BMJ Health & Care Informatics

Why is it so difficult to govern mobile apps in healthcare?

Farah Magrabi ,[1] Ibrahim Habli ,[2] Mark Sujan ,[3] David Wong ,[4] Harold Thimbleby,[5] Maureen Baker,[6] Enrico Coiera [1]

To cite: Magrabi F, Habli I, Sujan M, *et al*. Why is it so difficult to govern mobile apps in healthcare? *BMJ Health Care Inform* 2019;**26**:e100006. doi:10.1136/bmjhci-2019-100006

Received 13 September 2019
Revised 28 October 2019
Accepted 05 November 2019

[1]Australian Institute of Health Innovation, Centre for Health Informatics, Macquarie University, Sydney, New South Wales, Australia
[2]Department of Computer Science, University of York, York, UK
[3]University of Warwick, Coventry, United Kingdom
[4]Centre for Health Informatics, University of Manchester, Manchester, United Kingdom
[5]Computer Science, University of Swansea, Swansea, United Kingdom
[6]Your.MD Ltd, London, UK

Correspondence to
A/Prof Farah Magrabi;
farah.magrabi@mq.edu.au

Mobile apps have become a convenient way to provide health information and communication services directly in the hands of clinicians and consumers. Apps can be used to support consumers in a variety of health tasks to manage chronic diseases, support lifestyle changes and in self-diagnosis. For clinicians, they can improve access to patient information and clinical decision support tools at the point-of-care. While the use of apps in healthcare can bring many benefits, poor quality information and gaps in software functionality can pose new risks to patient safety.[1] For example, an app to support women undergoing breast cancer surgery was found to increase postoperative anxiety and depression.[2] Another app providing an intervention to reduce distress and alcohol consumption was found to increase heavy drinking, anxiety and distress.[3]

At their core, apps are software that run on a mobile device. When it comes to developing software, and assuring its quality, safety and security, rigorous engineering is fundamental. By applying engineering processes, developers should ensure that software is designed to requirements with safety and security integrated into the design, including regulatory requirements; hazards can be systematically identified and mitigated, not only prior to and during deployment but through the life of the system by monitoring use and preventative maintenance.[4] However, these processes break down with mobile apps because they are a unique form of software that is easy to develop and deploy. For a small subset of health apps that are developed as a medical device or tethered to a device, engineering processes are preserved, in part, by regulatory requirements.[5] However, the vast majority of health apps fall outside the remit of effective regulations in most nations.

This commentary examines the problem of assuring, or establishing, justified confidence in the clinical quality, safety and security of health apps. The overall objective is to raise awareness about this often neglected topic, and to highlight the need for standards and oversight. We begin by considering the inherent complexity of formalising processes for designing apps, and then examine aspects of their development, implementation and use that pose challenges when it comes to laying down clinical governance which is the set of formal processes that dictates how patient safety is ensured.[4] We argue that there is fluidity in app function and design that presents a challenge to identify mature use cases necessary to develop a clear understanding of risk and expected performance. Probable causes are the low entry barrier to app creation and absence of certification barrier to distribution to the public. Thus, apps are ubiquitous, posing risks on a large-scale where traditional clinical governance approaches may be too slow.[6] We show that the disparate contexts in which apps are developed are not uniformly conducive to assurance processes. Risks are also increased because there is no central surveillance of the use of health apps.

APPS ARE HIGHLY VERSATILE

The versatility of apps means they can be used to support a wide variety of health information or communication services at all levels of care delivery and in the community. As apps can support a single service or a combination of services, their function may not be clear at the outset to designers. A fundamental problem here is that there is no standard use cases for apps of any type and therefore the implementation of information and communication services is ad hoc.[7] While NICE's guidelines for digital health technologies distinguish broad categories of functionality,[8] their implementation is left to developers. For instance, asthma management: the use case for what specific functions apps must support, including information provision, peak flow

and symptom diaries, and medication tracking, is fluid and currently evolving with developments in technology and medical research. While the functionality of apps, or any other software to support health services, should be based on clinical standards that provide evidence-based requirements for information and communication, the slow rate at which such standards are produced presents a challenge for clinical governance because without standardised use cases, apps are providing functionality where there is no clear understanding of risk.

The lack of standard use cases makes it difficult to lay down clear rules for clinical governance of apps. With current regulations for medical devices, there is only a subtle difference between apps which are considered medical devices and those that are not. For example, symptom checkers are considered to be a medical device if they provide a subset of medical conditions matching the symptoms entered by users, indicate the likelihood of a match, or provide treatment recommendations.[9] Yet, those that list *all* conditions matching the symptoms entered by users and provide signposts to suitable care are not considered medical devices.[9]

Apps also pose challenges for applying clinical governance processes because they are used at all levels of care delivery and in the community. For instance, consumer health information is the purview of public health where the reliability and credibility of information is a prime consideration. In contrast, prevention and management of disease involve formal care delivery settings often with treatment by health professionals. This raises complex issues in processes to assess and manage risk because across these contexts, there is no consensus about the level of acceptable safety among health service providers, clinicians and regulators.

ANYONE CAN BUILD AN APP

The sheer number of health apps and their ubiquity is a consequence of how easy it is to develop and publish them. It is estimated that there are over 325 000 health apps available in the leading app stores. Apps can be created using online platforms that automate development, distribution and maintenance; such platforms (eg, Appy Pie) do not require any software programming skills. While there are no data about the use of such platforms for health apps, in a recent study of 2.3 million apps on Google Play, 11% were created using such online platforms.[10] Both clinicians and developers with little or no formal software engineering background are, therefore, rapidly developing apps. Such an ad hoc approach to development means that developers are unaware of underlying safety and security issues that can ultimately pose serious risks to data security and privacy. The lack of accountability is a serious issue because qualified engineers are professionals who can be held accountable for their actions while this may not be the case for clinicians and citizen developers ('citizen developer' is a new term implying a mix of skill and informality, even naivety compared with professional practice).[8]

Another rapid method for development is via mobile application frameworks which provide many pre-made components that can be used as building blocks for most health information and communication functions (eg, Ionic and React Native). This hybrid approach to build apps does not require developers to have extensive coding expertise or software development skills compared with the process of building native apps. The availability of hybrid approaches has no doubt contributed to the growing numbers of health apps, but the quality is not guaranteed because these tools have opened up development to citizen developers, clinicians and professional developers with varying levels of software engineering expertise. Worse, these building blocks were not originally developed for clinical use.

DEVELOPMENT OCCURS IN DIVERSE SETTINGS

Because the entry barrier to app creation is low, they are being developed in formal and informal settings. The sociotechnical disparity of these contexts poses significant challenges when it comes to formalising processes for software development and clinical governance.[4] For large-scale health IT systems, software development is typically undertaken by an IT business entity. For an electronic medical records system that is developed by a large multinational company, the organisation provides a formal setting for software engineering processes to be undertaken. The company will have clinical and technical expertise, including a large and well-organised IT group as well as organisational structures, policies and procedures to govern the quality, safety and security of the software it produces.[11] An app developed in such business settings should be subject to the same rigorous engineering and clinical governance processes not just for regulatory reasons but also for reputation reasons. In contrast, smaller health IT businesses and new businesses, such as start-up companies, may not provide the infrastructure conducive to formal software engineering and clinical governance processes—and they typically have smaller budgets available for the development compared to a large business entity.

Another setting for app development is within healthcare organisations, including providers, government agencies and not-for-profit organisations. While these settings have deep clinical expertise, those without a large and well-organised IT group are unlikely to have technical expertise and established software engineering processes for building and maintaining apps in-house; they may rely on third-party developers which reduces accountability. Another issue with healthcare organisations is that their clinical governance structures and processes are generally not set up to provide oversight for apps. With citizen developers, the informal context means that formal software development and clinical governance processes may altogether be absent. Because of a lack of skills and

experience, citizen developers may be unaware of best-practice development methods and standards. Development may proceed without engaging users, apps may not be maintained and updated in a timely manner, quality control may be missing and postmarket surveillance is often omitted—and so on. These problems also occur in apps developed bottom-up by clinicians on their own. Many apps are unplanned and grow 'organically': some are by-products of local clinical system improvement projects (eg, handover or antibiotic prescribing apps). While a bottom-up approach is advantageous for innovation and clinical engagement, apps developed in this manner may not be sustainable beyond pilot testing. Clinicians worried about excessive bureaucracy may not engage with formal organisational processes for software development and clinical governance. Ironically, some apps start life through clinicians working around perceived problems with organisational policies and processes. Strategies to formalise app development, therefore, need to account for the diverse contexts where they are being developed. It is noteworthy that citizen development and marketing of pharmaceuticals is illegal.

NO GATE AT IMPLEMENTATION, LITTLE FORMAL EVALUATION AND NO MONITORING OF USE

As there are no formal processes to specifically govern the deployment of apps for health, they can be deployed easily and widely. When publishing via app stores, developers are provided with general guidelines for safety, privacy and performance. There are no requirements to comply with standards for software development and quality processes which are an important clinical governance strategy to ensure sound end products. A more fundamental problem is that there are no agreed standards for developing health apps,[12] and efforts are underway to collate all the current standards, frameworks, best practices and guidelines.[13] Where guidelines and standards exist, such as NICE's guidelines for digital health technologies, they are not specifically intended for apps that are downloaded or purchased directly by users.[8]

Despite apps having a global market, thanks to the Internet and app stores, there is no global regulator; regulatory requirements for software as a medical device are not uniform worldwide.[14] Take, for instance, a symptom checker that would be a class 1 medical device in the UK, but is not considered a medical device in Australia, and in the USA would not have regulations enforced by the Food and Drug Administration. Because developers are not required to demonstrate performance and show effectiveness, the quality of evaluation studies is poor,[8] and there is little attention to safety.[15] Current European medical device regulation (CE marking) presumes apps are clinically effective, and therefore pushes liabilities for use errors, even if caused by software bugs, onto end users. Again, this contrasts with pharmaceutical development, which includes registering experiments and a mature peer-reviewed publication culture.

Once apps are downloaded, their postmarket use goes largely unchecked, and even those apps that report use data have no awareness of the wider clinical condition or outcome. While agencies and institutions may monitor their apps as part of their internal clinical governance processes, there is no ongoing surveillance and oversight of apps that are published by citizen developers (nor are citizen developers resourced to provide postmarket support to users—note that successful apps can have millions of users across all time zones). App stores might remove apps in response to user feedback; however, studies show that ratings are not correlated with quality or safety, and therefore, user feedback is not relevant.[16 17]

APPS DIRECTLY REACH USERS

Apps that are accessed by consumers and patients outside formal care delivery increase risks because they can be used to make decisions without having to consult health professionals. Compared to a clinician who is a learned intermediary, when using a software system apps are a direct-to-consumer channel for health information and services that increases clinical risk and is vulnerable to data exploitation (eg, sharing patient data).[18] Consumers and patients who use apps are a heterogenous user base with varying levels of health literacy and IT skills. Users lack the ability to search for and appraise the quality and trustworthiness of apps and their content.[19] They may not have the skills to use an app in the manner that was intended by the designers. Their understanding, skills and physical state (especially given they are likely to be ill) may also affect their ability to detect, manage and report errors. Software updates are another responsibility for users but developers have no control over whether or not users instal updates: therefore, bug fixes and security updates might not be installed. There could be many different versions of an app in use, making it difficult to manage risks. While strategies to assist users in selecting and using apps, such as grading labels, may go some way towards reducing risks,[20] the types of apps that are made available directly to consumers needs to be controlled.

DISCUSSION

Health apps are perhaps the most extreme example of challenges for clinical governance in the digital health ecosystem. While current efforts are usefully directed at curating the growing numbers of apps,[20] they are not sustainable. A parallel strategy could focus on the preceding stages of the IT system life cycle to stem the growing tide of apps, by controlling their design, build and distribution.

As with any other digital technology, we need to consider apps from a problem-driven perspective by the health information or communication service they support. For example, consumer health information services should be based on standards for clinical content irrespective of whether they are delivered on web sites or

via apps. Similarly, information and communication for patient self-monitoring in asthma should be clinically driven, based on standards where they exist or best practice guidelines. Requirements relating to the channel of service delivery can be separately addressed via technical standards that are channel-specific. For instance, privacy and data security considerations need to be channel-specific because apps have more direct access to personal information compared to websites. Other channel-specific aspects that need to be covered via technical standards are usability, availability, interoperability and maintenance, including updates. Such an approach is being considered for digital mental health services in Australia and could be applied to other health domains.[21] A major advantage of this approach is that it does not consider apps in isolation but in context of the health services they support or the community. Ultimately, this might become a necessary way forward as we move to the omnichannel age where there will be seamless delivery of health information and communication across different channels.[22] For instance, symptom checkers can be downloaded as apps or accessed on the web; a symptom checker service may be operated alongside a telephone helpline and a health information service.

Clinical and technical standards will provide a common framework for managing risks throughout the IT system life cycle and for operational oversight whether it is via developers self-certifying themselves, independent certification or regulation as medical devices. One possible avenue for common standards is via initiatives like the WHO and ITU processes for benchmarking artificial intelligence in health.[23] Common evaluation standards underpin an evidence-based approach to digital health,[24] and are necessary as each level of oversight can provide a foundation for the next.[25] With symptom checkers, self-certification by developers can form the basis of safety cases presented to regulators. The implementation and use of such apps in formal care delivery settings needs to be driven by appropriate guidelines and standards,[11 26] and operational oversight should be provided by organisational processes for clinical governance.[11] For example, a symptom checker operated by a public health information service should be subject to internal clinical governance processes of the government agency operating the service.

The level of oversight needs to be proportional to the degree of risks that apps pose to users. An evidence-based approach that is informed by the current landscape of health apps is required. At present, there is no publicly available information about the number and types of health apps, who developed them, how they were developed and for how long have they been available, let alone the risks they incur. If the majority of low-risk health and wellness apps are being developed by credible health organisations and government agencies, then self-certification could be a viable option. These mechanisms for oversight will need to be examined alongside regulations for software as a medical device. Operational oversight and surveillance can also be considered at a national and regional level using common frameworks so that it is possible to compare patterns over time and between settings, and to develop and prioritise preventive and corrective strategies.[27]

Our key conclusion is that the area of health apps is immature; this is unsurprising as apps are a radical and new development, which relies on sophisticated technology that has a record of frequent innovation. Patients, clinicians, developers and regulators are inevitably beholden to this current immaturity. Unlike established healthcare fields (eg, pharmaceuticals, radiotherapy, anaesthetics, etc) there is—as yet—no professional foundation, such as requiring certified and registered developers. Once there is a professional foundation, we envisage professional developers moving to regulation, just as registered pharmacists move into pharma regulation—this is a slow process, but without it, regulation is likely to remain behind the curve. The role of citizen developers in this ecosystem needs to be carefully considered. Given IT's record of continual radical innovation, regulatory lag is likely to be permanent, and therefore, an effective clinical governance response must be, or partly be, of a different sort than conventional regulation. This paper has set out some of the issues that must be addressed. Ultimately, apps should not be considered just by their form but by their function and as part of the digital health ecosystem.

Twitter Farah Magrabi @farahmagrabi, Ibrahim Habli @IHabli, Mark Sujan @MarkSujan, David Wong @drdavecwong, Harold Thimbleby @haroldthimbleby, Maureen Baker @Maureenprsb and Enrico Coiera @EnricoCoiera

Contributors FM and EC conceptualised the study. All the authors participated in writing and revising the paper. All the aspects of the study were led by the authors.

Funding FM and EC are supported by the Australian National Health and Medical Research Council Centre for Research Excellence in Digital Health, grant number 1134919. FM holds a fellowship with the Assuring Autonomy International Programme at the University of York. IH is partially supported by the project 'Wearable Clinic: Connecting Health, Self and Care' (EP/P010148/1), funded by the UK Engineering and Physical Sciences Research Council. MS is supported by a research grant from the Lloyd's Register Foundation and a fellowship with the Assuring Autonomy International Programme at the University of York. HT is funded by the See Change (R&MA-P, Scotland).

Competing interests MB is the Chief Medical Officer at Your.MD, and DW consults for Sensyne Health.

Patient consent for publication Not required.

Provenance and peer review Commissioned; externally peer reviewed.

ORCID iDs
Farah Magrabi https://orcid.org/0000-0002-8426-5588
Ibrahim Habli https://orcid.org/0000-0003-2736-8238
Mark Sujan http://orcid.org/0000-0001-6895-946X
David Wong https://orcid.org/0000-0001-8117-9193
Enrico Coiera https://orcid.org/0000-0002-6444-6584

REFERENCES

1 Akbar S, Coiera E, Magrabi F. Safety concerns with consumer-facing mobile health applications and their consequences: a scoping review. *J Am Med Inform Assoc* 2019;41:ocz175.
2 Foley NM, O'Connell EP, Lehane EA, *et al*. PATI: patient accessed tailored information: a pilot study to evaluate the effect on preoperative breast cancer patients of information delivered via a mobile application. *Breast* 2016;30:54–8.
3 Hamamura T, Suganuma S, Ueda M, *et al*. Standalone effects of a cognitive behavioral intervention using a mobile phone APP on psychological distress and alcohol consumption among Japanese workers: pilot nonrandomized controlled trial. *JMIR Ment Health* 2018;5:e24.
4 Coiera E, Magrabi F. *Information system safety. guide to health informatics*. Boca Raton, FL, USA: CRC Press, Taylor & Francis Group, 2015: 195–220.
5 International Organization for Standardization - Medical Devices. *Application of risk management to medical devices (en iso 14971:2007*. Geneva, 2007.
6 Coiera E, Aarts J, Kulikowski C. The dangerous decade. *J Am Med Inform Assoc* 2012;19:2–5.
7 Huckvale K, Morrison C, Ouyang J, *et al*. The evolution of mobile apps for asthma: an updated systematic assessment of content and tools. *BMC Med* 2015;13:58.
8 National Institute for Health and Care Excellence,. Evidence standards framework for digital health technologies, 2019. Available: https://www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies
9 UK Medicines and Healthcare products Regulatory Agency. Guidance for medical devices: software applications (apps). Available: https://www.gov.uk/government/publications/medical-devices-software-applications-apps [Accessed 6 Aug 2019].
10 Oltrogge M, Derr E, Stransky C, *et al*. The rise of the citizen developer: assessing the security impact of online app generators. *IEEE Symposium on Security and Privacy (SP)*, 2018:634–47.
11 Sittig DF, Ash JS, Singh H. The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records. *Am J Manag Care* 2014;20:418–23.
12 Torous J, Andersson G, Bertagnoli A, *et al*. Towards a consensus around standards for smartphone apps and digital mental health. *World Psychiatry* 2019;18:97–8.
13 Van Velthoven MH, Smith J, Wells G, *et al*. Digital health APP development standards: a systematic review protocol. *BMJ Open* 2018;8:e022969.
14 Ferretti A, Ronchi E, Vayena E. From principles to practice: benchmarking government guidance on health apps. *Lancet Digit Health* 2019;1:e55–7.
15 Stevens WJM, van der Sande R, Beijer LJ, *et al*. eHealth Apps replacing or complementing health care contacts: Scoping review on adverse effects. *J Med Internet Res* 2019;21:e10736.10.2196/10736
16 Plante TB, O'Kelly AC, Macfarlane ZT, *et al*. Trends in user ratings and reviews of a popular yet inaccurate blood pressure-measuring smartphone APP. *J Am Med Inform Assoc* 2018;25:1074–9.
17 Carlo AD, Hosseini Ghomi R, Renn BN, *et al*. By the numbers: ratings and utilization of behavioral health mobile applications. *NPJ Digit Med* 2019;2.
18 Grundy Q, Chiu K, Held F, *et al*. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ* 2019;22:l920.
19 Henson P, David G, Albright K, *et al*. Deriving a practical framework for the evaluation of health apps. *Lancet Digit Health* 2019;1:e52–4.
20 Bates DW, Landman A, Levine DM, *et al*. Health Apps and health policy: what is needed? *JAMA* 2018;320:1975–6.
21 Australian Commission on Safety and Quality in Health Care. Certification framework and national standards for digital mental health services, 2019. Available: https://www.safetyandquality.gov.au/our-work/e-health-safety/national-safety-and-quality-standards-digital-mental-health-services [Accessed 23 Oct 2019].
22 Aabel B, Abeywarna D. Digital cross-channel usability heuristics: improving the digital health experience. *J Usability Studies* 2018;13:52–72.
23 Wiegand T, Krishnamurthy R, Kuglitsch M, *et al*. Who and ITU establish benchmarking process for artificial intelligence in health. *Lancet* 2019;394:9–11.
24 Ammenwerth E, Rigby M. *Evidence-Based health informatics: promoting safety and efficiency through scientific methods and ethical policy*. IOS Press, 2016.
25 Runciman WB, Williamson JAH, Deakin A, *et al*. An integrated framework for safety, quality and risk management: an information and incident management system based on a universal patient safety classification. *Qual Saf Health Care* 2006;15 Suppl 1:i82–90.
26 ISB 0160 clinical risk management: its application in the deployment and use of health it systems. Available: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb0160-clinical-risk-management-its-application-in-the-deployment-and-use-of-health-it-systems [Accessed 6 Aug 2019].
27 International Organization for Standardization. *Health informatics — framework of event data and reporting definitions for the safety of health software (ISO/TS 20405:2018)*. Geneva, 2018.