). 10 Medidas para preparar a aplicação do regulamento europeu de proteção de dados. Available: https://www.cnpd.pt/bin/rgpd/10_Medidas_para_preparar_RGPD_CNPD.pdf

[9] M. Plachkinova, S. Andrés, and S. Chatterjee, "A taxonomy of mHealth apps - security and privacy concerns," presented at the 2015 48th Hawaii International Conference on System Sciences, 5-8 Jan. 2015, 2015. Available: http://ieeexplore.ieee.org/ielx7/7068092/7069647/07070200.pdf?tp=&arnumber=7070200&isnumber=7069647

[10] D. D. Luxton, R. A. McCann, N. E. Bush, M. C. Mishkind, and G. M. Reger, "mHealth for mental health: Integrating smartphone technology in behavioral healthcare," Professional Psychology: Research and Practice, vol. 42, no. 6, pp. 505-512, 2011.

[11] A. Ferreira, G. Lenzini, C. Santos-Pereira, A. B. Augusto, and M. E. Correia, "Envisioning secure and usable access control for patients," presented at the 2014 IEEE 3nd International Conference on Serious Games and Applications for Health (SeGAH), 2014. Available: http://ieeexplore.ieee.org/ielx7/7063805/7067066/07067093.pdf?tp=&arnumber=7067093&isnumber=7067066

[12] C. Pyper, J. Amery, M. Watson, and C. Crook, "Access to electronic health records in primary care-a survey of patients' views," Med Sci Monit, vol. 10, no. 11, pp. Sr17-22, Nov 2004.

[13] EDPS, "Guidelines on the protection of personal data processed by mobile applications," 2016.

[14] OAIC, "Mobile privacy: a better practice guide for mobile app developers," 2014.

[15] M. Sheppard, "Smartphone apps, permissions and privacy - concerns and next steps," Tekdesk: a division of the community opportunity and innovation network, 2013.