Second draft of guidelines

EU guidelines on assessment of the reliability of mobile health applications

This document is intended to capture and describe a set of voluntary guidelines for assessing the validity and reliability of data that mobile health applications collect and process. It has been produced in response to challenges identified within the mHealth market in Europe and, specifically, to address the issues raised as a results of a public consultation in January 2015.

Second draft of guidelines

A study prepared for the European Commission
DG Communications Networks, Content & Technology by:

Digital Agenda for

This study was carried out for the European Commission by

Consard Limited

Andrew Ruck

Susie Wagner Bondorf

Charles Lowe

Internal identification

Contract number: 30-CE-0763782/00-20

INDEX

1 INTRODUCTION

1.1 Background

This section outlines the work undertaken prior to the production of these guidelines.

It explains why they are needed, and how they will be refined.

The purpose of the mHealth app assessment guidelines is to establish a framework of safety, quality, reliability and effectiveness criteria to improve the use, development, recommendation and evaluation of mHealth apps. This is with the clear goal to facilitate prevention and an overall healthcare advancement through a controlled use of mobile technology.

The mHealth app market in Europe is facing challenges. In order to tackle these, on 10 April 2014 the European Commission published a Green Paper on mHealth [1]. The issues arising from consultation on the Green Paper are documented in the report issued by the European Commission in January 2015.

Safety and transparency of information were identified as key issues along with data quality when linking mHealth apps to Electronic Health Records (EHR) for the effective uptake in clinical practice. A number of stakeholder meetings were organised during 2015, and the outcome was a common understanding that there are health and safety risks related to mHealth apps which need to be handled with regards to:

1. Clinical evidence;
2. Claims on the purpose and functions of mHealth apps;
3. Test and validation of the performance.

Early in 2016, the European Commission appointed a Working Group, to progress the development of the guidelines.

The guidelines are foreseen to be drafted in four iterations each followed by stakeholder engagement that will lead to the changes to next draft in light of feed-back received:

First Iteration was presented at an open stakeholder meeting 4 May 2016, written feedback was invited until 16 May

Second Iteration (this version) is being published at the end of May 2016

Third Iteration is targeted for mid-October 2016

Fourth (and Final) Iteration is targeted for end-December, with feedback to be included in final report (2017-01-25).

The first draft of the guidelines was presented and discussed at an open stakeholder meeting, organised by the Commission on 4 May 2016 in Brussels. The feedback received at the meeting and the written input provided by the stakeholders through the online survey has been used to refine the contents of the first draft and will be further taken into account for the following iterations. Altogether 25 written responses were received to the online consultation.

This current version is the second draft. Following publication of the draft, consultation will occur with and feed-back will be sought from a range of stakeholders: for more information about how to get involved, please contact:

CNECTMHEALTH-EXPERTGROUP@ec.europa.eu

1.2 EU Regulatory Landscape and other related initiatives

This section reviews the regulatory landscape applicable to mHealth apps with a particular focus on legislation centring on medical devices, data protection and consumer protection legislation as well as voluntary EU-level activities including the privacy code of conduct for mHealth apps, possible implementation of an EU-wide PAS277 and other applicable standards.

1.2.1 Legislation

Together with the Green Paper previously referenced[1], in April 2014 the Commission published a Staff Working Document which provides a non-exhaustive description of the existing EU legal framework which is applicable to mHealth apps, including lifestyle and wellbeing apps. The Staff Working Document aims to provide simple legal guidance as to the EU applicable legislation for app developers, medical device manufacturers, digital distribution platforms, etc.[1]

While the Staff Working Document covers a variety of legislation, three legislative areas are of particular concern for mHealth apps[2]:

- Medical device/in vitro device

[1] https://ec.europa.eu/digital-single-market/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and

[2] A complete list would also reference Negligence, Product Liability Directive 85/374, General Product Safety Directive 2001/95, Information Society Technical Standards Directive 98/34, Electronic Commerce Directive 2000/31, Privacy & Electronic Communications Directive 2002/58, Misleading & Comparative Advertising Directive 2006/114, Bribery Act 2010, ABHI Code

- Data protection
- Consumer protection

1.2.1.1 Medical device/in vitro device regulation

The current applicable regulations comprise the Medical Devices Directive and the In Vitro Devices Directive (there is also the Implantable Devices Directive though it is considered unlikely to be relevant). These specify the conditions under which hardware, software and combinations of the two are classified as medical devices and therefore have to abide by specific medical safety requirements. The key phrase is what the "intended use" is. As explained in more detail below, precise guidance, including a helpful flow chart, on what is a medical device is provided in Meddev 1.2/6.

As these directives were written before the advent of apps, they are expected to be superseded by a Regulation which more specifically addresses the medical risk of apps that is now anticipated to come fully in to force in 2019. The current draft significantly extends the definition of a medical device.[3]

Prior to the voluntary guidelines in this document, there was no EU-wide guidance below the medical device level for mHealth, other of course than the consumer protection requirement mentioned below, and those items referenced in the footnote 2.

1.2.2 Data protection

The currently legal framework pertaining to the field of privacy is the Data Protection Directive[4] and the ePrivacy Directive[5]. Both Directives apply to any apps installed or used by end-users in the EU, regardless of the location of the app developer or app store.

1.2.2.1 Data Protection Directive

Having been transposed into national laws, the Data Protection Directive places obligations on apps stating that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The data must also be relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

According to the Data Protection Directive, the legal ground for processing personal data varies according to the nature of the data. Personal data concerning health[6] is classified as 'sensitive' data leading to strict requirements for its processing. Processing is only allowed

[3] http://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/revision/index_en.htm

[4] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[5] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (modified by Directive 2009/136/EC on privacy and electronic communications)

[6] Information on both physical and mental health of an individual (e.g. genetic data, consumption of medical products, etc.)

under 3 circumstances: explicit consent, vital interests of data subject, and requirement for medical diagnosis/preventative medicine. Lifestyle and well-being apps, which process personal data which are not deemed as sensitive, are not required to abide by the stricter rules impacting sensitive data, but must still comply with the remaining principles of the Directive (e.g. data minimisation, data retention and limitation, adoption of appropriate safeguards).

Personal data concerning health cannot be further processed for commercial purposes by third parties unless the data subject has provided their explicit consent after having been duly informed of specific commercial purpose(s). If processing data, third parties are required to respect all data protection principles, in particular the purpose limitation principle, and security obligations for the part of the processing for which it determines purposes and means. However, in accordance with national law, there may be cases where the prohibition to process sensitive data cannot be lifted regardless of the consent of the data subject.

1.2.2.2 ePrivacy Directive

Despite applying mainly to the electronic communications sector, the ePrivacy Directive sets out rules for any entity that wishes to store or access data stored in devices of users located in the European Economic Area (EEA)[7]. The main provision impacting apps is the cookie requirement, which notes that the storing of information or the access to information already stored in an end-user's terminal equipment is only allowed on condition that the end-user has given their consent. Such consent must be provided with clear and comprehensive information on the purposes of the processing. This consent requirement applies to any information meaning that when an end-user installs an app, they must be given the choice to accept or refuse cookies (or similar tracking technologies placed on devices).

1.2.2.3 General Data Protection Regulation ("GDPR")

In January 2012, the European Commission issued a comprehensive reform of the Data Protection Directive in an effort to address the national fragmentation of data protection law in Europe. The GDPR[8] is a single set of rules valid across the EU aimed at eliminating the current fragmentation and costly administrative burdens while reinforcing consumer confidence in online services. In May 2016, the official text of the Regulation was published in the EU Official Journal. While the Regulation entered into force in May 2016, it shall apply from May 2018 following the transposition by Member States into national law.

The GDPR preserves many of the principles enshrined in the Data Protection Directive, including classifying health data as sensitive data. However, the GDPR now specifically lists genetic data and biometric data as sensitive personal data and permits Member States to introduce further conditions around the processing of biometric, genetic, or health data. Furthermore, as under the Directive, the GDPR requires organisations collecting and using

[7] The EEA consists of Iceland, Liechtenstein, Norway and 27 of the 28 EU Member States (The agreement is applied provisionally for Croatia pending ratification of its accession)

[8] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing Directive 95/46/EC)

sensitive data to rely on limited ground of lawful processing including consent, public interest for public health reasons and providing preventive or occupational medicine.

Of particular note, app developers will be under specific obligations to introduce data protection by design and default into their processing systems when building apps. Moreover, data controllers and processors will be under new obligations about the documentation they must retain and the provisions their contracts must include. Controllers will need to implement appropriate data protection policies and both controllers and processors will be required to keep a record of processing activities. The GDPR also introduces an obligation to report data breaches to data protection authorities and to affected individuals. This is a new comprehensive obligation that is not industry specific but instead is triggered if the personal data breach is likely to result in a risk to individuals.

1.2.3 Consumer Protection

The current legal framework pertaining to the field of consumer protection is the Consumer Rights Directive[9], the eCommerce Directive[10] and the Unfair Commercial Practices Directive[11].

1.2.3.1 Consumer Rights Directive

The Consumer Rights Directive ensures a uniform EU-wide level of protection for consumers when buying an app in the EU. Under the Directive, app stores & developers (when the consumer receives an app directly from the developer) are considered as traders and must comply with a series of requirements when a consumer buys a lifestyle and well-being mHealth app (the Directive expressly excludes contracts for healthcare). Traders must provide consumers with a series of information (e.g. identity of trader and contact details, the existence/non-existence of a right to withdrawal, functions of digital content, technical protection measures, etc.) in a clear and understandable language. Traders must inform consumers directly before an order is placed about the main characteristics of the app, the total price, the duration and termination of the contract and the minimum duration of the consumer's obligations under the contract. The trader must ensure that the consumer explicitly acknowledges that the order implies an obligation to pay, by labelling the order button with words "order with obligation to pay" or an equivalent unambiguous formulation. If the trader does not comply with this obligation, the consumer is not bound by the contract. Consumers are provided a 14-day period to withdraw from any app contract.

The European Commission will carry out an evaluation of the Directive in 2016 to assess its impact on the Internal Market based on the criteria of relevance, coherence, efficiency, effectiveness, and European added value. The report of the evaluation is expected to be published in the first quarter of 2017.

[9] Directive 2011/83/EC on consumer rights (repealing Directive 97/7/EC)

[10] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market

[11] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the Internal Market

1.2.3.2 eCommerce Directive

The eCommerce Directive covers information requirements that must be provided by service providers who are providing an 'information society service'[12]. App stores and app developers (when directly selling an app) are considered under the Directive to be providing an 'information society service'. Free apps are also regulated by the Directive as the legislation covers any economic activity, including cases in which the remuneration is received from other sources, such as advertising.

The Directive lays down general information requirements which a service provider must provide before a consumer purchase an app (i.e. price, tax and delivery costs, relevant trade register, steps to conclude a contact, technical means for identifying and correcting input errors, etc.). Once an app is purchased, the service provider must acknowledge the receipt of the order.

The Directive also provides for a framework of liability for intermediary information society service providers. This is specifically relevant for app stores who may be regarded as hosting service providers as they provide storage of information provided by the app developer. In such instances, the hosting service provider may not be held liable for the information stored at the request of the recipient of the service. This occurs only when the provider does not have the actual knowledge of an illegal activity or information and when the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.

1.2.3.3 Unfair Commercial Practices Directive

The objective of the Unfair Commercial Practices Directive is to maintain a consumer's freedom of choice by prohibiting unfair commercial practices by traders. The Directive applies to all business-to-consumer ("B2C") commercial practices. A B2C commercial practice is deemed unfair if it does not comply with the principle of professional diligence as set out in the Directive and is likely to distort the economic behaviour of the average consumer. Of specific note, a B2C commercial practice is deemed unfair when it is misleading or aggressive[13]. Traders must, when promoting or selling an app, avoid any practices which could mislead a consumer or which could compromise his freedom of choice.

In May 2016, the Commission published a guidance document on the application of the Directive. In addition, the Commission will carry out in 2016 a 'fitness check' of the EU Consumer Acquis, including the Directive.

1.2.4 Voluntary EU-level activities

1.2.4.1 Interfacing with medical device legislation

[12] Information Society Service – *'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'*

[13] Practice containing false information deceiving the consumer and likely to significantly impair a consumer's freedom of choice by harassment, coercion or undue influence

The reliability and validity of health apps falling under the medical device definition are addressed through the medical device CE certification process, so these guidelines do not specifically address reliability and validity requirements for such apps. They may however be helpful (on a voluntary basis), when assessing other aspects.

As a result, the requirement for regulatory compliance (with medical device legislation for instance) is one aspect of the assessment proposed in the guidelines.

However, there is also a need to deal with the "grey zone" as the distinction between what falls within and outside the definition of a medical device is not always clear. The criteria for those apps that are on the borderline and could fall under the medical device definition, is aligned with the medical devices requirements as far as possible. Therefore, for safety purposes, where "health apps" may create a hazardous situation, they are treated - in terms of development scrutiny, documentation, verification, and validation for instance, in a similar manner to medical devices.

Recognising the importance of better delineation of mHealth apps that would need to be classified as medical devices and other health apps the Medical Devices Expert Group (MDEG) has adopted guidance in the medical devices regulatory framework. MEDDEV 2.1/6 "Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices"[14] is providing useful guidance for deciding whether the stand alone software should follow the medical devices regulatory route. The guidelines are currently being updated to clarify the definitions and also to align with the work carried out in the context of the IMDRF (International Medical Devices Regulatory Forum).

The "Manual on Borderline and Classification in the Community Regulatory Framework for Medical Devices" is also a useful document with concrete examples of software and mHealth apps which may or may not qualify as medical devices. The update of the manual is expected to be published soon with two additional entries on mHealth apps for managing and accessing moles.

Also, the International Medical Device Regulators Forum (IMDRF) has been working on guidance documents[15] that support innovation and timely access to safe and effective Software as a Medical Device (SaMD) globally. In particular, following documents provide useful references for both manufacturers and regulators:

- Software as a Medical Device (SaMD): Key Definitions (IMDRF/SaMD WG/N10FINAL:2013)
- Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations (IMDRF/SaMD WG/N12FINAL:2014)
- Software as a Medical Device (SaMD): Application of Quality Management System (IMDRF/SaMD WG/N23 FINAL:2015)

[14] http://ec.europa.eu/growth/sectors/medical-devices/guidance/index_en.htm

[15] http://www.imdrf.org/workitems/wi-samd.asp

1.2.4.2 Code of Conduct for mHealth App Privacy

In March 2015, as a result of the Green Paper consultation, the European Commission launched an initiative to create an industry-led mHealth privacy Code of Conduct ("CoC"). The CoC is targeted at app developers and its purpose is to foster justified trust among users of mHealth apps which process personal data that include data concerning health. The CoC, aims to provide easily understandable guidelines for app developers on how to respect (and comply with) EU data protection rules. Although voluntary, once certified entities will be legally required to respect the requirements set out under the CoC. The code is a voluntary instrument and will require interested parties to certify, meet and respect the obligations. In June 2016, the CoC was sent to the Article 29 Working Party[16] for formal approval.

1.2.4.3 Development of EU quality standards for mHealth apps

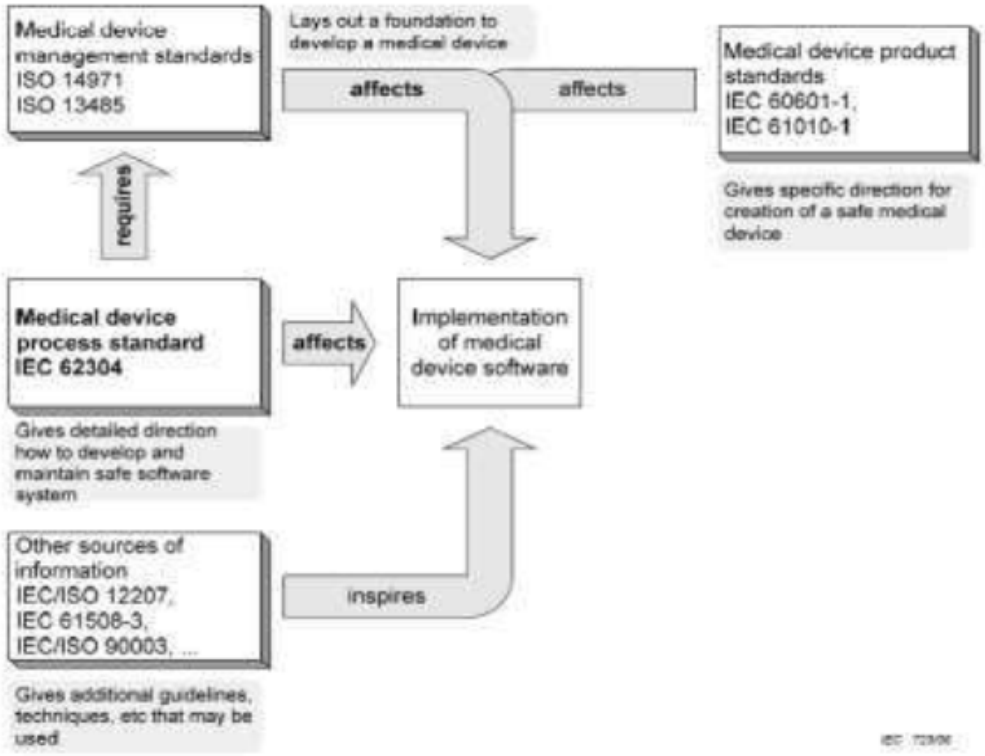
The European Commission 2016 Rolling Plan for ICT Standardisation [1] includes an action to develop European standards to provide guidance to the eHealth and wellness apps' developers by setting out quality criteria and principles to be followed throughout the app development life cycle. The British Standards Institution (BSI) has developed a publicly available standard "PAS 277:2015 Health and wellness apps – Quality criteria across the life cycle – Code of practice" which has been suggested as a basis for the standardisation action to be taken forward by CEN (Technical Committee 251 Health Informatics).

In addition, an International Standard IEC 82304-1 is being prepared by a Joint Working Group of IEC subcommittee 62A (Common aspects of electrical equipment used in medical practice) and ISO technical committee 215: Health Informatics. This international standard, when published (expected by end of 2016), applies to the safety and security of health software products designed to operate on general computing platforms and intended to be placed on the market without dedicated hardware. The primary focus of the standard is on the requirements for manufacturers. It covers the entire lifecycle including design, development, validation, installation, maintenance, and disposal of health software products. Health software products, within the context of this standard, are intended by their manufacturer for managing, maintaining or improving health of individual persons, or the delivery of care. Some health software can contribute to a hazardous situation. Accordingly, a risk management process is required for all health software. For health software that can contribute to a hazardous situation, risk control is needed to prevent harm or reduce the likelihood of harm occurring. Testing of the finished product is not, by itself, adequate to address the safety of health software. Therefore, requirements for the processes by which the health software is developed are necessary. This standard relies heavily on IEC 62304:2006 as amended by AMD1:2015 for the software development process which can be applied to health software products.

[16] Set up under Directive 95/46/EC, the Article 29 Working Party is composed of a representative of the supervisory authorities designated by each EU Member State, the European Data Protection Supervisor (EDPS), and the European Commission

1.2.5 Existing standards

This section outlines the main international and European standards relevant for the medical software development process.



The diagram above describes the principal standards[17] that are strongly advised for the development of lower risk medical devices, and effectively mandated for higher risk ones, so are given primarily for information here.

However, they do offer a structured process for identifying potential areas of risk and so are useful for managing the development of medical software to minimise subsequent risk of harm from the software. As such they are a valuable resource particularly for developers whose apps come close to the definition of medical devices.

[17] Others Include: medical/health focus: ISO/TR 17791:2013-12 (health informatics - enabling safety in health software), ISO/TR 27809:2007-07 (Health informatics - Measures for ensuring patient safety of health software), ISO/IEC 82304 (Health Software), DIN EN ISO 62366 (Medical devices/usability), general focus: ISO 25010 (Systems and software engineering - Systems and software Quality Requirements and Evaluation), ISO 9001, DIN EN ISO 9241, ISO/IEC 12207, DIN EN ISO 27001

2 PURPOSE

This section describes the aim of the guidelines and their status in relation to other applicable EU or MS legislation or regulation

A growing number of people use mHealth apps to monitor their lifestyle and health status or to manage chronic disease. They and the people caring for them, need to know that the data from these apps is trustworthy and reliable, and for instance be assured that data could be suitable for inclusion within electronic health records.

These guidelines therefore, build on existing initiatives and best practices from across Europe and beyond. They propose a set of common quality criteria and assessment methodologies to help different stakeholders including end users, developers, payers of care, and vendors of electronic health record systems to assess the validity and reliability of mHealth apps.

This means that patients would be able to give health professionals access to data collected by the apps for the purpose of improved consultations.

Further, health professionals will be reassured about the reliability and validity of the apps. Knowing that a health app works as intended and is based on valid scientific evidence and that patients' personal data will be recorded safely and securely, will give health professionals greater confidence in recommending or prescribing as part of the treatment/monitoring process.

To summarise in a sentence, the aim of the guidelines is "better use of better apps for better healthcare".

The purpose of the mHealth assessment guidelines is to meet this need in creating trust and confidence in mHealth apps to improve adoption. However, in order to ensure that clinicians recommend the apps and that citizens, patients & carers use them, it is necessary to establish a broad framework of criteria that provides the basis to improve the use, development, recommendation and evaluation of mHealth apps.

The guidelines proposed are voluntary. Where relevant, explicit linkages are identified to existing applicable EU or MS legislation or regulation; in which cases compliance to these regulatory requirements is mandatory.

3 SCOPE

This section describes the intended scope of the guidelines. Medical devices are regulated by EU Medical Device regulation. These guidelines propose supplementary voluntary guidance for apps in health and social care.

As is further explained below, some mHealth apps are regulated by existing EU legislation as medical devices. These guidelines therefore address all other mHealth apps that are not

medical devices, including apps that are used in a health and social care context which according to the intended use identified by the manufacturer do not fall under the definition of a medical device, as well as health & wellbeing apps aimed primarily at disease prevention. For those mHealth apps that are regulated by existing EU legislation as medical devices, the guidelines propose some additional voluntary assessment criteria.

As a result, the scope of these guidelines is broad. They cover the so-called 'grey zone' of those apps that just fall below the lowest category of medical devices (Class 1), through to apps such as medical appointment booking apps that nevertheless involve exchange of potentially sensitive personal information[18].

Many social care-related apps have an important medical element and it is expected that in some circumstances, use of the guidelines will be beneficial for these apps. Clearly there is a judgement call to be made here, however there is no desire to exclude this category from assessment by these guidelines where it is judged appropriate.

'Off-label' uses of apps with other intended use(s), in other words, apps being used in the health or social care context for which they were not originally intended, are excluded from the scope.

4 TARGET GROUPS: CURRENT SHORTCOMINGS AND NEEDS

This section identifies how some main stakeholder groups are likely to benefit from using the guidelines.

An initial listing of target groups likely to benefit from the guidelines has been prepared: the intention is that the guidelines would initially focus on meeting the needs of these groups. However, at this stage, the listing is not intended to be exhaustive. For each group, the 'do nothing' scenario and shortcomings of the current situation are described, and then the needs or expectations from the guidelines are highlighted.

The specific way in which these – and any other - target audiences for the guidelines would use them in practice, is a work in progress and is further described in Annex A. Work is ongoing to analyse further the needs and expectations of the main target groups, and make practical recommendations on how they can best use the guidelines in practice.

[18] Other examples include Patient/carer decision aids & self-management tools, Clinical decision support tools for diagnosis/treatment recommendation, Behaviour change apps – simple self-management tools, Healthcare education apps (for both professional & end-users), "Serious games", Point-of-care diagnosis, Monitoring or treatment aids, Access & editing of EHRs, Communication apps – e.g. teleconsultation, Apps providing documentation functionality &/or display a simple measurement, Registries & vital events tracking – public health surveillance, Simple calculators of on-personal information (e.g. BMI), Generic medical calculators, etc.

The results of this work are expected to be reflected in the next iteration of the guidelines.

Target Group	**Description**	**'Do nothing scenario' / Shortcomings of the current situation**	**Needs from the guidelines**
Citizens	Not a homogeneous group – includes healthy people, consumers, patients and their carers. Note patients (e.g. some chronic disease patients) or their carers are co-producers of health and very knowledgeable and engaged in the care process	Lack of trust leading to low use of apps.	Simple tool (check-list) to decide which app to use
			Citizens cannot be expected to go through all the scrutiny questions, but want to know that the app is 'safe' and 'effective'
			Information about app status: assessment outcomes should be public
		Widely varying levels of 'health literacy' and knowledge of the disease exist. Moreover, citizens vary substantially in their level of motivation to attain/retain good health.	
mHealth developers		Europe might become a less favoured place for mHealth business because of poor market conditions.	Guidance on how the different criteria could be built in in the development process. (for instance need to align with IEC8234-1 and PAS277)
			Usage of the guidelines should create value from the perspective of app developers
App Aggregators	App stores, App certifiers	Europe might become a less favoured place for	Trusted and practical process to identify the good from the

Target Group	Description	'Do nothing scenario' / Shortcomings of the current situation	Needs from the guidelines
	(including public authorities), App aggregators	mHealth business because of poor market conditions.	less good apps
		Proliferation of unassessed apps creates sub optimal uptake of 'quality' apps	
Healthcare Professionals		A risk may exist that the healthcare professional's duty to 'do no harm' to patients is compromised, due to lack of trusted information about app reliability and quality	An assessment tool for own use, when choosing or recommending an app
		Patients' use of (unassessed) apps can create extra work (for health professionals) and can lead to frustration (for patients)	Positioning of app assessment processes in the context of evidence of clinical effectiveness
		Joined up service provision (using apps) does not occur because available apps are not suited to their immediate environment or take account of specific clinical needs.	
Healthcare System	Healthcare providers	Currently face a requirement to	A fully fledged assessment tool providing the basis for detailed

Target Group	Description	'Do nothing scenario' / Shortcomings of the current situation	Needs from the guidelines
	(hospitals, primary and social care); Public authorities; Healthcare payers and commissioners Health insurance providers	devote effort and resources to developing their own guidelines, causing risk of duplication and conflicting guidelines country by country.	assessment/validation/ certification for those making the full certification, either public providers (e.g. Andalucía, Catalonia) or private third party assessment (e.g. DMD Santé, Medappcare, etc.)

In addition, Appendix 4 will describe some typical use cases.

5 FORMAT AND ADOPTION

The guidelines will be voluntary. Further work is planned to explore how target audiences can best use the guidelines in practice

Work continues to make practical recommendations on how target users of the guidelines can best use the guidelines in practice. This work will include consideration of presentation and format. However, some initial design parameters include:

- The guidelines should be simple to read.
- They should use visual flow charts and decision trees when possible, and consider optimal presentation for online use / viewing.
- If supplementary info required, click-throughs to fuller description and supporting information should be possible.
- A decision tree could be a good outcome.
- For patients, short simple communications will be essential.

The following potential use cases have been identified so far:

- Dissemination & Promotion activity and materials;
- Development/specification of tools, based on the guidelines;
- Evaluation of apps against Quality criteria;
- Legislation/regulation;
- Integrate into assessment methodologies (Quality MS) and audits;
- Certification/labelling;
- Tailored recommendations to e.g. stakeholders organisations, professional bodies and patient associations;
- Linkage of app data to electronic health records;
- Support for management of patients/caseloads.

It is expected that the full guidelines will be deployed primarily by organisations assessing or certifying apps who will then publish or otherwise provide the result of their activities to other stakeholders.

End users (citizens, patients, carers) and professional users (clinicians, nurses, social workers) will then use the output from the assessment bodies or certifiers to provide advice on appropriate app usage.

To support this, simplified versions of the guidelines could be produced which will explain to users the principal assessment categories and the basis for recommending or rejecting apps. A simple checklist could be envisaged which could be used by end-users.

6 GUIDELINES

6.1 Criteria

This section explains the main criteria and the basis for selecting those criteria

A total of nine criteria have been identified based on the analysis of existing assessment frameworks (Annex A1) that are relevant for the assessment of mHealth apps

In addition to validity and reliability, other aspects have been identified such as usability, accessibility, transparency that are important from the end-user perspective for improved confidence and wider adoption of mHealth apps; likewise, effectiveness & credibility from the professional perspective.

The diagram above illustrates these nine criteria, or domains, as all contributing to the data quality objective.

Subsequent sections, will describe these criteria in more detail. As mentioned in the previous section, a possible use case for some stakeholders could be assessing apps against these guidelines, so a detailed process is proposed in Appendix 3 as one of the possible models. This is structured as set of three activities:

- Initial validation – that the app exists, is appropriate for the evaluation, is downloadable etc.
- Risk assessment – which in turn determines the appropriate level of scrutiny
- Scrutiny – of both the technological and the medical aspects

Scrutiny forms a combination of a scoring system and mandatory pass/fail questions; apps failing a mandatory question or not reaching a sufficiently high score are not recommended.

6.2 Initial validation

This section describes the first step: initial validation

Initial validation comprises collecting important information that is of value to all users, and provides critical initial input for the assessment.

The questions begin with basic information such as App name, Supplier, Developer (if different), whether the app is CE certified as a medical device (if 'yes' not covered by these guidelines), whether the app is primarily for health or social care purposes.

There then follows a question seeking to classify the app for easy subsequent reference on a website of approved apps, then one on intended use. Next a request for a brief functional description is followed by a request for academic references for the principles underlying the functioning of the app.

After this comes questions on beneficiaries, cost, and whether if there are any subsequent payment requirements. An important question is who has funded the app, and whether any advertising is carried – in either case is there a conflict of interest with the app purpose?

The final section seeks information on how many users have tested the app? (if >one type of user, please give breakdown), if the app is covered by the EU voluntary code on mHealth app privacy, what platforms is the app available on, requests a brief technical description and asks what steps have been taken to validate the operation of the app on each platform.

6.3 **Risk assessment**

This section explains the purpose of the risk assessment, how it links to the overall assessment process, and the approach to be taken with apps in the 'grey zone'.

Although in theory any app that does not meet the definition of a medical device is low risk, the possibility remains that there will be some apps not defined as medical devices that pose at least moderate risks. This section therefore identifies risk levels, both as an important pointer for users, and also to determine the level of scrutiny to apply (see also 3.4. below).

In addition, for apps falling into the highest risk category and thus in the 'grey zone' referred to at 1.4. above, where "health apps" may create a hazardous situation, for the purposes of development scrutiny, documentation, verification, validation, the development process of the app would be expected to be similar to that used for medical devices.

The approach to risk assessment within these guidelines is still being worked on. The issues and approach being taken are further detailed at Annex A. However, the intention is to include text on the approach to be adopted in the next iteration of these guidelines.

Details of this section are still to be worked out. Other comments/questions posed include:

- What are the elements defining risk? E.g. should functionality be considered?
- Should not emulate the complexity of MD risk assessment
- Risk assessment should define which criteria are applicable – scrutiny questions should be risk sensitive. Should be a decision tree.

6.4 Assessment scrutiny

6.4.1 Assessment domains

This section explains the main assessment domains/criteria. Detailed scrutiny questions are proposed in Appendix 3 as one of the possible models for assessment scrutiny. The assessment domains and methodologies are under revision and will be further elaborated for the next iteration.

6.4.1.1 Usability & accessibility

This domain seeks to identify whether the app is usable by the people it is intended for, and whether it is accessible to those with limiting disabilities.

"Advice on **simple** usability tests from the WG would be greatly welcomed"

6.4.1.2 Desirability

This domain attempts to evaluate 'stickiness' – that vital factor without which people quickly tire of an app. It is extremely hard to define so doubtless the existing questions in the Annex can be improved on.

6.4.1.3 Credibility

This domain looks at the authority level of the app. This comprises the academic authority – for example whether the methodology is supported by appropriate papers, the standing of the developer, the degree to which the principles have been accepted by an appropriate authority (eg in the UK NICE's acceptance of eCBT (electronic cognitive behavioural therapy)), and perhaps the credibility of the specific algorithm used in the app if well known & tested.
In addition, some questions explore the frequency that the app is updated as medical knowledge develops, whether it notifies of changes made at the last update, and what the date was.

6.4.1.4 Transparency

This domain seeks to look through the app to explore who is behind it, who funded it, why, who holds any of the user's personal data, where it is held, and where the contents of the app came from.

6.4.1.5 Reliability

This domain covers the functioning of the device when in use under different circumstances.

6.4.1.6 Technical stability

This domain explores circumstances such as how the device reacts to incoming calls during use, loss of network, loss of power and such like.

6.4.1.7 Safety

This domain covers whether the app sets the user's expectations of safe operation appropriately and ensures that they take the necessary steps always to use the app safely.

6.4.1.8 Effectiveness

This domain seeks identify evidence of the effectiveness of the app at meeting its stated objectives.

6.4.1.9 Privacy & security

This domain will already be responded to if developers choose to adhere to the EU voluntary Code of Conduct on mHealth App Privacy. If they choose not to, a long series of questions explores this very important area.

6.4.2 Assessment methodology/tools

This section will explain the options for applying the main assessment criteria and how those could be tailored to the needs of different target groups

In order to utilise the guidelines to produce an assessment of the app, it is evaluated against the scrutiny questions. This involves a combination of a scoring system and of mandatory pass/fail questions; apps failing a mandatory question or not reaching a sufficiently high score are not recommended.

6.4.2.1 Scoring

This involves calculating a risk-related score for each app, with a cut-off below which the app is rejected, plus some questions for any of which the answer 'no' means rejection.

In more detail, and as an example of the many possible ways scoring can be done, columns are added to each of the above questions representing the different risk levels. Against each question in each column, there is then an indicator of *mandatory, desirable, additional,* or *not applicable*, as in the table below with just three questions:

	Low risk	Medium risk	High risk
8. If relevant, are there visual or vibration alternatives to warning sounds?	Not applicable	Additional	Desirable
30. Is colour coding uniform and aesthetically pleasing?	Not applicable	Additional	Additional
39. Has the app been validated by an appropriate group of specialised professionals, health organisation or scientific society?	Additional	Desirable	Mandatory

Confirming the answer yes to a question then either keeps the app in play if the indicator is *mandatory* (no would result in rejection), or scores 6 for *desirable* or an extra 4 (making 10 in total) for *additional*. A no to any *desirable* or *additional* question scores zero, as also does any answer where the risk level indicates *not applicable*.

So in the table above, if the app being assessed is high risk and the answer to Q39 is "No", then it is rejected immediately. If, however it is medium risk, it scores 6, and low risk it scores 4.

The total score for each section is then divided by the number of scored questions to give an overall score. Scores below a set level result in rejection of the app. There are endless versions of this possible. One option to consider is giving higher weighting for some questions & lower weighting for others – thus in the examples above, Q39 might be given a higher weight than Q30.

6.4.2.2 Certification

Either public or private bodies could be envisaged to carry out third party certification. These third party certifying bodies would be able to use the criteria and methodologies referred to in these guidelines for their own certification schemes.

Some private initiatives already exist, such as Kennis Centrum (Brussels), Medappcare (France) and Ourmobilehealth (UK).

For private initiatives, there should be either a "certification process for the certifiers" or at least random inspections of the certifiers (by official bodies) to ensure that the certifiers themselves adhere to appropriate standards. One of the reasons for mentioning this at all is the example of Happtique from 2013 (*http://mobihealthnews.com/28165/happtique-suspends-mobile-health-app-certification-program*). Relatively soon after starting their certification program, they had to suspend it due to serious flaws found in a few apps they had certified, although their catalog of criteria to be applied for certification was quite impressive and covered relevant aspects.

Table 1 Requirements for certifiers and the certification process[19]

Criterion	Explanation
Independence	There should be no reason (e.g. financially, involvement with other parties) to suspect that the certifier's independence during the evaluation process is influenced in any way.
Goals of the analysis	It should be made clear what the analysis includes (and what not). The goals of the analysis must be named explicitly.

[19] See "Albrecht, U.-V.: Kapitel 13. Orientierung für Nutzer von Gesundheits-Apps. In: Albrecht, U.-V. (Hrsg.), Chancen und Risiken von Gesundheits-Apps (CHARISMHA). Diminished Hochstetler Hannover, 2016, S. 282–300. urn: nbn:de: gbv:084-16040812052. http://www.digibib.tu-bs.de/?docid=60020"

Depth of the analysis	The depth of the analysis must be appropriate to be able to reach the aforementioned goals.
Methods of the analysis	The methods employed in the analysis phase must be appropriate. They should be state-of-the-art, their description should be publicly available and they must be legal.
Quality of the analysis methods	The methods employed need to make it possible to objectively, reliably and validly perform the evaluation.
Quality management	The analysis needs to conform to the appropriate standards of quality assurance.
Transparency	The certifiers need openly to communicate the steps they have taken in order to ensure adherence to the aforementioned aspects. Potential conflicts of interest need to be laid open. In addition, those who performed an external evaluation of the certification process should be named. The catalog of criteria and methods used for the evaluation should be documented and explained as well.

7 REFERENCES

[1] European Commission: Green Paper on Mobile Health. Go to: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147

[2] European Commission. *Summary Report on the Public Consultation on the Green Paper on Mobile Health.*

[3] BSI Standards Publication. "BS EN ISO 14971: 2012." *Medical devices—Application of risk management to medical devices*.

8 APPENDICES

8.1 Health evaluation and standardization bodies existing in EU

A review of all official Health evaluation and standardization bodies existing in EU member countries may be included in a subsequent iteration.

8.2 List of terms

This section lists terms used in this document - these terms and definitions are intended for use in this document only, and remain under review

mHealth	The provision of health services and information via mobile technologies such as mobile phones and Personal Digital Assistants (PDAs). www.who.int/goe/mobile_health/en/
Accessibility	Usability of a product, service, environment or facility by people with the widest range of capabilities
App	A software application; a self-contained software program designed to fulfil a particular purpose; an application, especially as downloaded by a user to a mobile device.
Citizens	For the purposes of this document only, the term 'citizen' is used to mean a person not being receiving treatment for a medical condition – this is to distinguish them from 'patients' who are receiving treatment, and carers who are delivering unpaid care to patients.
Credible	Able to be believed, reasonable to trust or believe, good enough to be effective
Desirable	Having good or pleasing qualities, worth having or getting (Merriam Webster
Effectiveness	Accuracy & completeness with which users achieve specific goals (ISO 9241 11) or: extent to which planned activities are realized and planned results achieved. (ISO 27000:2014)
Electronic Health Record	Information relevant to the wellness, health and healthcare of an individual, in computer-processable form and represented according to a standardized information model (ISO 18308:2011, 3.20)
Interoperability	The ability of two or more systems or components to exchange information and to use the information that has been exchanged. 'Functional' interoperability is the capability to reliably exchange information without error. 'Semantic' interoperability is the ability to interpret, and, therefore, to make effective use of the information so exchanged.
Harm	Injury or damage to the health of people, or damage to property or the

	environment (ISO/IEC Guide 51:2014, 3.1)
Health software	Software intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care (IEC 82304-1)
Medical device	Any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of: — diagnosis, prevention, monitoring, treatment or alleviation of disease, — diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap, — investigation, replacement or modification of the anatomy or of a physiological process, — control of conception, and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means (Directive 93/42/EEC and subsequent modifications – see also MEDDEV 2.1/6 and the text of this document for more detail)) Software intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care (IEC 82304-1)
Private	For the use of a single person or group: belonging to one person or group: not public
Research potential	Possibility to use the data collected by the app for research purposes (by app developers or third parties).
Reliability	The ability of an app to yield the same result on repeated trials. (Also: property of consistent intended behaviour and results (ISO 27000:2008)

Safety issue	An unexpected problem or malfunction that may affect a patient's health or cause or contribute to an injury, for example a blood glucose meter giving an incorrect blood glucose reading, leading to incorrect treatment. (adapted from Health Products Regulatory Authority https://www.hpra.ie/homepage/medical-devices/safety-information).
Secure	Free from risk of loss
Technical stability	A measure of whether the app starts up reliably and completes its task without crashing
Transparency	Managing and publishing information so that it is relevant and accessible and timely and accurate (http;//www.transparency-initiative.org)
Usability	The extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. (ISO 924111) or ISO 62366?
Validation	Confirmation, through the provision of objective evidence, that the requirements for a specific INTENDED USE or application have been fulfilled Note 1 to entry: The objective evidence needed for a VALIDATION is the result of a test or other form of determination such as performing alternative calculations or reviewing documents. Note 2 to entry: The word "validated" is used to designate the corresponding status. Note 3 to entry: The use conditions for VALIDATION can be real or simulated. (ISO 9000:2015, 3.8.13)

8.3 Assessment questionnaire

In this section a possible model for the app assessment process is proposed. Note that as the technology changes, so the detailed assessment will need to, to keep in pace. In places, comments made in response to consultation and which it has not yet been possible to process for inclusion are included in italics

8.3.1 Initial information gathering & validation: questions for the developer/supplier

Initial information gathering & validation: answers to be provided by the developer/supplier both for the certifying organisation and the intended end-user(s)

1. App name
2. Supplier
3. Developer (if different from (2))
4. Is the app CE certified as a medical device? (if 'yes' terminate assessment)
5. Is app primarily health or social care?
6. Which of the following categories does the app fit into (indicate all that apply):
    a. Patient/carer decision aids & self-management tools
    b. Clinical decision support tools for diagnosis/treatment recommendation
    c. Behaviour change apps – simple self-management tools
    d. Point-of-care diagnosis, monitoring or treatment aids
    e. Access & editing of EHRs
    f. Apps that control medical devices
    g. Communication apps – e.g. teleconsultation
    h. Apps providing documentation functionality &/or display a simple measurement
    i. Registries & vital events tracking – public health surveillance
    j. Simple calculators of on-personal information (e.g. BMI)
    k. Generic medical calculators

    (if it is a medical app and it does not fit any of the above, terminate assessment)
7. What is the intended use?
8. Please give brief functional description:
9. Please provide academic references for the principles underlying the functioning of the app:
10. Who are the principal beneficiary/ies? (indicate all that apply)
    a. Citizen
    b. Patient
        i. Novice
        ii. Expert
    c. Carer
    d. Professional user
    e. Healthcare provider

11. How much does it cost? (please put 0 if free) £
12. Are there subsequent payments required – please describe cost & frequency
13. Who has funded the app? Please give details
14. Is any advertising carried? If so is there a conflict of interest with the app purpose?
15. How many users have tested the app? (if >one type of user, please give breakdown)
16. Is the app covered by the EU voluntary code on mHealth app privacy?
17. What platforms is the app available on?
18. Please give a brief technical description:
19. What steps have been taken to validate the operation of the app on each platform?
20. What measures does the app take to provide security of user input and to authenticate the user?

Initial test

- Install/uninstall app on each available platform
- For each platform:
    - Is it easy for the intended user to understand?
    - Are the screens easy for the intended user to navigate?
    - Check basic operation: does it work as stated?

8.3.2 Risk assessment

Still being worked on
Patient safety
Data protection/technological risk

Comment "We agree with risk assessment globally. However, some examples would be reviewed. For example, accessing electronic health records might be high risk if there is a possibility of data modification/ data extraction, etc."

8.3.3 Scrutiny questions

8.3.3.1 Is the app usable & accessible?

NB – to be checked separately on every platform offered

Comments:

- *"Question 1: For registration, there are multiple questions asking about ease of use and if it's simple and open to use. We believe it should be considered that some applications may or may not require registration and, if required, the registration form the requirements to improve usability may depend on the information required. It seems the important questions here to include are: "Does the user have an option to register with the application?", "Does the app minimize the required information during the registration process?", or "Does the registration form provide appropriate error feedback if an error were to occur?". Question 9: We would like to suggest the following additional questions: Does the use have the option to select their language preference?; Is the regional language supported? Question 16: There*

may be some functions within the application that may not be used frequently (for example clear data, remove account, etc.) and therefore less important to be able to complete in three steps. Therefore, one may want to consider additional steps or limit this restriction to functions necessary for frequent/daily use of the app."

- *"followQ1 : Why does it matter if it is quick or slow once it's easy to use? Fast or slow is a subjective phenomenon for the user – a young user might be used to fast moving apps and expect that – an older user might only have little experience with apps and wants a slower experience to allow them to get familiar with the app. Q3: This question doesn't really make sense to me – technical jargon. Q5: This is a U/X issue – to be fair U/X and usability need a separate field….questions relating to these areas are littered throughout with structure. Q8: only an issue if not applicable or relevant to the app's functioning. Q11: again U/X stuff but placed amongst dissimilar questioning."*

1. Is the registration form easy to complete quickly?
2. Is the registration form format simple and open (unrestricted characters, numbers, uppercase, etc.)?
3. Do the registration fields incorporate support mechanisms to facilitate the process (pre-determined schedules, scroll down menu, descriptions, etc.)?
4. Are all the separate elements of the app (text, images, icons, buttons, etc.) identifiable and easy to use?
5. Are the colours of the elements appropriately contrasted with the background, (e.g. avoid similar red/green/brown colour intensities)?
6. Is the text easily readable (size, colour, font) & understandable?
7. Do controls, objects, icons and images have text tags to indicate their function or meaning?
8. If relevant, are there visual or vibration alternatives to warning sounds?
9. Does it accept & show all appropriate international characters correctly?
10. Does accessing the service (sending an email confirmation, validation of data access, etc.) happen quickly?
11. Does it fit within the standard interface of a typical mobile device?
12. Are the steps to follow clear; do they make sense?
13. Is there a navigation menu that provides direct access to all functionalities of the app?
14. Is navigation within the app easy & is it clear where in the app the user is?
15. Is it easy to go back to Home directly, and to return to the previous screen?
16. Can the user access any function in the app within three steps?
17. When inputting information, is it clear which fields remain to be completed, or are incorrect?
18. Is there access to self-help, video tutorials, guides and FAQ sections to help users?
19. Are there helplines (email, phone, contact form) readily available to resolve questions, problems or incidents?
20. Does the app developer provide appropriate guidance/training to healthcare professionals where necessary?
21. Do the required direct inputs (GPS, sensors, peripherals etc.) work properly?
22. Do the separate functions incorporated in the app load quickly, within a reasonable time?

23. Is the function of each element of the app obvious (clickable, static, drop down, selector, video, etc.)?
24. Are these elements in (22) appropriately positioned & sized to be intuitive, readable and effective to use?
25. Are the visual icons understandable; do they clearly reflect their associated functionality?
26. Is the keyboard used suitable for each type of entry?
27. Where there is a short timeout for screens, is the reading time sufficient?
28. Where the same app is available on different platforms, is the usability experience similar?

See Appendix 8.4 for usability questionnaires

8.3.3.2 Is the app desirable/appealing to use?

Comment "we could consider the following suggestion for the questions below: Question 31: An alternative could be " Is the use of color and icons easy to understand?" ; Question 33: To supplement this question: Does the user have the ability to control or set, the audiovisual content?; Is audiovisual content used appropriately?"

29. Is the visual identity of the logo in harmony with the visual pattern of the application?
30. Is colour coding uniform and aesthetically pleasing?
31. Are all the graphic elements (pictures, icons, buttons, etc.) used in the same way in all views, consistently?
32. Do the visual icons make the app attractive?
33. Are there any obvious usability problems? (e.g. a button on a device too small to be pressed)
34. Is audiovisual and textual content combined in a balanced & appealing way?
35. Is the color scheme is balanced, not using any particular colour excessively?
36. Is the application properly localised for each country in which it is to be used; is the language/choice of languages appropriate, the currency correct etc.?
37. Is each language used correctly, with no spelling or grammatical errors?
38. Does it follow the interface user guidelines of the operating system?
39. Does the app avoid stereotypes & stigmatization?

8.3.3.3 Is the app credible?

Comments "Questions 40---52 should probably be summarized under a single category and possibly simplified somewhat, as the points currently listed under "credibility" can also be understood as important aspects of transparently providing information about an app and its background."
Comment "The first question in this section could address one of the open questions around the validation and evidence to create "content". This question is potentially important for the overall approach and it perhaps need some further discussion as to whether it should form a key component of the methodology/risk assessment."

40. Has the app been validated by an appropriate group of specialised professionals, health organisation or scientific society?
41. Has the app content been similarly validated?
42. Does it Indicate the sources of information of the contents listed?

43. Does it provide references to the scientific evidence used to ensure content quality?
44. Is there appropriate information provided about the authors of the app content to generate credibility and provide quality assurance?
45. Does it indicate how often the app's content is reviewed/updated?
46. Does it indicate the last review date?
47. Does it notify changes/modifications made at the last update?

8.3.3.4 Is the app transparent?

48. Does it use simple and understandable language, with clear and short messages, adapted to the target user profile in terms of style and comprehension level?
49. Does it clearly identify who holds any personal data?
50. Does it clearly identify any organisations other than the supplier who have collaborated on the development of the app?
51. Is there concise information on the procedures used to select the app's contents?
52. Does it clearly identify who is/are responsible for the contents of the app?
53. Is there sufficient information on the funding sources, promotion and sponsorship of the app?
54. Is the supplier's cookie policy stated, and clear?

8.3.3.5 Is the app reliable?

Comments "Question 60: Many apps do not support orientation changes. If applicable, this should behave correctly. Question 62: In some instances, for security purposes, it may be important for the app to close or timeout if the user leaves the app for a period of time. Question 61: What is meant by : appropriately" – needs a clear definition. Behavior could also be defined as effectiveness."

55. If relevant, does the language change work and is adjusted properly to the interface and contents?
56. Is it able to properly handle problems with the device and errors of precision, hardware, or from an inadequate use?
57. Does it Inform the user if it requires a long boot up time (default < than 5 seconds)?
58. Dies it notify the user where there is a lengthy operation?
59. Does it allow the user to cancel lengthy operations?
60. Does it notify the user in the case of an external interruption (e.g. loss of network connectivity, database problem)?
61. Does it notify the user in the case of a low bandwidth network?
62. Does it indicate which mobile platform it will work with satisfactorily (according to the operating system, screen resolution, etc.)?
63. Does the screen refresh work properly on the device, including orientation changes, pop-up menus, pop-ups, etc.?
64. Is the information architecture of the application symmetrical, harmonious and proportionate?
65. If the user accepts an incoming call while the application is running, is it possible to return to the same point at the end of the call?

66. Does it behave appropriately in real conditions outside the laboratory?

8.3.3.6 Is the app technically stable?

67. Does it reject & warn of clearly erroneous data inputs (formats, ranges, etc.)?
68. Is it resilient to abrupt failure during use (locks, etc.)?
69. Is it resilient to changes in other apps, and to external interrupts (incoming call, receiving a message, etc.)?
70. Does it always only consume acceptable levels of resource: battery, CPU, memory, etc.?
71. Does it avoid ever using excessive network resources?
72. Does the app install and uninstall properly?
73. Does it performance remain at the same level in spite of prolonged usage?
74. When the application runs in the background does it do so without affecting other applications or system functions, unless it is specifically designed to do so?
75. Are the database resources appropriately shared between the application and the operating system?
76. Is the application speed acceptable for the purpose required without modifying the user experience or becoming uncontrollable?
77. Does it fail under high load or demand service?
78. Is it able to continue working correctly if repeatedly suspended and resumed?
79. Is it able to continue working correctly if network availability is intermittent?
80. Can it operate (albeit at reduced functionality) in airplane mode, or otherwise with loss of network connectivity?
81. If it requires regular interaction with the user, does it resume successfully from a suspended state at the agreed time/date of each diaried interaction?

8.3.3.7 Is the app safe?

82. Does it advise that the app is not intended to replace relevant professional services?
83. Does it warn of the possible risks if the app is misused?
84. Does it warn of possible adverse risks caused by the use of the app?
85. Does it provide appropriate guidance if it handles information/data about minors?
86. Does it provide appropriate guidance if it handles information/data about a dependent person who is not the user?
87. Are there persistent relevant warnings, until the user provides important information or accepts output information?

8.3.3.8 Is the app effective?

Comments

- *"Need to be clear here. Ideally based on best clinical evidence (guidance) but of course that may vary for member states so would have to be for that country."*
- *"Answers to questions 88 / 94 / 95 couldn't be "yes/no". On which basis is the value / benefits evaluated?"*
- *Comment "Some points can only be addressed by a study including prospective evidence (or perhaps via user surveys), therefore, it would be helpful if guidance were provided as to how and what level of evidence is expected to address the points. We*

suggest that the sections/items in the list of topics to be scrutinised are prioritized. Question 88: Or by offering a service that was not previously available? Question 89: What about changing behavior and improving lifestyle? Question 92: Or how to change their behavior to benefit. Question 93: We are not sure how developers can objectively assess this part. Question 94: Are you asking for studies of effectiveness for outcomes? What do you consider to be evidence? What is a real benefit is another type of benefit? This item is very vague and is crucially important to review. Question 95: peer-reviewed evidence? What is acceptable for you? The same standards used to assess benefit for a medicine, a medical device? This needs much more clarity." (Note the question numbers in the above comments have been amended to reflect the changes in question numbers).

88. Does the promoter of the app offer good justification that the functions incorporated provide value to users, in terms of saving time/money, improving information or better health/care?
89. Is it clear who the targeted users are for the app?
90. Is it clear what the intended benefits are to those users?
91. Are the contents and functions offered of potential interest for the user profile to which the app is addressed?
92. Is it clear how those users will need to change the care pathway they participate in (if professional), or lifestyle, in order best to benefit from the app?
93. Is this change (in (4)) realistically achievable?
94. Does it evidence real benefit to users?
95. Has that benefit been evidenced acceptably?

8.3.3.9 Is the app private & secure?

Note for this section, preferably, we could merely specify compliance with the EU Privacy Code of Conduct for mHealth apps.

96. Is it clear if user registration is necessary for full operation?
97. Is it clear to the user what user data is collected by the app and is specific consent to do this requested?
98. Is it clear to the user why consent is being requested for the data that is being collected, by whom and for what purpose?
99. Is it clear to the user whether the data collector will do anything else with the user's personally identifiable data?
100. Is it clear to the user whether the data collector will do anything else with the user's data appropriately anonymised?
101. If third parties have access to data, is this in an acceptable manner, with user approval only?
102. Does it describe the app's maintenance policy for storage & deletion of data provided by the user?
103. Are user data authentication processes acceptable?
104. Does it describe the rights of access, rectification, cancellation or removal of personal data?

105. Can it be confirmed that passwords are not stored directly on the device?
106. Does it manage access to the user's personal information appropriately, with user approval?
107. Are the permissions requested to access the different services of the device clearly described?
108. Are the communication channels used appropriately encrypted?
109. Are the mechanisms of authorisation and authentication adequate?
110. Is the app source code inaccessible & unalterable by the user?
111. Does the app comply with the GDPR principle of *data minimisation*?
112. Does the app comply with the GDPR principle of *data protection by default*?
113. Does the app comply with the GDPR principle of *data protection by design*?
114. If the app is able to write personal information to a patient's electronic health record does it comply fully with the EHR provider's interoperability and security requirements and does it request specific consent from the EHR owner to do this[20]?

[20] Note that in some MSs such as the UK, the owner of the data is not the patient/citizen.

8.4 Usability

8.4.1 The System Usability Scale

Participante ID: _____ Lugar: _____ Fecha: ___/___/___

System Usability Scale

Instrucciones: Para cada una de las siguientes afirmaciones, marque el cuadro que mejor describa hoy sus reacciones ante el uso del sistema.

		En total desacuerdo				Totalmente de acuerdo
1.	Creo que me gustará utilizar con frecuencia este sistema.	☐	☐	☐	☐	☐
2.	El sistema me pareció innecesariamente complejo.	☐	☐	☐	☐	☐
3.	El sistema me pareció fácil de utilizar	☐	☐	☐	☐	☐
4.	Creo que necesitaría del apoyo de un experto para utilizar el sistema.	☐	☐	☐	☐	☐
5.	Encontré las diversas posibilidades del sistema bastante bien integradas.	☐	☐	☐	☐	☐
6.	Pensé que había demasiada inconsistencia en el sistema.	☐	☐	☐	☐	☐
7.	Creo que la mayoría de las personas aprenderían rápidamente a utilizar el sistema.	☐	☐	☐	☐	☐
8.	Me pareció que el sistema era complicado e incómodo de utilizar.	☐	☐	☐	☐	☐
9.	Me sentí muy confiado en el manejo del sistema	☐	☐	☐	☐	☐
10.	Necesito aprender muchas cosas antes de manejarme en el sistema.	☐	☐	☐	☐	☐

Por favor, proporcione cualquier comentario acerca de este sistema:

URL for the above: http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html.

Other scales include:

QUIS: Questionnaire for user interaction satisfaction. http://www.lap.umd.edu/quis/

TAM: The Technology Acceptance Model.
https://pdfs.semanticscholar.org/3969/e582e68e418a2b79c604cd35d5d81de9b35d.pdf

8.5 Definition of Interoperability

This appendix explores the definition of Semantic Interoperability in the context of mHealth, i.e. in the various possible areas where data between an app and another app is exchanged and the necessity thereby of a common structure & common semantics.

The HL7 definition is as adopted by the working group in Appendix 9.2 as follows:

Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

- '**Functional'** interoperability is the capability to reliably exchange information without error.
- '**Semantic**' interoperability is the ability to interpret, and, therefore, to make effective use of the information so exchanged.

8.5.1 Needs for exchange

In order to achieve semantic interoperability, we need two things:

- "**Structural**" interoperability is an intermediate level that defines the structure or format of data exchange (i.e., the message format standards) where there is uniform movement of healthcare data from one system to another such that the clinical or operational purpose and meaning of the data is preserved and unaltered. Structural interoperability defines the syntax of the data exchange. It ensures that data exchanges between information technology systems can be interpreted at the data field level.
    - Possible candidates for data exchange:
        - HL7 FHIR
        - CCR
        - C-CDA
- "**Semantic**" interoperability provides interoperability at the highest level, which is the ability of two or more systems or elements to exchange information and to use the information that has been exchanged. Semantic interoperability takes advantage of both the structuring of the data exchange and the codification of the data including vocabulary so that the receiving information technology systems can interpret the data. This level of interoperability supports the electronic exchange of patient summary information among caregivers and other authorized parties via potentially disparate electronic health record (EHR) systems and other systems to improve quality, safety, efficiency, and efficacy of healthcare delivery.
    - Possible candidates for SI operations:

- Terminologies & Classification systems like SNOMED CT, LOINC, ICD-10
- The adaption of vocabularies in *Detailed Clinical Models (DCM)*: a DCM is according to ISO TS 13972[21] a specification of health content with explanation of medical knowledge, an information model with interrelated concepts and context presented in a standardized, reusable way, with mappings to terminology and classification systems in order to assess the quality of the information in the DCM.

8.5.2 Areas of Semantic Interoperability

In the figure below the areas where Semantic Interoperability should be achieved are marked in red text, but we like to see SI in the orange text as well.

[21] ISO TS 13972:2015. Technical Specification. Health informatics — Detailed clinical models, characteristics and processes. Geneva, International Organization for Standardization, Technical Committee 215 Health Informatics. www.iso.org

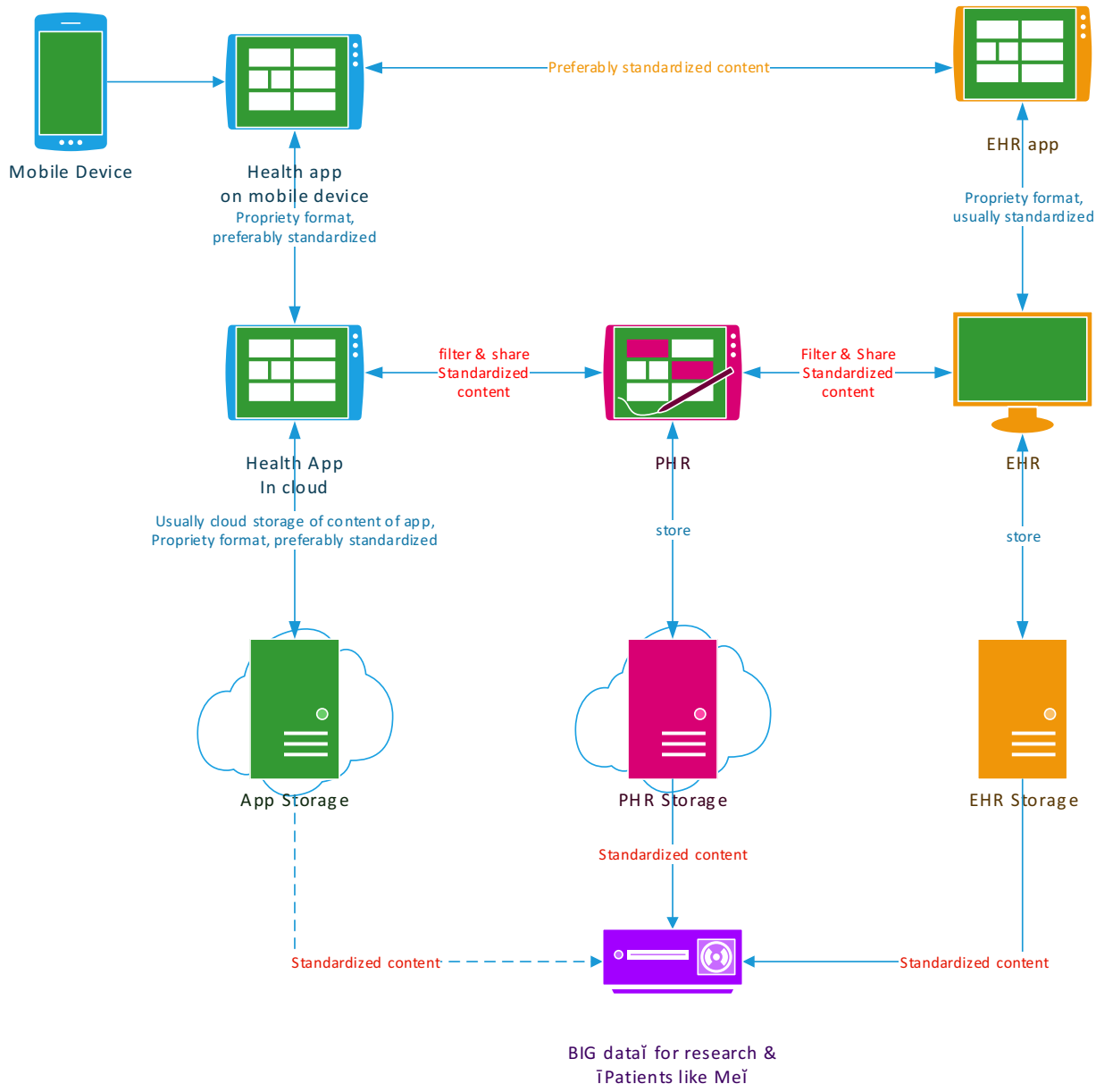


Figure 1: areas of SI in mHealth[22]

Explanation of figure 1

- A PHR is a Personal Health Record system
- An EHR is an Electronic Health Record system

[22] Legend: green is mobile device/app environment, pink is PHR environment, orange is EHR environment, purple is "Big Data" environment

- Pharmacy, GP systems and other parties with whom data can (and should) be collected and exchanged are left out of the picture but follow the same pattern as a PHR.
- A health app resides on a mobile device and collects data that is quite often shared with an external app residing somewhere in a cloud
- The data the health app collects can be shared with a PHR.
- The PHR data which collect data from various sources, including different EHR's, GP systems, pharmacies and what have you. It needs to be able to exchange data with these aforementioned systems in a sensible & interoperable way.
- EHR provider sometimes create apps as an extension of their EHR. The app resides on a mobile device and communicates uniquely with the EHR system.
- App data, PHR data & EHR data can be shared with big data like solutions.
- Some data will need to be filtered in order to avoid data-waterboarding, but filtering is left out of this scope since it's not dependent on SI, but a problem on its own.

8.6 **Case Studies**

(Some 3-5 studies are expected to be included in subsequent iterations, when provided by Members of the Working Group or from other sources)

LIST OF ANNEXES:

An Overview of mHealth App Evaluation Criteria