spectra

121

mHealth issue

2 mHealth and its benefits to health

Smartphones have given extra impetus to the megatrend that is digitalisation. According to the Federal Statistical Office, 72 per cent of people living in Switzerland used the Internet while on the move in 2017, and 98 per cent of them did so from a mobile phone. In line with this trend, the number of mobile apps for health and fitness has skyrocketed in recent years. This issue sets out to highlight the resulting developments, opportunities and challenges.

3 Health-specific data and ensuring they are protected

Health data are a valuable commodity. This makes it all the more important to address the question of what happens to the health data that are measured and tracked by apps and mobile devices. One of the things we find out in the interview with data protection expert Barbara Widmer is how users can protect their data more effectively.

4 Health equity and mHealth

The question of who benefits from technological achievements is one that is constantly cropping up. One of the areas it has been applied to is digital media. The gap that exists between the people who are able to use new digital services to expand their knowledge and those who cannot benefit from such progress is known as the "digital divide". This article shows how this divide can be minimised with reference to mHealth apps.

mHealth – what opportunities are there for mobile apps in the healthcar

Digital change is having a profound impact on our everyday life. The smartphone is further accelerating this process. It is a constant and ubiquitous presence, and is being increasingly used in prevention and health promotion (to measure fitness and health data) as well as in everyday medical practice (measurement of vital data, coordination and disease management). Compared with other economic sectors, however, the use of apps in the medical field has some catching up to do, not least because of the more stringent requirements regarding security and protection of health-specific data. We have sought to provide you below with an insight into the possible uses of mobile health and the challenges it faces.
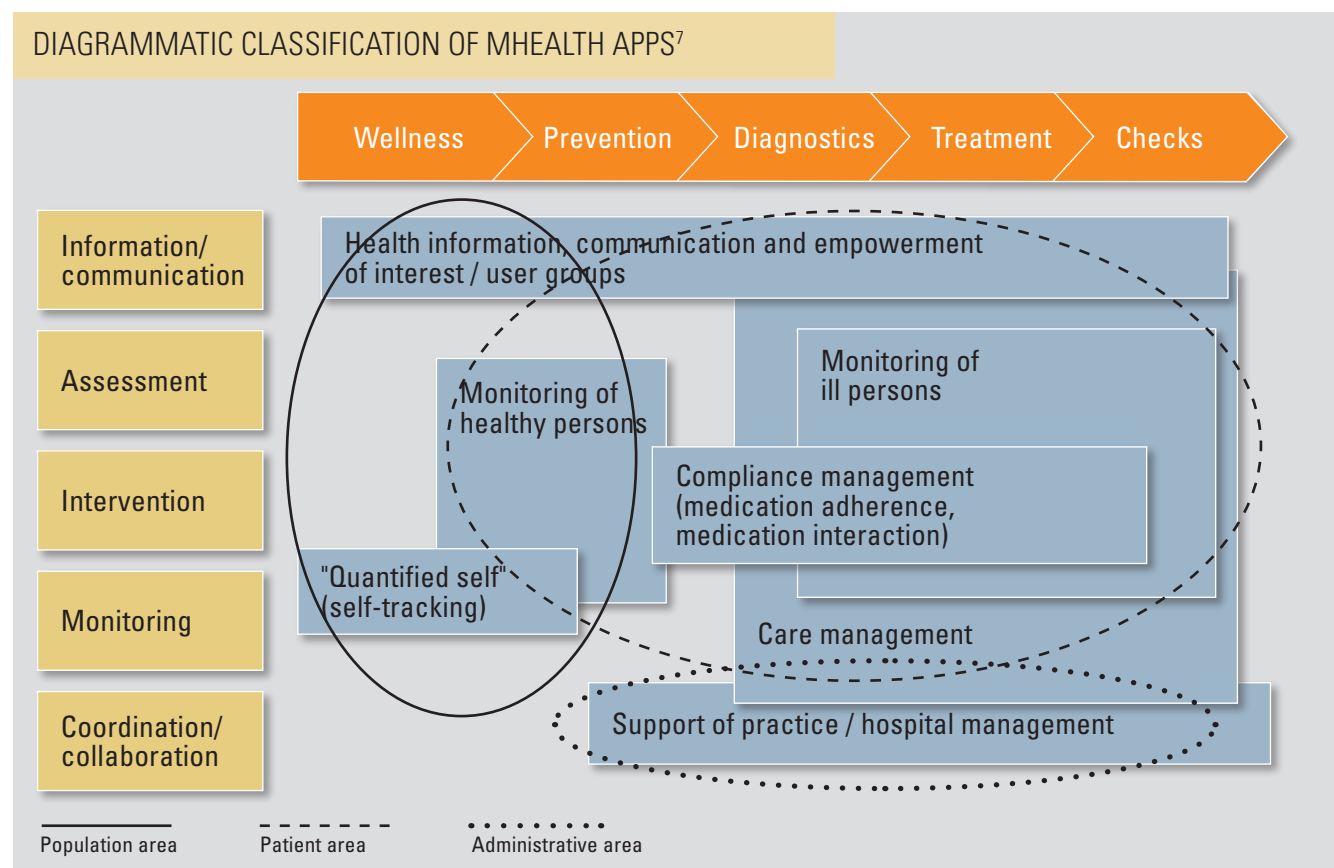
In the framework of the "Swiss eHealth Strategy 2.0", eHealth Suisse – the coordination body of the Federal Government and cantons – was mandated with the task of supporting the introduction of the electronic patient dossier (EPD)[1]. In 2017 it issued initial recommendations on the use of mHealth apps.[2] One vision of the "eHealth Strategy 2.0" is that the population of Switzerland is digitally literate and makes optimum use of the potential of new technologies for its health. A further vision is that healthcare facilities and health professionals are digitally networked to such an extent that they can exchange information electronically along the entire chain of care and make repeated use of recorded data.[3]

This means that patients in future can not only access their EPD but can also add data and documents to it, including any that stem from mHealth applications (apps). This would enable diagnoses to be made more rapidly and/or treatment to be supported by appropriate apps. For example, at the Inselspital Bern (Berne University Hospital) a bariatric app is used to support follow-up treatment after gastric bypass surgery. In general, however, there is still a lack of binding standards governing the exchangeability of information between mHealth apps (in the example cited here, between patient and service provider).

mHealth as part of eHealth
mHealth (mobile health) is a component of eHealth[4]. Based on the WHO definition, mHealth is designated as "medical procedures and measures of private and public healthcare that are supported by mobile devices such as mobile phones, patient monitoring devices, personal digital assistants (PDA) and other wireless devices".[5]

New technical options are no substitute for medical treatment
Besides the above example, mHealth apps are used in routine medical practice to measure vital parameters such as pulse, blood sugar, blood pressure, body temperature or cerebral activity or to remind patients to take their medicines or that they have an imminent doctor's appointment. mHealth apps can also be used to communicate fitness and dietary recommendations. The fact that more and more people own a smartphone means that mHealth is opening up a whole new range of healthcare functionalities to service providers. However, mobile healthcare apps are never a substitute for treatment by a doctor or for patient-doctor communication, though they can facilitate both of these.

Mobile healthcare apps are never a substitute for treatment by a doctor or for patient-doctor communication, though they can facilitate both of these.

The practical examples discussed in this issue are designed to provide an insight into current developments and the possible benefits for users, patients and health professionals. It remains to be seen whether mHealth can also help reduce costs.[6] Evidence and therefore sound results that enable mHealth to be recommended and used without reservations are still also lacking in many areas. Particular consideration is called for when it comes to using mHealth apps in "digital immigrants", i.e. older people or other disadvantaged groups (see the contribution on equality of opportunity on page 4). They, too, should be able to use digital technologies, and therefore they must be given an opportunity to acquire the necessary skills.

"Health 2020" and digital technologies
The Federal Government's "Health 2020" strategy calls for the use of digital technologies which will support the treatment process and help improve primary healthcare for the Swiss population. Besides launching the EPD, the Federal Government envisages measures to support developers of mHealth apps and achieve greater transparency for users with regard to data protection and data security of such apps. The stated aims of the strategy are to improve the quality and efficiency of healthcare and to ensure a better exchange of information and more efficient healthcare processes.

mHealth as a medical device
In Switzerland, whether or not an mHealth application qualifies as a medical device (i.e. as 'medical device standalone software' or as a 'mobile medical application'/app) is determined by the Medical Devices Ordinance (MedDO, SR 812.213), which is derived from the European Medical Devices Directive (93/42/EEC), and from EU guidance document MEDDEV 2.1/6. Swissmedic has published an information sheet on Standalone Medical Device Software containing further details (see bit.ly/2MPGfbA). In order to be marketed in Switzerland, the EEA states and Turkey, medical devices do not have to be officially authorised as is the case for medicinal products; instead they must have successfully completed the relevant conformity assessment procedure (certificate and/or EC conformity declaration). Medical devices placed on the market must also bear the CE marking. Data accuracy is an important aspect of the use of health-specific data. If the data are not reliable, they are more likely to jeopardise the health of users than to promote it. Research, too, is dependent on reliable data. A welcome development would therefore be the introduction of a form of certification or of quality labels, also for health and fitness apps, that would increase confidence in them among medical professionals as well as among users.

Data protection and security versus entrepreneurial freedom
Already at a legal level, health data are an asset that is particularly worthy of protection. There can therefore be no question of pitting this asset against the objections of industry, which regards such protection as a restriction on its entrepreneurial freedom. Yet we need to find joint solutions that do not allow overregulation to excessively limit the scope for using mHealth to the benefit of the healthcare system. Only then can products be marketed that are reliable and trustworthy enough to be used for healthcare purposes and comply with ethical and data protection law standards. Manufacturers would then find that building up a stake in this market pays off. But measures also need to be taken to prevent, say, insurance companies or employers from making illegal use of, or selling on, the health data of their insured customers or their employees. There is still a lot to be done in this respect as well (see also the interview with data protection expert Barbara Widmer on pp. 3–4).

Personal security for users of mHealth
mHealth app users should already be observing minimum security precau-

DIAGRAMMATIC CLASSIFICATION OF MHEALTH APPS[7]

Wellness | Prevention | Diagnostics | Treatment | Checks

Information/communication
Assessment
Intervention
Monitoring
Coordination/collaboration

Health information, communication and empowerment of interest / user groups

Monitoring of healthy persons
Monitoring of ill persons
Compliance management (medication adherence, medication interaction)
"Quantified self" (self-tracking)
Care management
Support of practice / hospital management

Population area — Patient area - - - - Administrative area ·········

mHealth applications are used along the entire chain of care.

re system?

tions with regard to their apps. They should, for instance, never use their Twitter or Facebook user data to register with (mHealth) apps. In turn, app producers should state which data they store, and where, and should offer transparent opt-in and opt-out choices that enable the actual users to decide which data they wish to release. In this connection, the providers' general terms & conditions prevent users from determining for themselves what they want done with their data. The terms & conditions are usually so long that nobody actually reads them. Users nevertheless have to agree to them if they want access to the app.

Digital technologies will play an increasingly important role in healthcare. Their success in the medium to long term will,

on the one hand, largely depend on the achievement of a degree of expertise and hence a healthy critical relationship with mHealth apps on the part of users and healthcare providers. On the other, it will need developers, producers, experts and specialists to join forces and resolve the challenges in respect of data security, protection and reliability while taking ethical standards into account. If these minimum requirements are met, there will be no need for strict regulations that could be challenged as being a "brake on innovation".

Contact:
Stefan Spycher,
Health Policy Directorate,
stefan.spycher@bag.admin.ch

1 eHealth Suisse: Strategie eHealth Schweiz 2.0 2018–2022, dated 1.3.2018.
2 eHealth Suisse: mobile Health. mHealth, Empfehlungen I, dated 16.3.2017.
3 Strategie eHealth Schweiz 2.0 2018-2022, 1.3.2018, p. 4.
4 "eHealth (or electronic healthcare services) is understood as the integrated use of information and communication technology to design, support and network all processes and stakeholders in the healthcare system". www.e-health-suisse.ch, [status: 13.4.2018].
5 From the study by the University of Applied Sciences, St. Gallen: mHealth im Kontext des elektr. Patientendossiers, Eine Studie im Auftrag von eHealth Suisse, p. VIII; WHO World Health Organization, in: mHealth. New Horizons for Health Through Mobile Technologies, Geneva, 2011, p. 6.
6 A study by A. T. Kearney from 2013 assumes "an improvement in patient treatment and safety" and "sustained cost reductions for the healthcare system from using the available technical infrastructure such as smartphones", in: A. T. Kearney (2013): Mobile Health: Fata Morgana oder Wachstumstreiber?, p. 4.
7 Source: Study by A.T. Kearney, see in: eHealth Suisse: mobile Health. mHealth, Empfehlungen I, dated 16.3.2017, p. 5

"The people affected are too little aware of current data protection rules."

Interview with Barbara Widmer. Our health data are particularly sensitive, yet today everyone and everything is tracked. Can we still protect the data that mHealth apps acquire from us and store? In our discussion, the lawyer and expert on data protection issues tells us where the greatest data protection risks lie with mHealth apps and what we can still do to make our data more secure.

spectra: mHealth apps collect health data. Why are these data particularly sensitive?

Barbara Widmer: Because of the inherent risk of breaching someone's privacy, say by accidentally disclosing a prejudicial medical diagnosis. A lot of people think they have nothing to hide. This assumption is generally false, and particularly so when it comes to health. Everyone has something to hide, and there's nothing wrong with that. You can glean a lot of information from health data that various market players such as health, daily benefits, disability or life insurance providers, authorities, employers or the pharmaceutical industry would be keen to have.

Dr Barbara Widmer is a lawyer who represents the Conference of Cantonal Data Protection Officers on various eHealth Suisse working groups.

A lot of people think they have nothing to hide. This assumption is generally false, and particularly so when it comes to health.

What are the greatest data protection-related risks associated with mHealth apps?

There are three major risks.
The first is the misappropriation of data. Under data protection legislation, data can only be used for the purpose communicated when it was gathered. Applied to mHealth apps, this will regularly mean measuring, collecting and analysing certain values. Unfortunately, there is also a risk that the manufacturer or provider will be making background use of the data for other purposes, such as advertising, without the consent of the people supplying the data.
The second risk stems from non-transparent data processing. Users of mHealth apps are often unaware of where the app is storing their data, who has access to it and the extent to which it is passed on to third parties.
The third risk is poor IT security. Data protection legislation stipulates that mHealth apps must provide state-

of-technology security. However, cost considerations mean that manufacturers tend to economise on security, especially with free apps. This jeopardises the accuracy of the data (data that is wrongfully accessed may be falsified or attributed to the incorrect people), and inadequate security increases the risk of data theft.

What should users do to gain maximum benefit from mHealth apps while at the same time minimising the risk of data misuse?

Paid apps give people greater control over how their data are used. This applies to paid apps in general, incidental-

Who of us has never used the pedometer function on our smartphone? This function and all the other health and fitness apps that can be found on the ever-present smartphone would not have been possible without the megatrend of digitalisation. These apps can measure data from our body with utmost accuracy, whether for the purpose of tracking our physical activity, improving our athletic performance and efficiency, recording our sleep phases or giving us nutritional recommendations.

They are ultimately no more than an aid. Nevertheless, they can help us to know our body better, keep it healthy or improve its health. In the light of this, there is no doubt that mHealth apps have enormous potential for preventing non-communicable diseases (NCDs) such as cancer, diabetes or musculoskeletal diseases; in particular for people who are already affected or who are very likely to contract one at some point in the future. The widespread availability of smartphones and the large number of free apps are thus helping more people to benefit from a greater range of ways of doing something beneficial for their health.

Showing people the benefits of taking more exercise or adopting a healthier diet can be a major challenge for specialists in the field of prevention. mHealth applications combine fun, are user-friendly and have strong data security. They could represent a recommendable tool in order to increase motivation and make it easier for people to take the first step towards improving their health.

To achieve, this will require an effort by everyone involved. Companies and researchers will have to develop and produce user-friendly apps that embody high ethical and moral standards, while doctors and other healthcare professionals will have to motivate their patients to exploit suitable digital applications. This is the only way we are able to benefit from the potential which mHealth offers.
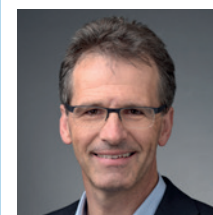
Roy Salveter
Head of the Department for the Prevention of Non-Communicable Diseases

ly, not just to mHealth apps. Many people do not appreciate that in the digital world, free apps are only superficially free because the providers earn money from evaluating the data they collect and, depending on the circumstances, selling them on to third parties – often without the affected people's knowledge. For this reason, anyone who uses mHealth apps should always buy their apps, rather than use free ones, and find out why data is collected, who has access to it, where it is stored and whether and how much of it is passed on to third parties.

If the data is not stored within the EU, you need to be careful.

What, if anything, can users do to protect themselves?

There's plenty you can do. You should always be wary of mHealth apps that appear to be free (cf. answer to question 4),

checking instead to see if there's a paid version, and making sure that you can get answers to the following questions: What purpose does the mHealth app collect the data for, who has access to it, where is it stored and does it get passed on to third parties? If you can't get answers to these questions, don't use the app, even if you have to pay for it.

What happens if I want to exercise my data protection rights, but the data is abroad, say in the EU, USA, China, Russia or India, for example?

It depends on what country the data is in. If it's in the EU, you have a very good chance of being able to exercise your rights successfully. The EU has completely overhauled its data protection legislation and tightened it up in various areas. The EU's data protection authorities can now impose heavy fines on anyone caught infringing the EU's data protection laws, for example.

If the data is not stored within the EU, you need to be careful. Although the

USA does have data protection legislation, there are substantial differences between it and European or Swiss notions of data protection. Countries such as China, India or Russia have no or at best limited data protection legislation. Users of mHealth apps should therefore only use apps that store data in either Switzerland or the EU.

What areas of Switzerland's data protection law do you think need updating?

I think the law is fine as it stands. The problem is less the law itself than the fact that stake-holders are too little aware – if they are aware at all – of existing data protection requirements. Alternatively, they simply don't care about them, something that also goes for a lot of users. In view of this, we need to intensify our efforts to enforce the existing legislation. The EU and eHealth Suisse have now produced guidelines containing checklists that producers and suppliers of eHealth apps can use to audit themselves. As a further meas-

ure, Switzerland is discussing the option of setting up a central government-run or partly government-run agency to carry out minimal testing of mHealth apps.

Our interviewee

Dr Barbara Widmer is a lawyer who represents the Conference of Cantonal Data Protection Officers on various eHealth Suisse working groups. These include the mHealth working group, which is addressing the subject of "mobile terminal devices" from various perspectives. She has a postgraduate qualification in international economic law and is a certified internal auditor. She has research interests in economic, intellectual property, information and EU law and also works on supervisory issues that need to be readdressed in the light of the spread of digitalisation.

Can mHealth deliver greater health equity?

Digital disadvantage. The widespread adoption of smartphones in all sectors of the population gives some idea of the potential that could be harnessed for health promotion and prevention purposes. However, owning a smartphone does not always equate with being able to make adequate use of mHealth apps.

Who's going to benefit from it? This is the question that gets asked with every new achievement. One concept that is frequently mentioned when talking about digital media in this context is the "digital divide". This term is applied to the gap that exists between the people who are able to use new digital services to expand their knowledge and those who cannot benefit from such progress. Furthermore, mHealth can only benefit people who own the necessary technical equipment, possess the skills needed to use it effectively and have the motivation to adopt it or at least see advantages in adopting it. Switzerland's Media Use Index for 2017 shows that 92 per cent of the population accesses the Internet from a mobile device. Nevertheless, it must be assumed that there are groups within the population who find using digital media or the content available on them challenging. This group, known as the "digitally disadvantaged", consists primarily of older people and people with a low socio-economic status or level of education.

mHealth skills – i.e. the ability to use mHealth apps effectively – include the following:
– The reading, writing and arithmetic skills needed to use written information.
– Technical skills to ensure access to functioning technical equipment and the Internet, and the ability to use apps, websites or other applications.

Access to mHealth can be facilitated by improving mHealth skills.

– Health skills, i.e. being able to take decisions in everyday life that have a positive impact on health.
– Being able to understand diagrams or illustrations containing information.

The skills needed to use mHealth apps can change over time and in certain life situations.

Another important consideration is the fact that the skills needed to use mHealth

apps can change over time and in certain life situations. The health skills of people with physical or mental problems are frequently impaired in particular situations. Access to mHealth can be facilitated by improving mHealth skills while at the same time ensuring that the barriers to using mHealth apps are kept as low as possible. mHealth skills can be enhanced by means of smartphone courses or patient empowerment, for example. The most effective way of reducing the barriers to using mHealth apps is to address the issue at the development stage. To enable an app to be used by as many people as possible, for example, the following

points should be taken on board: 1. Involve users in the development and evaluation process. 2. Provide action-centred information that addresses the question "What should I do?" 3. Avoid providing too much information. 4. Simple navigation and design. 5. Ensure interactivity: it must be possible to share and print out content.

While mHealth certainly has the potential to increase health equity, it can only do so if it is easy to access, if users have better mHealth skills and if clear data protection regulations are in place.

Contact:
Angela Bachmann,
National Health Policy Section,
angela.bachmann@bag.admin.ch

Further literature to the article can be found at www.spectra-online.ch