Spitzenverband

# Comments by the National Association of Statutory Health Insurance Funds from 13.09.2016

## to the public consultation on the safety of apps and other non-embedded software

**GKV-Spitzenverband**
Reinhardtstraße 28, 10117 Berlin
Telephone: +49 30 206288-0
Fax: +49 30 206288-88
politik@gkv-spitzenverband.de
www.gkv-spitzenverband.de
Transparency Register Number
839750612639-40

# I. Introduction

On 9 June 2016, the European Commission commenced a public consultation on the safety of apps and other non-embedded software. This includes, among others, apps for health and well-being. The aim is to define potential next steps and future policy measures at EU level, as well as to revise horizontal and/or sector-specific legislation.

The GKV-Spitzenverband welcomes the fact that the European Commission is looking at the safety of apps because health apps, medical apps and medical device apps not only have a great deal of potential but also pose different levels of safety risk. They can cause damage to health or delay recovery from health problems, for example, if the app is flawed or unreliable, if it is used incorrectly or if it is simply ineffective. In addition, other conceivable risks include those associated with economic damage, property damage and data security.

In the opinion of the GKV-Spitzenverband, current horizontal and sector-specific EU legislation does not sufficiently cover the safety of health apps and other non-embedded software. Due to the potential cross-border nature of processing and using health data, additional (uniform) rules for data security are necessary. European-wide rules must make it clear that an app falls under the EU Directive for medical devices (93/42/EEC) or the future EU medical devices Regulation if its purpose is to initiate or guide medical therapies, if it provides a medical diagnosis or if it is to be used for screening or prevention purposes.

The GKV-Spitzenverband represents all 117 statutory health and long-term care insurance funds in Germany and, thus, the interests of more than 70 million insured persons and contribution payers when dealing with politics and healthcare providers. It advises the German parliaments and ministries under current legislative procedures and has a statutory responsibility to look after the interests of German healthcare and long-term care insurance funds with regard to supranational and cross-national organisations and institutions. The GKV-Spitzenverband is a member of the European Social Insurance Platform (ESIP) via the German Social Insurance (DSV).

# II. Comments for the consultation

### 1. What type of apps or other non-embedded software pose safety risks? Please give examples.

Health apps, medical apps and medical device apps, which are sometimes linked with medical devices or sensors (e.g. wristbands or watches); personal advice and monitoring systems; SMS with health information and reminders to take medication; and telemedicine services can all pose a potential threat to safety. In addition, there are apps for administrative processes within the statutory health insurance system. Establishing a link with the IT systems of the health insurance funds places demands on the IT and information security of these systems.

Different categories of these apps not only have potential but also pose safety risks at different levels. A distinction should be made between health apps, medical apps, medical device apps and apps for managing business processes in the health insurance system.

- Apps for managing business processes use the electronic data of the insured person and are increasingly replacing paper-based processes as part of digitalisation. These processes are subject to the highest safety requirements because the content is often classified as social data.
- Health apps are mobile applications for citizens and patients with the primary aim of promoting good health (Lucht et al., 2015).
- Medical apps consist of mobile applications for healthcare providers to assist them with their everyday working life, as well as mobile applications for patients to help with self-management of mainly chronic diseases (Lucht et al., 2015).
- Medical device apps help to diagnose, prevent, monitor, treat or alleviate illnesses; to diagnose, monitor, treat, alleviate or compensate for an injury or disability; to investigate, replace or modify the anatomy or a physiological process; or to control contraception (Section 3, Nr. 1 Medical Devices Act, MPG).

### 2. What risks can apps or other non-embedded software pose?

X Economic damage

X Physical damage to individuals

X Physical damage to property

X Non-material damage (pain and suffering)

X Other

**Please explain:**

The apps mentioned above and non-embedded software have the potential to cause damage to health or to delay recovery from health problems, for example, if they are flawed or unreliable, if they are used incorrectly or if they are simply ineffective.

Various sources have documented that it is sometimes the case that the type of apps discussed here, as well as other software, do not function correctly. Examples of this are: information incorrectly entered by users is not rejected, e.g. diabetes apps that calculate insulin doses (Huckvale et al., 2015) or parameters for body function are not measured correctly and as a result there are no valid results for energy metabolism (Murakami et al., 2016) or for blood pressure (Plante et al., 2016). Under certain circumstances, an incorrectly calculated dose of insulin or showing that blood pressure is normal when in fact it is too high, can result in physical damage to an individual. Apps which assess skin changes can produce a false diagnosis (Wolf et al., 2013). It is obvious that these miscalculations or misjudgements can result in extra costs arising from the need to clarify the suspected diagnosis as well as non-material damage (pain and suffering). In the event that an error made by a diagnostic or therapeutic app results in a person not seeking necessary medical care, this can lead to damage to their physical health, a misdiagnosis or the wrong therapy.

There is also the potential for economic damage if costs arise as a result of a person using an unsafe or faulty health app, or if these costs are reimbursed by the German statutory health insurance. The costs associated with the provision of outpatient care via mobile-health services are, in principle, payable by the German statutory health insurance funds. In this situation, their cost-effectiveness needs to be considered, including a comparison with other methods already paid for by the statutory health insurance funds (see Question 10).

A key factor is the risk associated with data security. Health data is among the most sensitive personal data and needs special protection. Basic requirements for the secure processing of health data through mobile-health services include end-to-end encryption, clearly defined access rights, secure authentication of people authorised to access the data, and the use of secure end devices. The risk of unauthorised access to health data and the ability to distribute or manipulate this data should be minimised as much as possible.

Physical damage to property can result when the IT systems of service providers are compromised. Depending on the type of attack, there can be costs for restoring the system, costs for compensation and also costs for client information. A serious attack could mean that an IT system must be completely written off, for example, as seen with the current ransomware trojans.

**Please give your opinion on the following options:**

| | No risk | Low risk | High risk | Very high risk |
|---|---|---|---|---|
| Economic damage | ○ | X | ○ | ○ |
| Physical damage to individuals | ○ | ○ | X | ○ |
| Physical damage to property | ○ | ○ | X | ○ |
| Non-material damage (pain and suffering) | ○ | ○ | X | ○ |
| Other | ○ | X | ○ | ○ |

**Please explain:**

Depending on the app or software, the risks associated with using the application can vary in degree. An insulin app that miscalculates the dosage of a medication can represent a very high risk. A pedometer that counts steps incorrectly represents, in contrast, a low or zero risk for the user. For more on economic damage, physical damage to property and the risk associated with data security, see above.

**3. In which sectors are apps or non-embedded software most affected by safety problems?**

- ○ Agriculture
- ○ Electronic Communications/Telecommunications
- X Health
- ○ Home automation/Domotics
- ○ Energy
- ○ Financial
- ○ Transport
- ○ Other

**Please specify:**

Apps and non-embedded software in the health sector can pose safety risks. The GKV-Spitzenverband does not comment about the safety risks of apps in other sectors.

**4. In your professional experience have you already identified unsafe apps or other non-embedded software or have consumers approached you because they encountered problems with unsafe apps or other non-embedded software?**

X Yes

○ No

**Please specify:**

Specific apps are named in the sources (Huckvale et al., 2015; Murakami et al., 2016; Plante et al., 2016).

**4.1. If yes: What did you do to solve these problems?**

Until now, dedicated scientific authors, such as Huckvale et al., 2015, have written reviews on their own initiative. Based on these articles, the UK's Medicines and Healthcare products Regulatory Agency (MRHA) has written to the individual creators of faulty apps and invited them to make comments. In Germany, there is no information regarding intervention following the identification of faulty apps.

In the area of statutory health insurance in Germany, there is increasing reliance on e-government as part of digitalisation. Federal legislation clearly regulates the framework conditions for the providers of apps. Based on this, regulatory authorities specify clear requirements for offering apps. In particular, mechanisms for IT and information security are examined on the basis of guidelines set by the Federal Office for Information Security (BSI).

**5. Are existing EU or national safety rules and market surveillance mechanisms sufficient to monitor and withdraw, where necessary, unsafe apps or non-embedded software from the market?**

○ Yes

X No

**Please explain:**

In Germany, there exist provisions regarding the product safety of apps which are regulated by the Act on Medical Devices (MPG).

In terms of IT and information security, apps in the statutory health insurance system have an adequate foundation at national level. These are: (from ADV Test Guidelines for Electronic Communication and Long-Term Storage of Electronic Data, Last updated 22 April 2016)

- Federal Office for Information Security (BSI) Standard 100-1 to 100-4
- BSI IT-Grundschutz Catalogue
- Technical Guideline TR03138 "Substitute Scanning" (TR-RESISCAN)
- Technical Guideline TR03125 "Archiving of cryptographically signed documents" (TR-ESOR)
- "Guidelines for correctly handling sensitive data when using De-Mail" (Federal Commissioner for Data Protection and Freedom of Information, BfDI, from 1 March 2013)
- "Brief comments on the Act to promote electronic government and on the revision of other provisions" (Federal Ministry of the Interior, BMI, Unit O2 – Released: 27 June 2013).
- Minimum requirements for federal and state courts of auditors when using information and communication technology – guidelines and common standards for ICT audits, Last updated: November 2011
- Organisational concept for electronic government work (publisher: Federal Ministry of the Interior)
- BSI minimum standards for using SSL/TLS protocol by federal authorities (Version 1.0, last updated: 2014)

For EU regulations, see answer to Question 7.

**6. Have you been held accountable for damage caused to consumers because of unsafe apps or other non-embedded software?**

- ○ Yes, as manufacturer of the device the software runs on or controls
- ○ Yes, as an app or software manufacturer/developer
- ○ Yes, as an intermediary/distributor (e.g. app store)
- ○ Yes, other
- X No

**6.1. If yes: What did you do?**

Not applicable

**7. Do you think that existing horizontal and sector-specific EU legislation (e.g. General Product Safety Directive, Market Surveillance Regulation, Medical Device Directive, Radio Equipment Directive) taken together sufficiently cover the safety of all types of apps or other non-embedded software available on the market?**

- ○ Yes
- X No

**Please explain:**

Data security:
The basic prerequisite for the secure processing of health data through mobile-health services are: end-to-end encryption, clear access rights, secure authentication of people with access rights, and the use of secure end devices.

Due to the cross-border nature of processing and using health data, additional (uniform) rules are necessary. The following must be transparent: the purpose for collecting and using data; when and if the data will be deleted after the app is uninstalled; and where the data is stored.

Approval and product safety:
It is important to clearly distinguish between applications for medical devices and applications for health and medicine. It is true that mobile applications for measuring values, such as heartrate during high-intensity sport, can be categorised as “lifestyle and nutrition advice” apps (training planners, calorie calculators, etc). However, they measure important health and medical parameters with a scientific claim to the validity of the measurements.

An mHealth application becomes a medical device when its purpose is to initiate or guide medical therapies, when it provides a medical diagnosis or when it has a screening or prevention purpose. The term “medical therapy” includes prescribing and adjusting drug therapies, as well as personalised diet plans. An example of screening or prevention, in this sense, would be an app that estimates the malignant risk of skin lesions based on photos (see Wolf et al. Diagnostic Inaccuracy of Smartphone Applications for Melanoma Detection. JAMA Dermatol 2013, 149: 422-426).

In this context, there is work to be done. There must be European-wide rules which make it clear that an app falls under the EU Directive for medical devices (93/42/EEC) or the future EU medical devices Regulation, if the app has such a purpose. The GKV-Spitzenverband calls for an independent review of the performance of software products by a notified body to ensure that they are effective and function properly, as well as transparent information about their performance and risks. Just having a “self-declaration” from the manufacturer/developer, as is the case for

Class I medical devices, is not enough for mobile applications when they are designed for one of the aforementioned purposes, namely therapy, diagnosis, screening or prevention.

Apps must be classified according to the risk that is associated with their use and their quality must be tested according to this risk. In addition, their benefit for patients and their cost-effectiveness for therapy must be proven. Rule 10a on classifying active devices in the consolidated text of the new EU Medical Device Regulation (Version 27.06.2016) stipulates that software should be categorised as Class IIa when it provides information which can be used to make diagnostic or therapeutic decisions. If this decision may directly or indirectly cause a serious deterioration of the state of health or a surgical intervention, the software is to be categorised as Class IIb. If this decision can possibly lead to death or an irreversible deterioration of the state of health, the software is to be categorised as Class III.

According to the draft regulation, software intended to monitor psychological processes is in Class IIa, unless it monitors vital physiological parameters whose variation could result in immediate danger to the patient. In this case, the software falls into Class IIb. All other software falls into Class I.

To a certain extent, this precise classification of health apps into the respective product classes increases safety when using apps of this definition.

At the point a mobile app is placed on the market, it must be ensured that users can access public information about the tested performance of this app.

It is extremely important for the German statutory health insurance that existing liability regulations are not compromised. In the event of damage, the relevant provisions concerning product liability on the part of the manufacturer (especially manufacturers of medical devices) must apply in order to satisfy claims made by insured persons and patients.

**10. In the EU Member State where you operate, are there specific rules on safety requirements for apps or other non-embedded software?**

X Yes

○ No

The use of social data, in terms of apps offered in Germany by the health insurance funds or other providers of social insurance, is regulated by national legislation in Section 38 of the German

Social Code (SGB), Book I; Section 67 ff. of the SGB, Book X; and Section 284 of the SGB, Book V. This legislation strictly regulates how social data can be used and how consent is to be established. If an app, which accesses social data, is developed for a health insurance fund, the awarding of the contract to develop the app is only possible under the strict conditions of Section 80 of the SGB, Book X.

Apps for medical devices must provide information regarding their intended purpose as stipulated by German law. The intended purpose for the medical device is the use for which the medical device is intended according to the information provided by the manufacturer in the labelling, instructions or marketing materials of the device (Section 3, Paragraph 10, Medical Devices Act, MPG). This is done by the manufacturer via a self-declaration as per Section 5 of the MPG.

The costs associated with the provision of outpatient care via mobile-health services (called outpatient telemedicine services in Section 87, Paragraph 2a, Sentence 8 of the German Social Code, Book V) are, in principle, payable by the German statutory health insurance funds. The framework agreement between the National Association of Statutory Health Insurance Physicians and the GKV-Spitzenverband (see Attachment) can be drawn upon when it comes to telemedicine services and the conditions that must be met for payment by the statutory health insurance funds. In addition, if the outpatient telemedicine service deals with a new method of examination or treatment, the German Federal Joint Committee must first have issued recommendations regarding:

1) the recognition of the diagnostic and therapeutic benefit of the new method as well as its medical necessity and cost-efficiency (including a comparison to methods already undertaken at the expense of the health insurance funds) based on the current state of scientific knowledge of the respective therapy,
2) the qualifications necessary for doctors, the equipment requirements and requirements for quality assurance needed to ensure the proper application of the new method, and
3) the records necessary regarding medical treatment (Section 135, Paragraph 1, German Social Code, Book V).

Storing social data in the cloud is not permitted. For mobile health services that are operated by third parties on behalf of the German health care funds, there must be an assurance that the providers are adequately checked (for example, as required in Section 80, German Social Code, Book X). The processing and storing of health data in unsecured cloud systems is extremely problematic.

## 13. Further comments

The risk posed as the result of a disease should neither be affected by the social status of the person, nor by the person's rural or urban location, mobility and thus access to medical care.

Therefore, despite the due caution expressed here, it is important to highlight the opportunities provided by mobile health services (Dorsey et al., 2016). They can address existing shortcomings by being integrated into the existing healthcare system in strict compliance with applicable privacy policy, scientifically-evident content and independent quality assurance.

## 14. Evidence, references


- Rahmenvereinbarung zwischen der Kassenärztlichen Bundesvereinigung und dem GKV-Spitzenverband als Trägerorganisationen des Bewertungsausschusses gemäß § 87 Abs. 1 Satz 1 SGB V zur Überprüfung des Einheitlichen Bewertungsmaßstabes gemäß § 87 Abs. 2a Satz 8 SGB V zum Umfang der Erbringung ambulanter Leistungen durch Telemedizin.
- Dorsey, E.R., Topol, E.J., 2016. State of Telehealth. N ENGL J MED 375; 2. DOI: 10.1056/NEJMral1601705.
- Huckvale, K., Adomaviciute, S., Prieto, J.T., Leow, M.K.-S., Car, J., 2015. Smartphone apps for calculating insulin dose: a systematic assessment. BMC Med. 13, 106. doi:10.1186/s12916-015-0314-7
- Lucht/Bredenkamp/Boeker/Kramer, 2015. Gesundheits- und Versorgungs-Apps. Hintergründe zu deren Entwicklung und Einsatz. Studie des Universitätsklinikums Freiburg im Auftrag der Techniker Krankenkasse.
- Murakami, H., Kawakami, R., Nakae, S., Nakata, Y., Ishikawa-Takata, K., Tanaka, S., Miyachi, M., 2016. Accuracy of Wearable Devices for Estimating Total Energy Expenditure: Comparison with Metabolic Chamber and Doubly Labeled Water Method. JAMA Intern. Med. 176, 702-703.
- Plante, T.B., Urrea, B., MacFarlane, Z.T., Blumenthal, R.S., Miller, E.R., Appel, L.J., Martin, S.S., 2016. Validation of the instant blood pressure smartphone app. JAMA Intern. Med. 176, 700-702.
- Wolf, J.A., Moreau, J.F., Akilov, O., Patton, T., English, J.C., Ho, J., Ferris, L.K., 2013. Diagnostic inaccuracy of smartphone applications for melanoma detection. JAMA Dermatol. 149, 422-426.