Public consultation on the safety of apps and other non-embedded software not covered by sector-specific legislation*  
* such as medical devices or radio equipment

Fields marked with * are mandatory.

1 Introduction

This consultation concerns software and applications (apps) which are neither embedded, nor contained in a tangible medium at the time of their placement in the market, their supply to consumers or when they are otherwise made available to consumers (non-embedded software). Examples include health and well-being apps that can be used on a mobile device, digital models for 3D printing or apps controlling other devices (such as electronic appliances).

The purpose of the consultation is to gather input from various stakeholder groups, in particular consumers, businesses and authorities, on their experience related to the safety of apps and other non-embedded software. The questions aim at obtaining a better understanding of the possible risks and problems that non-embedded software may pose and how these problems could be dealt with. The views gathered will help to define potential next steps and future policies at the EU level including, if appropriate, possible revisions of existing horizontal and/or sector-specific EU legislation.

If apps are giving access to a service, this consultation addresses only the safety aspects in the functioning of the app, and not the underlying service itself (e.g. transport or accommodation). For the purpose of this consultation, only apps and non-embedded software that are downloadable on a device such as a personal computer, tablet or smartphone or accessible on a remote location (cloud) would be covered.

For the purpose of this consultation "safety" and "safe use" should be understood as freedom from unacceptable danger, risk or harm, including security-vulnerabilities ("cyber-security") and cover physical, economic as well as non-material damage.

This consultation will only look into the safety of apps and other non-embedded software which is not already addressed and foreseen by sector-specific legislation such as the Medical Devices Directives, the Machinery Directive or the Radio Equipment Directive which include provisions on safety ensuring that equipment within their scope, if compliant, is safe.
2 General information on respondents

* Your feedback will be published on the Commission’s website unless this would damage your legitimate interests. Do you agree to publication?

- Yes – under the name supplied I consent to publication of all the information in my feedback, and I declare that none of it is subject to copyright restrictions that would prevent publication.
- Yes – anonymously, I consent to publication of all the information in my feedback except my name/the name of my organisation, and I declare that none of it is subject to copyright restrictions that would prevent publication.
- No - my feedback cannot be published, though I consent to its being used internally by the Commission.

* I’m responding as:

- An individual in my personal capacity.
- The representative of an organisation/business.
- The representative of a public authority/international organisation/academia.

For representatives of an organisation/business please select the applicable option:

- Manufacturer of the device the software runs on or controls
- App or software manufacturer/developer
- Distributor/intermediary (e.g. app store)
- Industry association
- Trade union
- Consumer organisation
- Other

Please specify:

Professional Association
Is your organisation registered in the Transparency Register of the European Commission and the European Parliament?

Please register your organisation in the Transparency Register of the European Commission and European Parliament before completing this public consultation.

- Yes
- No

Please register in the Transparency Register before answering this questionnaire. If your organisation responds without being registered, its input will be considered as that of an individual and will be published separately.

Please indicate your organisation's registration number in the Transparency Register.

Briti103340111
My institution/organisation/business has its main establishment:

- All EU Member States
- Austria
- Belgium
- Bulgaria
- Czech Republic
- Croatia
- Cyprus
- Denmark
- Estonia
- France
- Finland
- Germany
- Greece
- Hungary
- Italy
- Ireland
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Spain
- Slovenia
- Slovakia
- Sweden
- United Kingdom
- Other

*Please specify:

British Medical Association, Tavistock Square, London WC1H 9JP, United Kingdom
Please indicate the name of your institution/organisation/business:

British Medical Association (BMA)

Please indicate your address and contact details:

*First name:
Robert

*Last name:
Delis

*E-mail address:
rdelis@bma.org.uk

Address:
BMA European Office, Rue du Luxembourg 3, Brussels 1000, Belgium

More information:

3 Consultation:

3.1 For individuals or representatives of a public authority / organisation / business.
In your view:
1. What type of apps or other non-embedded software pose safety risks? Please give examples.

*10 character(s) minimum*

The BMA is concerned primarily with apps and non-embedded software related to health and healthcare. In this context, the following types of app/software potentially pose a safety risk to healthcare professionals and patients that use them:

- Any that presents the user with health-related and/or clinical information that is intended to help the user to make a decision to modify their behaviour
- Any that is used alone or as part of a set of technologies that tracks and collects data/information about the user that is used to assess and monitor health-related metrics (e.g. number of steps, heart rate) that are intended to help the user make decisions about behaviour
- Any that requires the user to collect and/or report health-related personal information, which is then stored by the app
- Any that interfaces with an electronic health record and can upload or download information to a patient’s EHR with or without consent from the GP

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

- ✔️ Economic damage
- ✔️ Physical damage to individuals
- □ Physical damage to property
- ✔️ Non-material damage (pain and suffering)
- □ Other

*Please explain:*

*10 character(s) minimum*

The BMA believes that health apps and other non-embedded software have the potential to support patients to self-manage conditions, as well as to support clinicians to deliver care more quickly, access improved decision support and communicate more effectively between primary, secondary and social care. However, there are some potential risks if unsafe apps are developed and used by the public and health professionals. The BMA is aware that many apps that pose a high risk to users are likely to be captured under the EU Medical Devices Directive, which are not considered by this consultation.

Economic damage

There is little evidence that health and wellbeing apps reduce demand on the health system, and in fact could even increase demand and therefore, economic costs. It appears that there can be economic benefits to be gained by apps being used by people to self-manage existing conditions and their health more
generally, resulting in decreased costs in acute care and long-term condition management. Conversely, however, using health and wellbeing apps that do not provide correct and adequate information and guidance may result in people delaying the point at which they engage with the health care system, which can significantly increase the costs of their care than if the health service were engaged earlier.

As technology develops to enable patients to upload real-time health data from an app to their GP’s EHR, it becomes important to consider the GP’s liability in relation to the information they receive. Using mobile apps to send vast amounts of data may increase the expectation patients have of their GP, expecting that the GP will regularly review the data received. Issues may arise if the GP does not view or act on this information, especially if the patient then experiences an adverse event or deteriorating health. GPs must always be able to retain control of the EHR, choosing which apps to accept data flows from, and switching incoming data flows on or off as required. GPs would also require safeguards and support to ensure they are protected from liability based on the information they receive from health apps.

Physical damage to individuals

An app that provides health professionals or patients with information about health-related topics needs to be clinically accurate, as well as regularly updated with new information. Any incorrect information in an app risks people making unsafe decisions that may lead to physical or mental harm to patients. People use an app to identify symptoms and potentially self-diagnose instead of consulting a health professional. This may lead to poorer health outcomes.

There is also a risk that complex and specific health information provided by an app may not be understood or interpreted correctly by the user. This can be exacerbated when apps synced with wearable technology such as Fitbit provide continuous monitoring of activity levels, heart rate and sleep patterns. Where people lack capacity to interpret the information, or the app does not provide adequate support to interpret it, some people may become overly focused on monitoring their results and become highly concerned by readings that may indicate normal variation and/or faulty readings. This lack of understanding can also lead to people making poor health-related decisions and increasing the burden on health care providers.

Non-material damage (pain and suffering)

Health apps that collect and/or use health information (classified by the General Data Protection Regulation as a special category of personal data), need to take extra care to ensure data is processed correctly and safely, in line with the GDPR. If data about a person’s health is unlawfully collected, used, or inadequately protected from loss or theft, there is a clear risk of pain and suffering to users. Furthermore, if a national health system is to encourage the uptake and use of health and wellbeing apps, it is imperative that available apps adequately comply with the GDPR, as confidentiality breaches by apps will decrease public trust in apps, and the health professionals that recommended them. Failure to do so may result in damaged
relationships between patient and doctor.

Please give your opinion on the following options:

<table>
<thead>
<tr>
<th></th>
<th>No risk</th>
<th>Low risk</th>
<th>High risk</th>
<th>Very high risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>*Economic damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Physical damage to individuals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Physical damage to property</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Non-material damage (pain and suffering)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please explain:

10 character(s) minimum

The EU Medical Devices Directive requires health and wellbeing apps that actually act as medical devices to obtain and carry CE marking to ensure they are safe to use. This means that many apps that pose higher physical risks to users and professionals will be captured under this directive, and therefore not considered in this response.

However, there remains a higher risk that the personal health data collected and used by apps not classified as medical devices may be collected and used unlawfully. For example, the NHS Apps Library was closed after it was found that the accredited smartphone health apps could be putting users’ privacy unnecessarily at risk of identity theft and fraud, with many sending unencrypted personal and medical information over the internet. Given that this occurred despite the NHS having accredited the health apps, it is clear that careful consideration needs to be given as to how to ensure all apps use personal information safely, not only ones classified as CE marked medical devices.
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

3.2 For representatives of a public authority / organisation / business.

In your view:

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?

- [ ] Yes
- [x] No

Please specify:

10 character(s) minimum

The BMA has not undertaken any investigation into individual health apps or other non-embedded software to ascertain their safety, but has reviewed the evidence undertaken by other researchers.
4.1 If yes: What did you do to solve these problems?

*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
- No

*Please explain:

The BMA does not have a response to this question

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
- No
6.1 If yes: What did you do?

10 character(s) minimum

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
- No

Please explain:

10 character(s) minimum

The BMA does not have a response to this question

8. Have you considered opening up an Application Programming Interface (API) of a device you manufactured or a service you provide to app and software developers to link their app to your device/service and use its functionalities? If so, have you taken into consideration safety aspects?

- Yes
- No
- Not applicable
9. Has the legal framework on safety influenced your decision on whether to invest in developing apps or software?
   - Yes
   - No
   - Not applicable

Please explain:
   10 character(s) minimum

10. In the EU Member State where you operate, are there specific rules on safety requirements for apps or other non-embedded software?
   - Yes
   - No
*Please select the country where you operate:

- [ ] All EU Member States
- [ ] Austria
- [ ] Belgium
- [ ] Bulgaria
- [ ] Croatia
- [ ] Cyprus
- [ ] Czech Republic
- [ ] Denmark
- [ ] Estonia
- [ ] Finland
- [ ] France
- [ ] Germany
- [ ] Greece
- [ ] Hungary
- [ ] Italy
- [ ] Ireland
- [ ] Latvia
- [ ] Lithuania
- [ ] Luxembourg
- [ ] Malta
- [ ] Netherlands
- [ ] Poland
- [ ] Portugal
- [ ] Romania
- [ ] Slovakia
- [ ] Slovenia
- [ ] Spain
- [ ] Sweden
- [x] United Kingdom
- [ ] Other
Medical device regulation by MHRA

In the UK, software and apps that are defined as medical devices must gain a CE mark (kite mark) from the Medicines and Healthcare Products Regulatory Agency (MHRA). This is in line with the EU medical device directives requiring relevant apps to show they are ‘regulated and acceptably safe to use and also perform in the way the manufacturer/developer intends them to’.

In August 2016, the MHRA updated its guidance (https://www.gov.uk/government/news/is-your-app-a-medical-device-its-healthy-to-know-regulator-issues-updated-guidance) on whether a health app should be subject to medical device oversight. The guidance is presented as a step-by-step interactive PDF. App users can use this guidance to check if their health app is a medical device, and what to look for to make sure the app is safe and works. The new guidance addresses some of the concerns around classifying health apps, with the likelihood of an app being treated as a medical device by the MHRA depending on what the app does and the corresponding level of patient risk associated with it.

App accreditation in UK

The UK’s National Information Board (NIB) is also undertaking work to re-establish the NHS Apps Library, by providing citizens with access to an accredited set of NHS and social care ‘apps’. Plans include the health and care system validating apps, and advertising this validation to the public. These apps can be downloaded from app stores or people may be directed to them from digital health services such as NHS.UK or healthcare professionals. Health and care professionals and commissioners will be provided with guidance on which apps to recommend to citizens. Apps for use by professionals will also be reviewed and accredited. App developers will have clear guidance to support the development of better quality health apps.
13. Do you have any further comments?

14. Please upload any files with evidence or references that you consider relevant:

Contact

CNECT-PUBLIC-CONSULTATION-APPS-SAFETY@ec.europa.eu