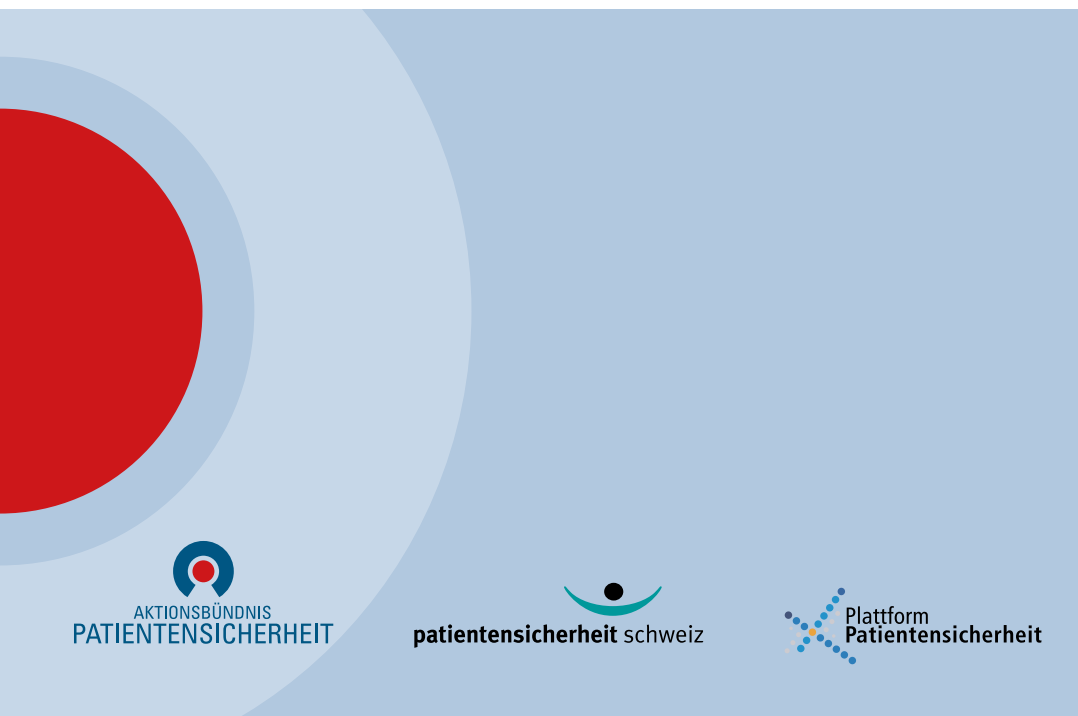


PATIENT INFORMATION



DIGITIZATION AND PATIENT SAFETY CHECKLIST FOR THE USE OF HEALTH APPS



INHALT

INTRODUCTION	3
1. PURPOSE AND FUNCTIONALITY	4
2. QUALITY AND EVALUATION	4
> Apps for diagnosis and treatment	4
> Ratings by other users	5
> Quality certificates and certification marks	5
3. DATA PROTECTION AND ACCESS	6
> Data privacy notice	7
> Access to functionality and data	7
4. PROVIDER INFORMATION AND IMPRINT	8
> Imprint	8
5. FUNDING AND FINANCIAL BACKGROUND	9
Glossary	10
Feedback	10
Bibliography	10
Imprint	11

INTRODUCTION

The rapid advances in digitization are a key area of activity for the German Coalition for Patient Safety (Aktionsbündnis Patientensicherheit e.V., APS). Alongside these guidelines for the use of health apps, a set of recommendations for managing risks in patient care in the digital age has also been published.

Many different types of health apps are available. Some apps help to support particular health-related behaviours, for example by measuring physical activity (fitness trackers), while others remind users to take their medication. Other apps allow users to book doctor's appointments, to transmit patient histories to a physician, or to take readings such as blood sugar levels.

In this checklist, we have summarized some key facts to help you weigh up the risks and benefits associated with using health apps on mobile devices such as tablets, smart phones or wearables and also give tips for the safer usage of such apps.

As a consumer, it is important that you are aware of both the potential benefits as well as risks to patient safety inherent in digital health applications. Benefits manifest in the form of support for a treatment through patient education and information provision. On the other hand, risks emerge in the form of false information or the misuse of personal data.

In these guidelines, we offer advice to help you find the right application for you. At the end of each section, we have summarized the key facts. This checklist is intended to help you in choosing and using health apps. The idea is not to just tick all or a minimum number of boxes since these guidelines do not provide an evaluation of the medical utility or scientific accuracy of the information or recommendations provided by health apps. Under no circumstances should an app replace personal medical advice because only your doctor or therapist can evaluate which treatment is right for you.

1. PURPOSE AND FUNCTIONALITY

Every health app provides a specific set of functions that have to be evaluated by each (potential) user according to their individual needs and preferences. Screenshots and descriptions of a given app can be found in app stores and provide an overview of its functionality. Possible limitations to functionality and the benefits of the app often only present themselves when the app is actually used. Many apps are updated fairly regularly, for example to remove software errors or to add new functions. The operating system of the mobile device should be kept up-to-date in order to prevent security gaps.

CHECK!

Regardless of your individual requirements for the app, in order for it to run safely and reliably the following criteria should be met:

- The specific scope of the app is clearly described, e.g. daily reminders to take medication.
- The app lists its own limitations (e.g. disclaimer stating that the app cannot replace a real-life medical consultation).
- The last update was provided less than six months ago (as a rule of thumb).
- The app runs reliably and does not crash or restart unprompted.

2. QUALITY AND EVALUATION

It is important to question the accuracy and the sources of the information provided by health apps. Unfortunately, for most users the risks associated with outdated or false information and recommendations are difficult to assess. To help you make such assessments, in this section we list several characteristics that signify quality and reliability in an app.

> Apps for diagnosis and treatment

Apps that claim to help you make your own diagnosis should be evaluated critically. Diagnoses should always be made by a (specialist) physician. False

diagnoses can have fatal consequences. You should also exercise extreme caution when using apps that recommend treatments to be carried out without any medical supervision.

CHECK!

Check whether the following two criteria definitely apply to a given app:

- The app **does not** provide a definitive diagnosis and corresponding treatment recommendations.
- The app does support existing treatment plans (e.g. by recording biometrics).

> Ratings by other users

Ratings given by other users and shown in app stores (e.g. 1–5 stars) can provide an initial indication of the quality of a given app. A large number of positive reviews can indicate that an app is popular and useful, but this does not necessarily have to be the case. Always be critical and cautious! It is not always possible to ascertain the authorship or motivation behind online reviews. Additionally, new apps may not yet have very many user reviews, so the validity of the rating may be limited.

CHECK!

- The app has frequently been rated positively by a many different users.

> Quality certificates and certification marks

Consumer protection organizations, organizations for testing consumer goods (e.g. *Which?* or *Consumer Reports*), medical associations and/or private companies also provide recommendations and certification for particular apps. The meta-criteria catalogue created by the Fraunhofer Institute provides a platform for evaluating health apps.

A certification process usually results in an app receiving a certification mark that can be displayed within the app itself or on its website.

The requirements an app has to fulfil in order to receive certification can vary significantly, so they should be evaluated cautiously. If the evaluation criteria are described clearly, you can tell which organization awarded the certification on what basis.

- Certification marks awarded by the TÜV, e.g. “Trusted App” awarded by TÜV TRUST IT GmbH, or the TÜV Rheinland mark, which is primarily concerned with data protection.
- “DiaDigital”, for example, is a certification mark seal for good diabetes apps awarded by the German diabetes associations.

Most app stores indicate whether an app has been certified or awarded a quality mark. If this specific information is missing, you can find out more about the certification mark in the internet. If you cannot find any information here either, then view the certification critically.

CHECK!

- The app has been certified and awarded a trustworthy certification mark.
- The evaluation criteria associated with the certification mark are clear and understandable.

3. DATA PROTECTION AND ACCESS

How well your personal data are secured and protected when you use health apps should play a key role in your decision concerning whether or not to use a specific app.

The German constitution guarantees the right of all citizens to decide how their personal data should be used (right to digital self-determination). In Germany, the specifics are regulated by, among others, the Federal Data Protection Act, the Data Protection Acts of each federal state, the Telemedia Act as well as the new European General Data Protection Regulation.

Given the breadth and complexity of the topic, our guidelines cannot engage comprehensively with the issue of data protection. Questions like “Where will my data be stored”, “How well will my personal information be protected from third parties?” and “Will my data be passed on to others?” are often dif-

difficult to answer, because data traffic is international and servers are frequently located abroad. Germany's stringent data protection laws are therefore not always applicable.

> Data privacy notice

CHECK!

Generally, an app should provide a data privacy notice covering the following points:

- The app provides a data privacy notice, which...
 - is easy to find and to view (e.g. directly within the application, on its websites or in app stores),
 - provides information about the type, extent and purpose of data collection as well as the particulars of how data are processed and whether they are passed on to third parties,
 - specifies where (in which country) and how (encrypted/ anonymized) your data are stored,
 - specifies whether and how (via email or post etc.) you can withdraw your consent for data storage.

> Access to functionality and data

CHECK!

Generally, apps that request and/or store your personal data should have the following characteristics:

- The app only requests data that are important to its functionality.
- Requests for access to functions of the mobile device (e.g. access to location via GPS or to the calendar) are only requested in order to facilitate app usage.
- The app specifies that it is possible for collected and stored data to be deleted. Given that it is rarely possible to delete data irretrievably, you should be careful in deciding which data to share.

4. PROVIDER INFORMATION AND IMPRINT

Research the provider of a given app. The imprint usually contains information on developers and providers. Determining who has developed and is marketing an app can reveal background information about the app as well as financial dependencies and potential commercial interests (see 5. Funding and Financial Background).

The imprint can help identify the background to the development of the app, possible motives for developing it as well as dependencies and possible commercial interests. For instance, a particular health app may advertise a certain service or product (e.g. medication).

> Imprint

An app has to contain an imprint. The contents of this imprint are legally defined. The absence of an imprint can indicate that a given app may be of questionable quality.

Do not use apps without an imprint!

CHECK!

The imprint of an app is required to contain at least:

- The name and address of the provider. Legal entities (e.g. Inc., PLC, Ltd., Co.) in particular must state their legal form and authorized representatives.
- Details for direct and immediate contact (telephone or fax number, email address).

5. FUNDING AND FINANCIAL BACKGROUND

Every app requires financing to cover the costs of development, regular product maintenance and the provision of services as advertised. Aside from sponsorship and public funding, other means of financing apps include in-app purchases and advertising. **Always watch out for hidden costs when using an app.**

Apps that recommend a specific product (e.g. medication) are always questionable – such recommendations undermine the objectivity and independence of the app.

The business model, i.e. funding model, of an app is often not immediately apparent. On the one hand, this type of information tends to be slightly obscured, on the other hand it is often not published. **Currently, health app providers are not required to be open about their funding sources, so it is difficult for users to find out whether a given app was designed to promote specific interests.**

CHECK!

- The financial background of an app is apparent if, for example,
 - users pay for the app and it finances itself,
 - the costs for the app are reimbursed by health insurance providers (this is very rare),
 - sponsors and/or public funding finance the app.
- The app is neutral, meaning that its contents are not influenced by commercial interests, if for example,
 - the app **does not** advertise a specific product,
 - the app is provided by a public or charitable organization.

Glossary

Further information on terminology related to digitization can be found on the homepage of the German Coalition for Patient Safety (Aktionsbündnis Patientensicherheit e.V., APS):

<http://www.aps-ev.de/glossar/>

Bibliography

- Albrecht, U.-V.; Höhn, M. & von Jan, U.: Kapitel 2. Gesundheits-Apps und Markt. In:
- Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 62–82. urn:nbn:de:gbv:084-16040811225.
- <http://www.digibib.tu-bs.de/?docid=60007>, Zugriff am 03.11.2017
- Albrecht, U.-V.: Kapitel 13. Orientierung für Nutzer von Gesundheits- Apps. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Medizinische Hochschule Hannover, 2016, S. 282-300. Urn:nbn:de:gbv:084-16040812052. <https://www.digibib.tu-bs.de/?docid=60020>
- „Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl I S. 3618) geändert worden ist“. Zugriff über: http://www.gesetze-im-internet.de/bds_g_1990/BDSG.pdf, Zugriff am: 21.11.2017
- Düsseldorf Kreis. Orientierungshilfe zu den Datenschutzerfordernungen an App-Entwickler und App-Anbieter. Zugriff über: https://www.datenschutz-bayern.de/technik/orient/OH_Apps.pdf, Zugriff am: 21.11.2017
- Gesundheits- und Versorgungs-Apps, Lucht M, Boeker M, Kramer U, Universitätsklinikum Freiburg, 2015. <https://www.tk.de/tk/themen/digitale-gesundheit/studie-einsatz-gesundheits-apps-freiburg/744480>
- „Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530) geändert worden ist“ § 5 – Allgemeine Informationspflichten, Zugriff über: https://www.gesetze-im-internet.de/tmg/_5.html, Zugriff am: 03.11.2017
- „Telemediengesetz vom 26. Februar 2007 (BGBl I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530) geändert worden ist“. Zugriff über: <https://www.gesetze-im-internet.de/tmg/TMG.pdf>, Zugriff am: 21.11.2017
- TÜV TRUST IT, Trusted App, <https://it-tuv.com/leistungen/zertifizierungen/zertifizierung-von-apps-trusted-app/>
- TÜV Rheinland, Geprüfter Datenschutz, https://www.tuv.com/de/deutschland/ueber_uns/pruefer_pruefen/pruefungen_in_der_virtuellen_welt_1/gepruefter_datenschutz/gepruefter_datenschutz.html
- AG Diabetes & Technologie, DiaDigital, <https://diadigital.de/>
- Aktionsforum Gesundheitsinformationssystem (afgis) e.V., <https://www.afgis.de/>
- eHealth Suisse, <https://www.e-health-suisse.ch>
- HealthOn e.V., Verein zur Digitalen Gesundheitsförderung, <https://www.healthon.de/impressum>
- Stiftung Health On the Net, HONcode, <https://www.healthonnet.org/HONcode/German/>
- Verbraucherzentrale. Apps und Datenschutz. <https://www.verbraucherzentrale.de/Smartphones-Alleskoennen-mit-Risiko-1>

Feedback

The APS Guidelines are intended to improve patient safety and require continuous adjustment and development. Feedback and suggestions for improvement as well as your ideas and criticisms are therefore explicitly welcomed.

Please contact:

Aktionsbündnis Patientensicherheit e.V.
Am Zirkus 2, 10117 Berlin, Germany
E-Mail: info@aps-ev.de

Imprint

Editors

Aktionsbündnis Patientensicherheit e.V. (German Coalition for Patient Safety)
Plattform Patientensicherheit Österreich (Austrian Network for Patient Safety)
Stiftung Patientensicherheit Schweiz (Swiss Patient Safety Foundation)

Working Group on “Digitization and Patient Safety – Mobile Apps for Patients”

Chair: Britt Kaulen (Priv. Adler Apotheke oHG)

Representative of the APS Board: Marcel Weigand (Weisse Liste gGmbH)

Members of the Working Group and Authors of the Recommendations

Beate Balzuweit (Pfizer Deutschland GmbH), Gerald Burgard (Helios Kliniken), Dr. Kerstina Horch (Robert Koch-Institut), Marcel Kusch (Universitätsklinikum Heidelberg), Manja Nehrkorn (Ärztekammer Berlin), Annabelle Neudam (4QD - Qualitätskliniken.de GmbH), Prof. Dr. Guido Noelle (gevko GmbH), Ulrike Schmitt (Kassenärztliche Bundesvereinigung), Veronika Strotbaum (ZTG Zentrum für Telematik und Telemedizin GmbH)

First German edition: May 2018

First English edition: February 2019

DOI: 10.21960/201903/E

Layout: Alice Golbach, APS

Photo credits: iconimage/Fotolia

Copyright and right of use: These guidelines can be downloaded free of charge from www.aps-ev.de. The brochure is protected by copyright and may not be changed in any way, neither in layout nor text. Commercial usage is not permitted.

Citation: German Coalition on Patient Safety (APS) e.V. (ed., 2019): Digitization and Patient Safety – HE2) Checklist for the Use of Health Apps, Berlin.

