From principles to practice: benchmarking government guidance on health apps

Patient-facing mobile health applications (apps) hold the promise to change the way individuals take responsibility for their own health by enabling more effective delivery of health information, allowing better monitoring of symptoms, and encouraging healthier lifestyles. Enthusiasm about the potential of health apps has grown rapidly, generating uncertainty as to who should regulate such apps and how. In most countries, medical device regulation applies only to a subset of high-risk health apps that have well defined medical purposes. However, most health apps available on the market target a wide range of health-related issues, including diet and exercise, pregnancy, and mental health, while still being considered non-medical devices. These apps can collect a variety of personal data and, because they are designed to affect health, it is important to ensure their safety, validity, reliability, privacy, and security. Many low-quality health apps exist that, as well as providing advice that is incomplete, misleading, or wrong, might also fall short of meeting the expected standards in privacy and security. In a 2017 report, the Organisation for Economic Co-Operation and Development (OECD) concluded that the use of low-quality, non-medical health apps raises a wide range of ethical, legal, and governance issues, and pointed to the need for international agreement on minimum standards in quality assurance controls.

We examined guidance for the development of safe, secure, and reliable apps issued by data protection authorities in nine OECD countries (see appendix for methodological details). All these authorities had reported guidance relating to mobile apps in response to the 2017 Census of the International Conference on Data Protection and Privacy Commissioners. We also examined guidance by national health authorities in the same nine countries, and international guidance issued by WHO and the European Commission (EC). We did a comparative assessment of the guidance against the qualitative indicators and the principles and best practices set out in the 2013 OECD Privacy Guidelines and the 2016 OECD Recommendation on Health Data Governance (appendix).

The documents issued by data protection authorities are largely similar to one another. Most address app developers, providing information in question format or checklists, and are easily accessible online. All the documents from data protection authorities focus mainly on privacy and data protection, and include the core principles of the two OECD recommendations. These documents aim to clarify how to comply with relevant national legislation for app development in general, but not specifically for non-medical health apps.

Among the documents from data protection authorities, the extent to which explanatory and operational guidance is included varies. Although most documents cover rules on user data (eg, guidance on user’s consent, right to access their data, and data portability), only four documents address privacy impact assessment. The documents also included few specifications concerning third party access and use of data. In particular, the documents did not contain advice on good practice to adopt when data is used for marketing and in-app advertising. Furthermore, few documents discuss good practice on apps for children or disabled people.

We also searched the websites of the national health authorities in the same nine countries for specific guidance, and contacted their respective OECD representatives for confirmation (appendix). Most European ministries and the Australian department of health confirmed that their countries had not developed specific guidance. Guidance might have been produced at a territory level or by professional organisations, but reviewing such documents was not in the scope of this report. Only two national health authorities have issued specific guidance: the UK National Health Service (NHS) and the French Haute Autorité de Santé (HAS). The types of guidance delivered by these authorities differ substantially. HAS good practice guidelines are aimed at app developers and evaluators (evaluating bodies, consumer associations, or medical professional organisations), and the guidance is based on five categories of good practice requirements: informing users, health

See Online for appendix
Comment

content, technical content, security and reliability, and usability. The guidance includes a risk matrix to help tailor and assess good practice according to the app’s intended uses. In the UK, the NHS has developed a review process for the selection of non-medical apps to be included in the NHS app library. The review process is based on an online questionnaire listing good practice goals in eight core areas: clinical effectiveness, regulatory approval, clinical safety, data protection, security, usability and accessibility, interoperability, and technical stability.

At the EU level, in 2016, the EC issued the draft Privacy Code of Conduct on health apps for public consultation. This document includes most of the criteria listed by the UK and French health authorities, in addition to specific and practical guidance on privacy and data protection principles to be taken into account by health app developers. At international level, the mHealth Evidence Reporting Assessment, developed by the WHO Technical Evidence Review Group in 2016, also includes most of the criteria listed by the NHS and HAS, with a focus on assessment of an app’s technical features, rather than non-technical aspects such as clinical safety and privacy.

In summary, although governments are developing regulation and guidance for app developers, our report shows that this guidance is siloed and not comprehensive. Data protection authorities are focused on privacy and data protection issues, whereas health authorities introduce safety and efficacy considerations. The spread of different sources of guidance across agencies leaves it up to developers to navigate the complex regulatory environment. As apps are often global products, multiple guidelines and different agencies and requirements make compliance onerous and accountability measures unclear. Although our analysis cannot directly link this fragmented landscape with the poor quality standards of non-medical health apps that has been documented, fragmentation and lack of comprehensive guidance is probably not conducive to effective governance.

Professional organisations, academics, and the private sector have stepped in to provide additional guidance. For example, guidelines have been produced by Xcertia to support consumers and clinicians in choosing mobile health apps, and to help developers in complying with industry-wide accepted standards. The British Publicly Available Specification 277 (health and wellness apps—quality criteria across the life cycle) provides a wide variety of specifications on health apps, including topics such as fitness for purpose, risk management, quality criteria, and support. Additionally, medical associations, such as the Royal Dutch Medical Association,7 have provided sector-specific guidance and standards to evaluate effectiveness and safety of health apps. At the national level in the USA, the Agency for Healthcare Research and Quality issued an evaluation of the efficacy, usability, and features of commercially available apps for diabetes self-management in 2018.8 In the UK, the NHS, in collaboration with the National Institute for Health and Care Excellence, has issued an evidence standards framework. Finally, although standardised voluntary self-certification or star rating tools could help consumers and clinicians to reach informed decisions regarding app use, these tools rely on developers’ accountability and competence and have yet to be proven reliable.9

Greater policy coordination for the governance of health apps is needed to reduce guidance gaps (eg, on data access and user autonomy), to make quality standards visible and clear, and to create an accessible common reference for developers, users, and payors. As countries move to develop strategies for greater patient-centred care, we must enable cross-country agreement on minimum quality assurance standards to guide app development and use. An OECD-led multi-stakeholder initiative, building on OECD’s ongoing work on health data governance, would be a crucial step towards global consensus.

Agata Ferretti, Elettra Ronchi, *Effy Vayena

Health Ethics and Policy Lab, Department of Health Sciences and Technology, Swiss Federal Institute of Technology, Zürich 8092, Switzerland (AF,EV); and Organisation for Economic Co-Operation and Development (OECD), Paris, France (ER)
effy.vayena@hest.ethz.ch

We declare no competing interests. AF is supported by the Swiss National Science Foundation (grant number 407440_167223; NRP 75 Big Data). ER is a Senior Policy Analyst for the Organisation for Economic Co-operation and Development (OECD). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the OECD or of the governments of its member countries.

Copyright © 2019 The Author(s). Published by Elsevier Ltd. This is an Open Access article under the CC BY 4.0 license.

Comment