Teknisk specifikation
SIS-CEN ISO/TS 82304-2:2021

Programvara för hälsoappar – Del 2: Kvalitet och tillförlitlighet (ISO/TS 82304-2:2021)

Health software – Part 2: Health and wellness apps – Quality and reliability (ISO/TS 82304-2:2021)

sis Svenska Institutet för Standarder

Språk: engelska/English
Utgåva: 1

Svenska
Institutet för
Standarder

Det här dokumentet kan hjälpa dig att effektivisera och kvalitetssäkra ditt arbete. SIS har fler tjänster att erbjuda dig för att underlätta tillämpningen av standardiseringsprodukter i din verksamhet.

SIS Abonnemang
Snabb och enkel åtkomst till gällande standardiseringsprodukt med SIS Abonnemang, en prenumerationstjänst genom vilken din organisation får tillgång till all världens standardiseringsprodukter, senaste uppdateringarna och där hela din organisation kan ta del av innehållet i prenumerationen.

Utbildning, event och publikationer
Vi erbjuder även utbildningar, rådgivning och event kring våra mest sålda standardiseringsprodukter och frågor kopplade till utveckling av standardiseringsprodukter. Vi ger också ut handböcker som underlättar ditt arbete med att använda en specifik standardiseringsprodukt.

Vill du delta i ett standardiseringsprojekt?
Genom att delta som expert i någon av SIS 300 tekniska kommittéer inom CEN (europeisk standardisering) och/eller ISO (internationell standardisering) har du möjlighet att påverka standardiseringsarbetet i frågor som är viktiga för din organisation. Välkommen att kontakta SIS för att få veta mer!

Kontakt
Skriv till kundservice@sis.se, besök sis.se eller ring 08 - 555 523 10

Upplysningar om sakinnehållet i standardiseringsprodukten lämnas av Svenska institutet för standarder, telefon 08 - 555 520 00. Standardiseringsprodukter kan beställas hos SIS som även lämnar allmänna upplysningar om svensk och utländsk standardiseringsprodukt.

Dokumentet är framtaget av kommittén för Hälso- och sjukvårdsinformatik, SIS/TK 334.

Har du synpunkter på innehållet i den här standardiseringsprodukten, vill du delta i ett kommande revideringsarbete eller vara med och ta fram andra standardiseringsprodukter inom området? Gå in på www.sis.se - där hittar du mer information.

Fastställd: 2021-08-16
ICS: 35.080;35.240.80

Denna tekniska specifikation är inte en svensk standard. Detta dokument innehåller den engelska språkversionen av CEN ISO/TS 82304-2:2021.

This Technical Specification is not a Swedish Standard. This document contains the English language version of CEN ISO/TS 82304-2:2021.

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN ISO/TS 82304-2

August 2021

ICS 35.080; 35.240.80

English Version

Health software - Part 2: Health and wellness apps - Quality and reliability (ISO/TS 82304-2:2021)

Logiciels de santé - Partie 2: Applications de santé et de bien-être - Critères de qualité tout au long du cycle de vie - Code de pratique (ISO/TS 82304-2:2021)

Gesundheits- und Wellness-Apps - Qualitätskriterien während des gesamten Lebenszyklus - Verhaltenskodex (ISO/TS 82304-2:2021)

This Technical Specification (CEN/TS) was approved by CEN on 28 June 2021 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN ISO/TS 82304-2:2021 E

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 215, *Health informatics*, in collaboration with Technical Committee IEC/TC 62, *Electrical equipment in medical practice*, Subcommittee SC 62A, *Common aspects of electrical equipment used in medical practice*, and with the European Committee for Standardization (CEN) Technical Committee CEN/TC 251, *Health informatics*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

A list of all parts in the ISO 82304 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

European foreword

This document (CEN ISO/TS 82304-2:2021) has been prepared by Technical Committee ISO/TC 215 "Health informatics" in collaboration with Technical Committee CEN/TC 251 “Health informatics” the secretariat of which is held by NEN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body/national committee. A complete listing of these bodies can be found on the CEN websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Endorsement notice

The text of ISO/TS 82304-2:2021 has been approved by CEN as CEN ISO/TS 82304-2:2021 without any modification.

Introduction

Context

Health and wellness apps are a fast-growing market, and there are now hundreds of thousands, with the most popular of these having many millions of downloads each. Some of these apps fall under medical devices regulations, most do not. These apps are often promoted directly to consumers through app stores without going through any formal evaluation. The apps often collect sensitive personal information yet do not have appropriate privacy controls, and provide advice on topics such as fertility, diet or activity that are not supported by any evidence. There are widespread concerns about the risks involved. At the same time, health apps that have proven to be effective and add to quality of life and even length of life, are not necessarily adopted at scale and reimbursed.

Many health organizations have projects to evaluate, endorse and procure apps that meet locally defined requirements. These activities are important for any app manufacturer who want to promote or sell their product to or through providers of health and wellness services, as providers want the reassurance that the apps they recommend to patients will be safe, reliable and effective. However, the cost of responding to different extensive sets of criteria and different evaluation regimes in each country, organization, or region is a barrier for app manufacturers wanting to make their products available in multiple markets. It is also a problem for those evaluating apps and maintaining libraries of health and wellness apps. They can miss out on products that effectively address health issues and health system inefficiencies, do not benefit from economies of scale of others evaluating the same apps and different evaluations can contradict one another, causing further confusion instead of trust. Because of the time investment involved, the vast majority of apps are not evaluated at all, although top 10 lists suggest otherwise.

There are several International Standards on health software related to product safety and lifecycle processes that are applicable to all health software, including health apps. This document provides quality requirements and health app quality labels as ways for app manufacturers and app assessment organizations to communicate the quality and reliability of health apps.

The working practice within app development is to deliver a focused piece of functionality, building on an existing platform - often with a small team doing the work who can be unfamiliar with health software development. This document includes Annex D to provide guidance specific to this community.

A vibrant transparent market for health apps will benefit individuals and programs across the world that are addressing issues such as aging population, unhealthy lifestyles, chronic diseases, affordability of or constrained budgets for health and care, unequal quality and access to health services, and shortages in health professionals.

This document makes no attempt to determine whether a health app is or should be regulated.

Development methodology

The quality requirements (Clause 5) and health app quality score calculation method (Annex B) have been developed with a Delphi consensus study. Further input was gathered with surveys, interviews, and review of existing standards and health app assessment frameworks. The health app quality label (Annex A) has been inspired by the EU energy label that is also used in more than 50 countries outside Europe, the Nutriscore and the FDA over-the-counter medicine label. Think-aloud testing of the health app quality label with people with low health literacy in the Netherlands and subsequently Egypt and Mexico was used to ensure adequate understanding in different contexts.

Outline

This document defines a set of questions and supporting evidence that can be used to clarify the quality and reliability of a health app. A health app quality label is defined to summarize this information in a visually appealing way.

The questions and evidence are listed under the following headings taking into account the need to be understood by those with low health literacy:

- Product information;
- Healthy and safe;
- Easy to use;
- Secure data;
- Robust build.

This document provides requirements for the specification for the health app quality label in Annex A, and a calculation method in Annex B to generate the quality score information that is displayed on the label.

This document also contains annexes covering the following:

- Annex C: the rationale for the scope of this document and content;
- Annex D: a walk through the relevant international health software products and process standards, providing recommendations and explanations, where appropriate, to help those developing or evaluating health and wellness apps to understand how the standards can be applied;
- Annex E: an example of how a profile of this document can be defined for the assessment of contact tracing apps. Similar profiles can be produced for other specific use cases;
- Annex F: ethical considerations for app manufacturers and evaluators to take into account;
- Annex G: a range of ways that this document can be used by different stakeholders throughout the lifecycle of a health app.

Health software —

Part 2: Health and wellness apps—Quality and reliability

1 Scope

This document provides quality requirements for health apps and defines a health app quality label in order to visualize the quality and reliability of health apps.

This document is applicable to health apps, which are a special form of health software. It covers the entire life cycle of health apps.

This document is intended for use by app manufacturers as well as app assessment organizations in order to communicate the quality and reliability of a health app. Consumers, patients, carers, health care professionals and their organizations, health authorities, health insurers and the wider public can use the health app quality label and report when recommending or selecting a health app for use, or for adoption in care guidelines, care pathways and care contracts.

NOTE 1 Health apps can be subject to national legislation, such as for medical devices.

NOTE 2 See Annex C for additional details on the scope.

Outside the scope of this document are guidelines to comply to the medical device regulation.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1 General terms

3.1.1
accessibility
extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of user needs, characteristics and capabilities to achieve identified goals in identified contexts of use

Note 1 to entry: Context of use includes direct use or use supported by assistive technologies.

[SOURCE: ISO 9241-11:2018, 3.2.2]

3.1.2
effectiveness
ability to produce the intended result

[SOURCE: ISO 81001-1:2021, 3.2.5]

3.1.3
efficiency
resources used in relation to the results achieved

Note 1 to entry: Typical resources include time, human effort, costs and materials.

[SOURCE: ISO 9241-11:2018, 3.1.13]

3.1.4
evidence
directly measurable characteristics of a process and/or product that represent objective, demonstrable proof that a specific activity satisfied a specified requirement

[SOURCE: ISO/IEC 21827:2008, 3.19]

3.1.5
health
state of complete physical, mental and social well-being and not merely the absence of disease or infirmity

[SOURCE: WHO 1948[53]]

3.1.6
health benefit
positive impact or desirable outcome of the use of health software on the health of an individual

3.1.7
health intervention
act performed for, with or on behalf of a person or population whose purpose is to assess, improve, maintain, promote or modify health, functioning or health conditions

[SOURCE: WHO 1948[53]]

3.1.8
health issue
representation of an issue related to the health of a subject of care as identified by one or more healthcare actors

Note 1 to entry: According to this definition, a health issue can correspond to a health problem, a disease, an illness or another kind of health condition.

EXAMPLE A loss of weight, a heart attack, a drug addiction, an injury, dermatitis.

[SOURCE: ISO 13940:2015]

3.1.9
health need
deficit in the current health state compared to aspects of a desired future health state

[SOURCE: ISO 13940:2015]

3.1.10
intended use
intended purpose
health-related use for which a product, process or service is intended according to the specifications, instructions and information provided by the manufacturer

Note 1 to entry: The intended health benefit, patient population, part of the body or type of tissue interacted with, user profile, use environment, and operating principle are typical elements of the intended use.

Note 2 to entry: A health app has an intended use irrespective of whether it is a medical device. A concept of "intended use" is used in a more restrictive sense in some medical device regulations.

[SOURCE: ISO/IEC Guide 63:2019, 3.4, modified — Note 2 to entry added, "intended purpose added" as a preferred term.]

3.1.11
intended users
group(s) of people for whom a product is designed

Note 1 to entry: In many cases the actual user population is different from that originally intended by the manufacturer. The intended user group is based on realistic estimations of who the actual users of the product will be.

[SOURCE: ISO 20282-1:2006, 3.12]

3.1.12
interoperability
ability of two or more systems or components to exchange information and to use the information that has been exchanged

[SOURCE: IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries. New York: Institute of Electrical and Electronics Engineers; 1990]

3.1.13
joint PII controller
PII controller that determines the purposes and means of the processing of PII jointly with one or more other PII controllers

[SOURCE: ISO/IEC 27701:2019, 3.1]

3.1.14
medical device
instrument, apparatus, implement, machine, appliance, implant, reagent for in vitro use, software, material or other similar or related article, intended by the manufacturer to be used, alone or in combination, for human beings, for one of more of the specific medical purpose(s) of

- diagnosis, prevention, monitoring, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of or compensation for an injury,
- investigation, replacement, modification, or support of the anatomy or of a physiological process,
- supporting or sustaining life,
- control of conception,
- disinfection of medical devices,
- providing information by means of in vitro examination of specimens derived from the human body,

and does not achieve its primary intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such means

Note 1 to entry: Products that can be considered to be medical devices in some jurisdictions but not in others include

- disinfection substances,
- aids for persons with disabilities,
- devices incorporating animal and/or human tissues, and
- devices for in-vitro fertilization or assisted reproductive technologies.

[SOURCE: ISO/IEC Guide 63:2019, 3.7]

3.1.15
personally identifiable information
PII
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9, modified — Note to entry removed.]

3.1.16
privacy
freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual

[SOURCE: ISO/TS 27790:2009, 3.56]

3.1.17
processing of PII
operation or set of operations performed upon Personally Identifiable Information (PII)

Note 1 to entry: Examples of processing operations of PII include, but are not limited to, the collection, storage, alteration, retrieval, consultation, disclosure, anonymization, pseudonymization, dissemination or otherwise making available, deletion or destruction of PII.

[SOURCE: ISO/IEC 29100:2011, 2.23]

3.1.18
quality
degree to which a set of inherent characteristics of an object fulfils requirements

[SOURCE: ISO 9000:2015, 3.6.2, modified — Notes to entry removed.]

3.1.19
reliability
ability of a device or a system to perform its intended function under given conditions of use for a specified period of time or number of cycles

[SOURCE: ISO 14907-1:2020, 3.23]

3.1.20
safety
freedom from unacceptable risk

[SOURCE: ISO/IEC Guide 63:2019, 3.16]

3.1.21
satisfaction
extent to which the user's physical, cognitive and emotional responses that result from the use of a system, product or service meet the user’s needs and expectations

Note 1 to entry: Satisfaction includes the extent to which the user experience that results from actual use meets the user’s needs and expectations.

Note 2 to entry: Anticipated use can influence satisfaction with actual use.

[SOURCE: ISO 9241-11:2018, 3.1.14]

3.1.22
security
condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

Note 1 to entry: Hostile acts or influences could be intentional or unintentional.

3.1.23
usability
extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use

[SOURCE: ISO 9241-210:2019, 3.13]

3.1.24
user
person who interacts with a system, product or service

Note 1 to entry: Users of a system, product or service include people who operate the system, people who make use of the output of the system and people who support the system (including providing maintenance and training).

[SOURCE: ISO 9241-11:2018, 3.1.7]

3.1.25
use error
reasonably foreseeable misuse

3.2 Terms relating to apps

3.2.1
app
software application that can be executed (run) on a computing platform

Note 1 to entry: Apps were initially established as a category of software developed to run on mobile platforms for a single or limited number of purposes. However, the distinction between apps and other software applications has become less clear as a wider range of computing platforms are marketed as supporting apps and app repositories, and as apps with a wider range of functions are developed.

Note 2 to entry: An example is a software application running on a handheld commercial off-the shelf computing platform, with or without wireless connectivity, or a web-based software application that is tailored to a mobile platform but is executed on a server.

[SOURCE: BS PAS 277:2015, 3.1.1, modified — 'and is typically a small application run or accessed on mobile devices' removed from the definition, Note 2 to entry modified.]

3.2.2
app assessment organization
organization that evaluates apps

Note 1 to entry: This can be done to inform the purchasing or recommendation of an app, or as part of a certification program.

3.2.3
health app
health and wellness app
app intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care

[SOURCE: IEC 82304-1:2016 3.6, modified — Changed 'software' to 'app' in term and definition, 'health and wellness app' was added as a term, notes to entry deleted.]

3.2.4
health software
software intended to be used specifically for managing, maintaining or improving health of individual persons, or the delivery of care

Note 1 to entry: Health software fully includes what is considered software as a medical device.

Note 2 to entry: The scope of IEC 82304-1 refers to the subset of health software that is intended to run on general computing platforms.

[SOURCE: IEC 82304-1:2016, 3.6]

3.2.5
health software product
combination of health software and accompanying documentation

[SOURCE: IEC 82304-1:2016, 3.7, modified — 'documents' changed to 'documentation'.]

3.2.6
manufacturer
app manufacturer
natural or legal person with responsibility for design and/or manufacture of a health app with the intention of making the health app available for use, under their own name; whether or not such a health app is designed and/or manufactured by that natural or legal person themselves or on their behalf by (an)other natural or legal person(s)

Note 1 to entry: This ‘natural or legal person’ has ultimate legal responsibility for ensuring compliance with all applicable regulatory requirements for the health app in the countries or jurisdictions where it is intended to be made available or sold, unless this responsibility is specifically imposed on another person by the Regulatory Authority within that jurisdiction.

Note 2 to entry: ‘Design and/or manufacture’ can include specification development, production, assembly, processing, packaging, repackaging, labelling, relabelling, installation, or remanufacturing of a health app, or putting a collection of apps, and possibly other products, together for a health purpose.

Note 3 to entry: Any natural or legal person who assembles or adapts a health app that has already been supplied by another person for an individual subject of care or wellbeing, in accordance with the instructions for use, is not the app manufacturer, provided the assembly or adaptation does not change the intended use of the health app.

Note 4 to entry: Any natural or legal person who changes the intended use of, or modifies, a health app without acting on behalf of the original app manufacturer and who makes it available for use under their own name, should be considered the app manufacturer of the modified health app.

Note 5 to entry: An authorized representative, distributor or importer who only adds its own address and contact details to the health app or the packaging, without covering or changing the existing labelling, is not considered an app manufacturer.

[SOURCE: ISO/IEC Guide 63:2019, 3.6, modified — 'medical device' replaced with 'health app', 'app manufacturer' was added as a term, Notes 2 and 7 to entry deleted.]

3.2.7
session management
process of securing repeated access of a user to the health app, once authentication has been established, e.g. automatic logout after a certain time of inactivity

3.2.8
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 can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for validation are sometimes called a qualification process.

Note 3 to entry: The word "validated" is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.13, modified — Notes 2 and 3 to entry have been changed.]

3.2.9
verification
confirmation through the provision of objective evidence, that specified requirements have been fulfilled

Note 1 to entry: The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents.

Note 2 to entry: The activities carried out for verification are sometimes called a qualification process.

Note 3 to entry: The word "verified" is used to designate the corresponding status.

[SOURCE: ISO 9000:2015, 3.8.12]

3.3 Terms relating to risk management

3.3.1
authentication
process of validating a user or process to verify that the user or process is not a counterfeit

Note 1 to entry: Methods to validate the identity of the user of a health app may include password, Face ID, Touch ID, Oauth2.

[SOURCE: ISO/IEC/IEEE 9945:2009+Cor 1:2013+Cor 2:2017, 3.31, modified — Note to entry added.]

3.3.2
authorization
process of verifying that a user or process has permission to use a resource in the manner requested

Note 1 to entry: To ensure security, the user or process would also need to be authenticated before granting access

[SOURCE: ISO/IEC/IEEE 9945:2009+Cor 1:2013+Cor 2:2017, 3.32, modified — Second sentence in the definition changed to Note to entry.]

3.3.3
harm
injury or damage to the health of people or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

3.3.4
hazard
potential source of harm

[SOURCE: ISO/IEC Guide 51:2014, 3.2]

3.3.5
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014, 3.9]

3.3.6
risk analysis
systematic use of available information to identify hazards and to estimate the risk

[SOURCE: ISO/IEC Guide 51:2014, 3.10]

3.3.7
risk control
process in which decisions are made and measures implemented by which risks are reduced to, and maintained within, specified levels

[SOURCE: ISO/IEC Guide 63: 2019, 3.12]

3.3.8
residual risk
risk remaining after risk control measures have been implemented

[SOURCE: ISO/IEC Guide 63: 2019, 3.9]

4 Health app assessment process

4.1 Quality assessment

The health app manufacturer shall provide answers to the questions defined in Clause 5 in order to conform with this document. The evidence defined in Clause 5 for each question is provided by the health app manufacturer to an app assessment organization.

Where the health app is available on different platforms and the answers to the questions defined in Clause 5 are not the same for each platform, then a separate set of answers shall be provided for the health app for each platform.

Annex G describes potential uses of this document for stakeholders including app assessment organizations.

4.2 Quality requirements

The quality requirement questions in Clause 5 are grouped under five sections, with ‘Product information’ and four aspects of quality:

- Healthy and safe;
- Easy to use;
- Secure data;
- Robust build.

The questions have different purposes that are indicated using the subheading ‘PURPOSE’:

- Label content: Question to capture information to be provided in the health app quality label. The answer does not impact the health app score;
- Requirements level: Question to establish which subsequent questions are to be asked;
- Colour coding: Question to establish a quality and reliability aspect of the health app. The answer affects the health app score (in Annex B) and colour in a particular quality aspect on the health app quality label (in Annex A). The colour coding questions shall be answered with ‘Yes’ or ‘No’ or, in some cases, ‘Not applicable’. This way, the answers can be used to derive scores for the health app quality label;
- Filtering: Question to help app repository users to search and filter for relevant apps in a consistent way. The answer does not impact the health app score;
- App assessment: Questions to enable app evaluation. The response is provided to the app assessment organization only.

4.3 Health app quality report

The set of answers to the ‘Label content’, ‘Requirements level’, ‘Colour coding’ and ‘Filtering’ questions, excluding evidence provided to enable app assessment, form the health app quality report.

The health app quality report can be made available to potential customers and users of the health app to enable informed decision making.

4.4 Health app quality evidence pack

The health app quality evidence pack is the set of evidence as specified in Clause 5 that shall be made available to health app assessment organizations to enable the assessment process.

4.5 Health app quality label

The health app quality label enables consumers, patients, carers, health professionals, payers such as health insurers and health authorities to make informed decisions. The health app quality label enhances transparency concerning the quality and reliability of a health app.

The health app quality label is unrelated to any labelling requirements for medical devices.

The health app quality label shall conform to the requirements documented in Annex A, using quality scores calculated using the method defined in Annex B.

5 Quality requirements

5.1 Product information

5.1.1 Product

5.1.1.1 Which operating systems or platforms does the health app support?

PURPOSE: Label content, Filtering

RESPONSE OPTIONS: Android™[1] / iOS®[2] / Web app / Other (Multiple-choice)

If 'Other' is selected, provide the name(s) of the other operating system(s) or platform(s) for the label.

NOTE 'Health and wellness app' and 'health app' are synonyms.

5.1.1.2 What is the name of the health app?

PURPOSE: Label content

RESPONSE OPTIONS: Text

NOTE The name of the health app is the name used in the platform's digital marketplaces.

5.1.1.3 Provide the health app icon, if available.

PURPOSE: Label content

RESPONSE OPTIONS: Image file

NOTE The health app icon is the image that helps consumers to find and distinguish a specific app in, e.g. a platform's digital marketplace.

5.1.1.4 In which languages is the health app available?

PURPOSE: Filtering

RESPONSE OPTIONS: Multiple-choice (see ISO 639-3)

NOTE Language refers to the user interface languages of the health app, instructions for use and other user documentation relating to the health app, that are available for this version of the health app on this / these operating system(s) or platform(s).

5.1.1.5 Provide health app access instructions for the app assessment organization.

PURPOSE: App assessment

RESPONSE OPTIONS: Text

Login credentials should be included with the instructions if appropriate.

Test information input during app assessments should not affect normal use of the app or data derived from its normal use.

5.1.2 App manufacturer

5.1.2.1 What is the name of the health app manufacturer?

PURPOSE: Label content

[1] Android ™ is a trademark of Google LLC. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

[2] IOS® is the registered trademark of Cisco for a product supplied by Apple®. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

RESPONSE OPTIONS: Text

NOTE 1 App manufacturer refers to the legal or natural person that places the health app on the market and is responsible for the correct function according to applicable legislation. In some cases, the term for the responsible legal or natural person is app publisher.

NOTE 2 The name is provided in the health app quality label to help potential customers and users establish the identity of the app manufacturer.

5.1.2.2 Provide e-mail address and telephone number of the person who is authorized to represent the health app manufacturer.

PURPOSE: App assessment

RESPONSE OPTIONS: Text + Number

The contact details are for app assessment purposes only. As people can change roles, a role-based e-mail address and telephone number is recommended.

5.2 Healthy and safe

5.2.1 Health requirements

5.2.1.1 Who are the intended users of the health app?

PURPOSE: Label content (Benefit of the app), Filtering

RESPONSE OPTIONS: Anyone / Persons with, or at risk of, specific health issues / Informal carers / Health professionals / Researchers / Other (Multiple-choice + Text)

EVIDENCE: Screenshots of intended user specification communication and sources of the screenshots

If ‘Other’ is selected, provide a text description.

EXAMPLE 1 Informal carers include parents of underaged children and relatives who provide care.

EXAMPLE 2 Health professionals include clinicians, public health professionals, health policy workers, care workers and wellness professionals such as yoga teachers and personal trainers.

NOTE This is a multiple-choice question to allow for health apps that have more than one intended user type.

5.2.1.2 Are age restrictions of the intended users or subjects of care made clear to potential customers and users?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of age restriction communication and sources of the screenshots (e.g. digital marketplace, section website)

Restrictions that apply to both supervised and unsupervised use should be specified.

NOTE ‘Not applicable’ indicates that the health app has no age restrictions.

5.2.1.3 For which health issue(s) and/or health need(s) is the health app intended?

PURPOSE: Label content (Benefit of the app), Filtering

RESPONSE OPTIONS: Text

EVIDENCE: Screenshots of health issues and/or health needs communication and sources of the screenshots

NOTE Health needs include engaging in health promotion and wellness objectives, such as fitness and mental wellbeing.

5.2.1.4 What is the intended use of the health app?

PURPOSE: Label content (Benefit of the app), Requirements level, Filtering

RESPONSE OPTIONS: System services / Inform / Simple monitoring / Communicate / Preventative behavior change / Self-manage / Research / Treat / Active monitoring / Calculate / Diagnose / Other (Multiple-choice + Text)

EVIDENCE: Screenshot for each intended use

If 'Other' is selected, provide a text description.

Table 1 provides examples of descriptions for intended uses.

Table 1 — Examples of descriptions of intended uses

Intended use	**Description**
System services	Health apps that improve health system efficiency. Unlikely to have direct and measurable individual health outcomes. Includes for example electronic prescribing systems, electronic health record platforms and ward management systems [45].
Inform	Health apps that provide information and resources to anyone or persons with, or at risk of, specific health issues. Can include information on specific health issues or about healthy living. Includes for example apps describing a health issue and its treatment, apps providing advice for healthy lifestyles (such as recipes), and apps that signpost to other services [45].
Simple monitoring	Health apps that allow users to record health parameters to create health diaries. This information is not shared with or sent to others. Includes for example health tracking information such as from fitness wearables, symptom or mood diaries [45].
Communicate	Health apps that allow two-way communication between anyone or persons with, or at risk of, specific health issues and health professionals, informal carers, third-party organizations or peers. Health advice is provided by a health professional using the app, not by the app itself. Includes for example instant messaging apps for health and social care, video conference-style consultation software, and platforms for communication with informal carers or health professionals [45].
Preventative behavior change	Health apps that are designed to change intended user behaviour related to, for example, smoking, eating, alcohol, sexual health, sleeping and exercise. Prescribed to intended users by a health professional. Includes for example smoking cessation apps, apps used as part of weight loss programs and apps marketed as aids to good sleep habits [45].
Self-manage	Health apps that aim to help persons with specific health issues to manage their health. Can include symptom tracking function that connects with a health professional. Includes for example apps that allow users to record, and optionally to send data to a health professional to improve management of their health issue [45].
Research	Health apps that generate data for research [56]: — measure the magnitude and distribution of a health problem; — create understanding of the diverse causes or determinants of the problem; — develop solutions or interventions that will help to prevent or mitigate the problem; — implement or deliver solutions through policies and programs; and/or — evaluate the impact of these solutions on the level and distribution of the problem.

Table 1 *(continued)*

Treat	Health apps that provide treatment for a specific health issue (such as CBT for anxiety), or guide treatment decisions. Includes for example apps for treating mental health or other conditions, and health professional-facing apps that advise on treatments in certain situations [45].
Active monitoring	Health apps that automatically record information and transmit the data to a health professional, informal carer or third-party organization, without any input from the user, to inform health management decisions. Includes for example apps linked to devices such as implants, sensors worn on the body or in the home. Data are automatically transmitted through the app for remote monitoring [45].
Calculate	Health apps that perform calculations that are likely to affect health care decisions. Includes for example apps for use by health professionals or users to calculate parameters pertaining to care, such as early warning system software [45].
Diagnose	Health apps that use data to diagnose a health issue in a person, or to guide a diagnostic decision made by a health professional. Includes for example apps that diagnose specified health issues using clinical data [45].

NOTE This is a multiple-choice question to allow for health apps that have more than one intended use.

5.2.1.5 Are assessments done to establish whether the health app is a medical device and if applicable is regulatory approval obtained before the app is made available in each country?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: E.g. depending on the country 510(k) number, EUDAMED registration number and CE mark, device certification list issued by notified body, decision tree of applicable legislation with indications why this health app is not a medical device.

To determine if the health app is a medical device, the app manufacturer shall compare the intended use/intended purpose with the medical device definition applicable in each country the app is intended to be made available.

NOTE This assessment includes health apps that are part of, a component of or an accessory to a medical device.

5.2.1.6 Are health professionals involved in the development of the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: One paragraph describing the names of health professionals and professional associations involved, frequency and nature of their involvement and level of influence, with their acknowledgement

The health professionals shall be involved to establish an adequate understanding of health requirements, health risks, contexts and current health interventions. That understanding shall be used in the design of the health app.

If the health app is on the market in different countries, then involvement of local health professionals should be considered as contexts and health interventions can vary between countries.

5.2.1.7 Is appropriate peer reviewed scientific literature used in the development of the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate peer reviewed scientific literature

To be appropriate, the peer reviewed scientific literature shall help establish an understanding of health requirements, health risks, contexts and/or current health interventions. The understanding shall be used in the design of the health app.

Where many resources cover the full range of health needs and health issues addressed by the app, provide the most important 5 to 10 peer reviewed articles used.

EXAMPLE A systematic review of existing publications, including academic research, on intended users' health requirements and current practices published in specialist magazines, conference proceedings and journals.

5.2.2 Health risks

5.2.2.1 Are the health risks of the health app analysed?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Risk analysis documentation

The manufacturer shall identify hazards and estimate the associated risks. Where appropriate, include situations where the health app can be configured and/or supports interfaces to other products (adapted from IEC 82304-1:2016, 4.1).

Information or data for estimating risks can be obtained (adapted from ISO 14971:2019, 5.5), for example, from:

- published standards;
- scientific or technical investigations;
- field data;
- usability tests employing typical users;
- clinical evidence;
- results of relevant investigations or simulations;
- expert opinion;
- external quality assessment schemes.

The health app manufacturer shall identify and document known and foreseeable hazards to intended users in both normal and fault conditions through the introduction and use of the health app (from Reference [44], section 4.3).

Health risks can include over-reliance, disproportionate attachment and addiction to the health app, or manipulation that affects human autonomy [32].

A hazard identification technique that can be used is Functional Failure Analysis, which takes a functional view of the health app and considers for each function what the potential safety consequences can be if the function is:

- lost, i.e. not available when it is required;
- wrong, i.e. is available but performs an unintended action;
- provided when not required, i.e. function performs as intended but not at the correct time or out of sequence.

(from Reference [44], appendix B.1]

Health risk analysis can be carried out by a multi-disciplinary group including a safety officer.

The risk management processes in ISO 14971:2019 are appropriate for medical devices and can be used for other health apps.

5.2.2.2 Are measures in place to control the health risks of the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Overview control measures for specified health risks

The manufacturer shall determine risk control measures that are appropriate for reducing risks to an acceptable level. Risk control measures can reduce the severity or the probability of occurrence of the harm, or both (ISO 14971:2019, 7.1).

Risk control can be achieved through the application of one or more of the following measures:

— changes to the design or the inclusion of protective measures in the health app (adapted from Reference [44], section 6.1);

— health app verification and validation, for example testing. A testing program should address each of the hazards and thus provide a practicable demonstration that the claimed risk reduction has been achieved;

— administrative and implementation procedures, for example requiring users to register and checking whether they are indeed intended users;

— user and other stakeholder training and briefing;

— information for user safety, including warnings.

Warnings can include alerts to notify the user of potential faults that can cause inconvenience or harm to the user, e.g. low battery alerts, and notifications to the user in case of external interruptions or delays, for instance loss of network connection, database problem or lengthy operation [32].

NOTE 1 Risk control measures refer to risk mitigation.

NOTE 2 'Not applicable' indicates that the health app does not have any health risks.

5.2.2.3 Are the residual risks of using the health app found to be acceptable?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Overview residual risks and acceptability

The app manufacturer shall decide whether a health risk is acceptable; and take into account current values of society, as appropriate expressed in local, national or regional regulations (adapted from Reference [44], section 5.1).

When a residual risk is not acceptable and further risk control is not practicable, the manufacturer can gather and review data and literature to determine whether the benefits of the intended use outweigh this residual risk. When this evidence does not support the conclusion that the benefits outweigh the residual risk, the manufacturer can consider modifying the health app or its intended use. Otherwise, this risk remains unacceptable (adapted from ISO 14971:2019, 7.4).

NOTE 'Not applicable' indicates that the health app does not have any health risks.

5.2.2.4 Describe when the health app requires approval from a health professional before use.

PURPOSE: Label content

RESPONSE OPTIONS: Text

If a Text response is given, the health app quality label will include: ‘Check [here] when app requires approval from health professional before use’. If there are no circumstances in which a health professional’s approval is required before use, a Text response is not required, and the message will not appear on the label.

5.2.2.5 Are potential customers and users of the health app made aware of the health risks, contra-indications and limitations of use?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots of communication on health risks, contra-indications and limitations of use, and sources of the screenshots

The app manufacturer shall document contra-indications, potential risks and limitations of use. For example, environmental or patient conditions under which apps or connected devices can be unreliable (e.g. tattoos that impact optical sensor, avoid usage when pregnant, avoid usage outside a temperature range) [32].

The contra-indications can include health issues and symptoms.

If the overall residual risk is judged acceptable, the manufacturer shall inform users of significant residual risks and shall include the necessary information in the product information in order to disclose those residual risks (adapted from ISO 14971:2019, Clause 8).

If the health app provides health recommendations (e.g. general guidelines), the health app manufacturer shall disclose the potential risks to patient safety and their controls. If the health app offers health advice (e.g. specific and personal health decision support), it should be stated that use of the health app does not replace the health professional-patient relationship or the recommendation, opinion or diagnosis of a health professional. Users should be warned of updates caused by possible errors in functionality, in health-related information or in any other sensitive data [32].

If research shows no-contra-indications, health risks or limitations of use are to be expected, or the type of health app makes health risks impossible and contra-indications and limitations of use not applicable, this shall also be made clear to potential customers and users of the health app.

5.2.2.6 Is a process to collect and review safety concerns and incidents for the health app maintained?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of how users can report incidents or issues and sources of the screenshots, appropriate Standard Operating Procedure

This process extends beyond the health app itself and shall include the impact on users, related healthcare processes and any change in intended use (adapted from Reference [44], section 7.2). Dependent on the intended use it can include establishing a detection and response mechanism for undesirable adverse effects for the user [32].

The process shall (adapted from Reference [44], section 7.2):

- enable users of the health app to report incidents they have had or issues they consider can have an impact on patient safety;
- provide a communication mechanism;
- ensure appropriate and sufficient resources are allocated by the app manufacturer to manage and resolve the reported incident;
- enable customers and users to respond to any safety alerts or bulletins issued by the app manufacturer;
- include maintaining a record of safety incidents, including their management and resolution;
- include maintaining a record of potential hazards and their resolution.

The manufacturer shall review the information collected for possible relevance to safety, especially whether (from ISO 14971:2019, 10.3):

- previously unrecognized hazards or hazardous situations are present;
- an estimated risk arising from a hazardous situation is no longer acceptable;
- the overall residual risk is no longer acceptable in relation to the benefits of the intended use; or
- the generally acknowledged state of the art has changed.

The app manufacturer might not be able to communicate with users, unless the users opt in to receiving such information.

NOTE 1 Medical device manufacturers typically apply ISO 14971:2019 in risk management and ISO 13485:2016 to manage quality throughout the life cycle of a medical device.

NOTE 2 ‘Not applicable’ indicates that the health app does not have any health risks.

5.2.3 Ethics

5.2.3.1 Are ethical challenges of the health app assessed with intended users and health professionals?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Names of users and health professionals and user and professional associations involved, ethical issues discussed, challenges and responses

Ethical challenges include discrimination, stigmatization, fairness, bias in data sets, algorithms and users’ interpretation, human agency, liberty, dignity and environmental wellbeing.

Discrimination includes the unfair treatment on the basis of sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation (from Reference [40], FRIA1).

The assessment of ethical challenges is a form of continuous deliberation, critique, and inquiry between manufacturers, deployers, users and in some cases also the general public or policy makers at regional or national level [32].

The assessment of ethical challenges shall include measures to control the identified ethical challenges, testing and monitoring their effectiveness during development, deployment and use and correcting measures deemed not effective [32].

Ethical issues covered in the quality requirements are (adapted from Reference [40], FRIA1):

- technical robustness and safety;
- privacy and data governance;
- transparency (understand how the app achieves its decisions);
- individual and societal wellbeing;
- accountability.

NOTE 1 The "Health inequalities and eHealth" report[66] of the eHealth stakeholder group provides examples to consider in discussing ethical challenges for specific groups.

NOTE 2 Tables F.1 and F.2 provide a mapping of the ethical principles defined by the High Level Expert Group on Artificial Intelligence[40] with the relevant subclauses in this document

5.2.3.2 Is the health app approved by an independent ethics advisor or ethics advisory board?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Copy of approval or exemption documentation, which includes app name, date of assessment, considerations and resulting approval or exemption

NOTE ‘Independent’ means not being part of the design team.

5.2.4 Health benefit

5.2.4.1 Describe the health benefit of using the app.

PURPOSE: Label content

RESPONSE OPTIONS: Text

The described health benefit shall be consistent with health benefits mentioned in the product information and marketing materials.

EXAMPLE 1 With this app [see 5.2.1.1 for intended users] [see 5.2.1.3 for health issue or health need] [see 5.2.1.4 for intended use-specific benefit]. For instance:

- *Inform:* ‘With this app, persons who aim to increase their fitness can learn exercises’
- *Simple monitoring:* ‘With this app, persons with mood disorders can log goal attainment / symptoms / wellbeing’
- *Calculate*: ‘With this app, health professionals can calculate drug dosages’
- *Active monitoring:* ‘With this app, persons with diabetes (can) keep health professionals updated on blood sugar levels’

Where possible, this description should include measurable and testable relevant outcomes, which are supported by evidence. The word ‘can’ in the above examples is then replaced by the quantified information.

EXAMPLE 2

- *Diagnose:* ‘With this app, 6 in 10 persons feel supported in identifying atypical moles that require contact with a dermatologist’

- *Treat:* ‘With this app, 5 in 10 persons who have had a stroke return to work earlier and increase working hours with 10 % or more’

This description shall include the conditions for the health benefit to be realized.

EXAMPLE 3

- *Self-manage:* ‘With this app, 8 in 10 persons with cancer increase quality of life and 6 in 10 prolong survival with on average 5 months, if the app is used on a weekly basis’

The description should be readable by a large audience and shall be no more than 200 characters long.

NOTE This health benefit is included in the health app quality label to help potential customers and users make informed decisions.

5.2.4.2 Are potential customers and users made aware of the health interventions applied to achieve the health benefit?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of communication on the health interventions applied to achieve the health benefit and sources of the screenshots

The communication shall include naming the health interventions applied, such as Cognitive Behavioral Therapy, and describing any calculations used.

If there is human and/or automated interpretation of health-related content, the credentials of qualified health professionals and/or the algorithms shall be disclosed [32].

If the app contains algorithms that change through learning during use, the disclosure shall include:

- for what aspects and how the app changes during use, including its change dynamics and change boundaries;
- how the user can monitor and control change.

For apps that require tradeoffs between fairness and accuracy, the disclosure shall include:

- if and how this trade-off can be adjusted by the user.

Providing human oversight can for example be done through a stop or pause button, by enabling the user to return to an earlier version of the algorithm (roll back mechanism), by enabling a user to trace back which algorithm model or rules led to the decision or recommendation, or by providing a procedure to safely abort an operation when needed [32].

NOTE ‘Not applicable' indicates that the health app does not include any health interventions.

5.2.4.3 Are potential customers and users made aware of all financial costs to achieve the health benefit?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of financial costs communication and sources of the screenshots

This shall include providing details of any in-app purchases, services or other products that are needed to achieve the intended use health benefit, any recurring subscription or upgrade costs and how to end the agreement.

If the app includes in-app payments, the base functionality without payment, the functionality that requires additional payment and its benefits shall be made clear, in a manner that allows a user to make an informed decision about making or declining an in-app payment [32].

If in-app payments exist, they shall not be triggered in such a way that the health app can expose healthcare-related information to payment organizations [32].

NOTE 'Not applicable' indicates that there are no financial costs to achieve the health benefit of the health app.

5.2.4.4 Are potential customers and users made aware of the need for support of a health professional to achieve the health benefit?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of need for which support by which type of health professional and sources of the screenshots

This can refer to apps being prescribed by health professionals to persons at risk of or with a health issue or health need.

NOTE 1 'Not applicable' indicates that the health app does not need the support of a health professional to achieve the health benefit, or the app is solely for use by health professionals, not by consumers.

NOTE 2 ISO 13131 provides guidance in the provision of telehealth services.

5.2.4.5 Is evidence available to support the health benefit of using the app?

CONDITION: 5.2.1.4 Preventative behaviour change / Self-manage / Research / Treat / Active monitoring / Calculate / Diagnose

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Can include observational studies, non-randomized intervention studies, randomized controlled trials (RCT), systematic reviews or meta-analysis of RCT's, and in case of research apps ethics reviews and approvals, official exemptions or waivers and published research protocols. When sources are many, provide the 5 to 10 most important.

The evidence can include evidence relating to non-digital versions of the health intervention and evidence of demonstrably equivalent health apps [54].

To qualify as evidence (adapted from Reference [45]):

- the population in the study shall be a representation of the intended users in the intended setting;
- the health intervention shall be demonstrably equivalent or this specific health app;
- the comparator shall be a care option that is reflective of standard of care in the current care pathway, such as a commonly used active intervention;
- the follow up of both groups shall be over a relevant period of time;
- clinically relevant improvements should be shown in relevant outcomes. The outcome measures reported should reflect best practice for reporting improvements in the specific condition. Relevant outcomes depend on the intended use and include diagnostic accuracy, patient-reported outcomes (preferably using validated tools), symptom severity or quality of life, other clinical measures of disease severity or disability, healthy behaviours, physiological measures, user satisfaction and

engagement, and health and social care resource use, such as admissions or appointments. Generic outcome measures can also be useful when reported alongside condition-specific outcomes;

— the study shall include statistical considerations such as sample size and statistical testing, and shall be clear on reporting the outcomes of every person in the group testing the health app.

NOTE 'Evidence' refers to the health benefit described in 5.2.4.1.

5.2.4.5.1 Does this evidence include peer reviewed research involving the use of this health app?

CONDITION: 5.2.4.5 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Peer reviewed research that acknowledges the use of this health app

5.2.4.5.2 Is the level of the evidence appropriate?

CONDITION: 5.2.4.5 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Abstracts of peer reviewed research studies that acknowledge the level of the evidence

The appropriateness of the evidence depends on the intended use of the app. Table 2 specifies appropriateness.

Table 2 — Examples of appropriate evidence for different intended uses of health apps

Apps with an intended use of	Appropriate evidence
Treat, Active monitoring, Calculate and/or Diagnose	Randomized Controlled Trial (RCT) or systematic review or meta-analysis of RCT's
Only Research	An ethics review and approval or an official exemption or waiver. Publishing the research protocol is good research practice.
Preventative behaviour change and/or Self-manage, that do not have an intended use of Treat, Active monitoring, Calculate and/or Diagnose	An observational study. A quasi-experimental study, experimental study, RCT or Systematic review or meta-analysis of RCT's improves the level of evidence.

NOTE Research design is typically described in the abstract of peer reviewed scientific articles.

5.2.4.6 Is there a maintenance process for the health information in the app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Appropriate Standard Operating Procedure

The maintenance process shall ensure that any health information provided by the health app is:

— valid (aligned to best available sources, such as relevant professional organizations or recognized patient organizations, and appropriate for the target population);

— accurate;

- up to date;
- reviewed and updated by relevant experts at defined intervals, such as every year;
- sufficiently comprehensive [45].

In case of peer-support in the app and other communication functions, appropriate safeguarding measures shall be in place. These include documenting:

- who has access to the platform in what role;
- why these people or groups are suitable and qualified to have access;
- any measures to ensure safety in peer-to-peer communication, such as user agreements or moderation [45].

NOTE 'Not applicable' indicates that the health app does not contain health information.

5.2.4.6.1 Are all sources for the health information in the health app disclosed to potential customers and users?

CONDITION: 5.2.4.6 Yes or No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots of health information in the app that include source details and sources of the screenshots

When the health app provides health recommendations, the scientific degree of evidence and the types and dates of sources used (e.g. clinical practice guidelines and protocols, peer-reviewed articles, professionals and organizations with their credentials) that guided the app content shall be disclosed [32].

5.2.4.7 Are all sources of funding of the health app disclosed to potential customers and users?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots of disclosed sources of funding in the app, and sources of the screenshots

Disclosure about sources of funding and possible conflicts of interest for the app (e.g. app use could incentivize user to buy products or services from app manufacturer) shall be provided [32].

Funding can be provided for example by health authorities, investors, philanthropists, patient organizations, research grants, commercial companies and/or the app manufacturer itself.

5.2.4.8 Is the use of advertising mechanisms in the health app disclosed to potential customers and users and are these advertisements clearly distinguishable?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of disclosed use of advertising and clearly distinguishable advertisements, and sources of the screenshots

Potential use of PII to personalize advertisements from the app shall be disclosed to the user, who shall be given the opportunity to consent or decline [32].

NOTE 1 Advertisements are not clearly distinguishable when they could be mistaken for non-commercial health education.

NOTE 2 'Not applicable' indicates that the health app does not contain advertisements.

5.2.5 Societal benefit

5.2.5.1 Is evidence available of a societal benefit of using the app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Societal benefit evidence. Where many resources are available, provide the most important 5 to 10.

Evidence can include evidence relating to non-digital versions of the health intervention and evidence of demonstrably equivalent health apps.

Societal benefit can refer to Reference [55]:

- Information, which includes a positive effect on lack of population denominator, delayed reporting of events, lack of reliable data, communication roadblocks, lack of access to information or data, insufficient utilization of data and information and lack of unique identifiers;
- Availability, which includes a positive effect on insufficient supply of commodities, services, equipment and/or qualified health professionals;
- Quality, which includes a positive effect on poor experiences for persons with health needs, health issues, at risk for health issues or informal carers, insufficient health professional competence, low quality health commodities, low health professional motivation, insufficient continuity of care, inadequate supportive supervision and poor adherence to guidelines;
- Acceptability, which includes a positive effect on lack of alignment with local norms and programs which do not address individual beliefs and practices;
- Utilization, which includes a positive effect on low demand for services, geographic inaccessibility, low adherence to treatments and loss to follow up;
- Efficiency, which includes a positive effect on inadequate workflow management, lack of or inappropriate referrals, poor planning and coordination, delayed provision of care and inadequate access to transportation;
- Cost, which includes a positive effect on high cost of manual processes, lack of effective resource allocation, expenses of persons with health needs, health issues, at risk for health issues or informal carers and lack of a coordinated payer mechanism;
- Accountability, which includes a positive effect on insufficient engagement of persons with health needs, health issues, at risk for health issues or informal carers, unawareness of service entitlement, absence of community feedback mechanisms, lack of transparency in commodity transactions, poor accountability between the levels of the health sector, and inadequate understanding of the beneficiary populations.

5.2.5.1.1 Does this evidence include peer reviewed research involving the use of this health app?

CONDITION: 5.2.5.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Peer reviewed research involving the use of this health app. Where many resources are available, provide the most important 5 to 10 peer reviewed articles.

5.3 Easy to use

5.3.1 Accessibility

5.3.1.1 Is the health app WCAG 2.1 AA or AAA compliant?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Evidence of internal implementation of the WCAG guidelines or reports from third parties

NOTE 1 WCAG: Web Content Accessibility Guidelines [52].

NOTE 2 WCAG has three levels of compliance, A, AA and AAA. Level AAA is the maximum level of compliance [52].

NOTE 3 Apps designed to be adaptable will facilitate ease of use for all users, rather than just those with disabilities [57].

5.3.1.1.1 Are WCAG 2.1 AA compliant measures taken to ensure that all intended users can perceive all relevant information and user interface components of the health app and related documents?

CONDITION: 5.3.1.1 No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Test results, e.g. for contrast or alternatively screenshots of measures taken with one sentence explanation and sources of the screenshots

Related documents include terms of service, instructions for use and privacy statement.

NOTE This refers to the health app being fit for use for persons with e.g. a visual or hearing disability.

EXAMPLE [52]:

- Zoom/magnification;
- Sufficient contrast, can be measured with free apps;
- Text alternatives for visuals, audio or video alternatives for texts;
- Test for colour blindness, tools to test and colour palettes that do work are available;
- Enable portrait / landscape orientation;
- Sufficient line, text and font spacing;
- Sans serif font types.

5.3.1.1.2 Are WCAG 2.1 AA compliant measures taken to ensure that all intended users can operate all relevant user interface and navigation components of the health app and related documents?

CONDITION: 5.3.1.1 No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots of measures with one sentence explanation and sources of the screenshots, alternatively test results

NOTE WCAG compliance refers to the health app being also fit for use for persons with e.g. physical disabilities and seizures.

EXAMPLE [52]

- Keyboard control for touchscreen devices;
- Sufficient touch target size and spacing;
- Placing buttons where they are easy to access;
- Being able to use screen readers;
- Control mechanisms to enable enough time;
- Prevent loss of data due to user inactivity or re-authenticating;
- No content that can cause seizures or physical reactions, such as repetitive flashes;
- Designs that help users navigate, such as titles, links, (section)headings and labels that describe topic or purpose;
- Alternative input modalities, such as speech recognition.

5.3.1.1.3 Are WCAG 2.1 AA compliant measures taken to ensure that all intended users can understand all relevant information and user interface components of the health app and related documents?

CONDITION: 5.3.1.1 No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Test results, e.g. results of readability tools, alternatively screenshots measures with one sentence explanation and sources screenshots

NOTE WCAG compliance refers to the health app being also fit for use for persons with language or skill barriers, such as those with low literacy and low technology skills or non-native speakers.

EXAMPLE [52]

- Position important page elements before the page scroll;
- Use lower secondary education level texts and simple short active sentences;
- Avoid metaphors, proverbs, double negatives, percentages, formulas, graphs, tables and distracting details in imagery;
- Explain intent and rationale;
- Provide definitions of jargon and meaning of abbreviations;

- A mechanism to identify pronunciation of content that can otherwise be misinterpreted;
- A predictable and consistent appearance and operation, following platform standards.

5.3.1.2 Is the health app age-appropriate?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots illustrating age appropriateness with one sentence explanation and sources screenshots

Age appropriateness can include, but is not limited to, measures to safeguard minors in accordance with applicable legislation,[32] reference measurements such as maximum pulse rate, sensitivity of subjects such as sexuality, and information complexity.

Information complexity should take account of the following guidelines [51]:

- For children from birth through 6 years: Use simple language with descriptive and sensory words, repetition, rhythm and song, as well as animal and human characters. Use rhymes, riddles, tongue twisters and simple jokes to make content as appealing as possible;
- For children 7 through 10 years: Use stories about friendships, new skills or talents. Use daily occurrences that are opportunities for growth as well as testing one's values and critical thinking skills;
- For adolescents 11 through 14 years: Use positive role models with high moral standards. Use stories about balancing the influence of family / friends / media and non-pedagogical formats and guidance in helping channel the need for experimentation and independence into health life choices;
- For all age groups: Produce communication that invites children to see, imagine, hear and create things that they would not have thought about previously.

5.3.2 Usability

5.3.2.1 Is the health app design based on an explicit understanding of users, tasks and environment?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: One paragraph describing how the explicit understanding has been obtained and addressed

All relevant user and stakeholder groups should be identified (ISO 9241-210:2019, 5.2)) and up to date knowledge on for example user experience, behaviour change techniques, availability of type of devices and access to wifi and electricity for these groups should be used to promote real world continued usage of the health app.

EXAMPLE Observation of users (ethnographic research), interviews, use cases, personas.

NOTE 1 The explicit understanding includes but is not limited to the health requirements addressed in 5.2.1.

NOTE 2 The extent to which health apps are usable (and accessible) depends on the context, i.e. the specified intended users having specified goals, performing specified tasks in a specified environment. The characteristics of the users, tasks and environment, also known as the context of use, is a major source of information for establishing usability requirements and an essential input to the design process (adapted from ISO 9241-210:2019, 5.2).

NOTE 3 The European Blueprint on Digital Transformation of Health and Care for the Ageing Society[39] provides information on 12 personas, i.e. how different ages and severity of health issues can affect requirements.

NOTE 4 ISO/TR 16982:2002 provides information on a variety of methods.

NOTE 5 IEC 62366-1:2015+AMD1:2020 specifies a process for manufacturers to analyse, specify, develop and evaluate the usability of a medical device as it relates to safety.

5.3.2.2 Are intended users involved throughout design and development of the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: One paragraph describing the number and type of intended users and specified organizations involved, frequency and nature of their involvement, and level of influence, with their acknowledgement.

User involvement shall be active, whether by participating in design, acting as a source of relevant data or evaluating solutions. The people who are involved shall have capabilities, characteristics and experience that reflect the range of users for whom the health app is being designed. The nature and frequency of this involvement can vary throughout design and development, depending on the type of health app. The effectiveness of user involvement increases as the interaction between the developers and users increase (adapted from ISO 9241-210:2019, 5.3).

EXAMPLE A user-centric approach for behavioural health interventions is described in Reference [43].

NOTE User engagement contributes to the explicit understanding as referred to in 5.3.2.1.

5.3.2.3 Is the design of the health app driven and refined by user-centred evaluation?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure, alternatively one paragraph describing how the design of the health app is driven and refined by user-centred evaluation

The health app shall be assessed for usability by a sample of intended users. If geared towards a certain age segment or to people with a specific health issue or to persons with disabilities, usability testing subjects are drawn from these populations [32].

The health app manufacturer should create and document a usability assessment plan, including known problems and controls (adapted from Reference [32], section 3.2.3).

User-centred evaluation should take place as part of the final acceptance of the product to confirm that requirements have been met.

Where available and appropriate the human interface guidelines from the platform should be followed.

NOTE 1 There is a variety of user-centred evaluation methods to evaluate designs. Guidance on these and other usability methods, and on selecting the most appropriate method or set of methods, is provided in ISO/TR 16982:2002.

NOTE 2 Evaluating designs with users and improving them based on their feedback provides an effective means of minimizing the risk of a health app not meeting user or organizational needs, including those requirements that are hidden or difficult to specify explicitly. Such evaluation allows preliminary design solutions to be tested against ‘real world’ scenarios, with the results being fed back into progressively refined solutions (ISO 9241-210:2019).

NOTE 3 The term ‘user-centred’ is used here to emphasize that this evaluation is made from the user's perspective (ISO 9241-210:2019).

NOTE 4 Feedback from users during operational use identifies long-term issues and provides input to future design (ISO 9241-210:2019).

5.3.2.4 Are measures in place to avoid use error and reasonably foreseeable misuse of the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots with one sentence describing measures in place to avoid use error and reasonably foreseeable misuse and sources of the screenshots

Opt-in consent shall be required by the intended user before receiving notifications and alerts from an app. Notifications and alerts contain the least amount of information necessary for the recipient to take a focused action. If the app alerts notify the user of conditions such as ‘abnormal’ or ‘exceptional’ or ‘out of range’ the sources (evidence base) of the formulas / algorithms upon which such alerts and notifications are based shall be documented or referenced [32].

EXAMPLE

- Instructions for user input;
- Error prevention such as double checks;
- Input error detection such as body temperature having a range, maximum change in body weight in a specific time span;
- Notifications and alerts with suggestions for corrections;
- Context-sensitive help.

NOTE ‘Not applicable’ indicates that use error or misuse is not possible given the nature of the app.

5.3.2.5 Are potential customers and users provided with adequate product information about the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Link to the primary publicly available source of information about the health app for potential customers and users, for example a website or entry in a digital marketplace.

Product information shall be provided to potential customers and users, to help them decide whether the app is suitable. The app descriptions:

- shall include the main functionality, the intended use, the intended users and the potential use of the user’s personal data by the app;
- shall accurately depict screen shots of the current version of the health app;
- shall clearly note the payment amount for the app, if any, if applicable, according to digital marketplace rules;
- should clearly state the human languages the health app supports, referred to in 5.1.1.4;
- should communicate information about the app manufacturer, referred to in 5.1.2.1, and mechanisms to communicate with the app manufacturer;
- should show the date of the last update to the health app and describe the changes from the previous release, for instance revisions due to new scientific evidence;
- should declare the degree of admission of liability (app manufacturer acceptance or disclaimer of responsibility regarding the selection and use of the app’s content);

- can identify the health professionals and those who worked on the app and/or at least the professional organization that made, reviewed, endorsed, or sponsored the app;
- can include data related to app reliability and validity [32];
- should provide information about accessibility characteristics [32];
- shall give attribution to any open source code library or code under copyright used to develop the app [32].

5.3.2.6 Are instructions for use readily available for users?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots of readily available instructions for use and link to instructions for use, and sources of the screenshots. If the instructions for use are available in the health app, then access to the health app as provided in 5.1.1 is sufficient.

Instructions for use should be delivered either within the app, for example when hovering over a button, or elsewhere. All with the intent to adequately inform users how to use the health app.

The instructions for use shall (adapted from IEC 82304-1:2016, 7.2.2):

- document what is necessary for proper operation of the health app, including installation procedures where appropriate;
- if applicable, specify restrictions on a platform on which the health app is intended to be used;
- contain the intended use, a brief description, any operational security options for the use and any known technical issues, limitations, disclaimer or contra-indications to the use of the health app;
- list all warnings and notices for safety and/or security related to the use of the health app and explain or expand them when they are not self-explanatory;
- contain the necessary information for the user to bring the health app into operation, to safely shut down the operation, and all information necessary to operate the health app. This shall include explanation of the function of controls, displays and signals, the sequence of operation and the meaning of figures, symbols, warning statements and abbreviations;
- list all system messages including important causes, and possible actions by the user, if any, that are necessary to resolve the situation indicated by the message;
- contain all information necessary for the user or the responsible organization to safely decommission and dispose of the health app. This shall include, where appropriate, safeguarding personal and health-related data in connection with security and privacy;
- contain the technical description or a reference to where the technical description can be found.

The technical description shall provide all data that is essential for safe and secure operation, transport and storage, and measures or conditions necessary for installing the health app and preparing it for use (adapted from IEC 82304-1:2016, 7.2.3).

Information about accessibility characteristics should be provided in the app descriptions and in contextual assistance sections of the app [32].

EXAMPLE Training, briefings, quick references, audio or video tutorials.

5.3.2.7 Are appropriate resources available to adequately help users who experience problems with the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Screenshots showing resources to adequately help in case of problems using the app and sources of the screenshots

The health app manufacturer shall ensure that:

- the product documentation clearly states information as to how to access user support, and channels of support (e.g. voice, email, text, Twitter) and anticipated response and follow up times;
- user support is provided in the languages in which the app is published;
- user support is available prior to establishing a user account (e.g. user can contact user support with questions about the app's privacy statement or terms of use before making a decision to actively use the app);
- if a support request involves accessing, disclosing or changing user data, the identity of the user or the user's data access rights are verified before any disclosure or changing of user data.

The health app manufacturer should provide a Frequently Asked Questions (FAQ) resource where users can find answers to common questions [32].

5.3.2.8 Is relevant data on the usability of the health app systematically gathered throughout its entire lifetime, in order to make regular improvements?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Regular usability improvements visible in version history digital marketplace, appropriate Standard Operating Procedure, alternatively regular user survey, frequency and follow up

Improvements can be limited by the need for appropriate user consent.

5.4 Secure data

5.4.1 Privacy

5.4.1.1 Does the health app process Personally Identifiable Information (PII)?

PURPOSE: Requirements level

RESPONSE OPTIONS: Yes/No

EVIDENCE: Overview of PII processed in the health app and via alternative routes, screenshots and sources of the screenshots

Processing includes indirect use of PII, such as when the health app uses device resources or device hardware which provide access to PII or process it themselves. Device resources include system stored credit card information, accessing social networking resources, photos. Device hardware includes Wi-Fi, LAN, GPS/location, camera, microphone, step counter, calendar, address book, SMS or MMS messaging and Bluetooth [57].

5.4.1.1.1 Does the health app process health related PII?

PURPOSE: Requirements level

RESPONSE OPTIONS: Yes/No

EVIDENCE: Overview of health related PII processed in the health app and via alternative routes, screenshots and sources of the screenshots

The classification of PII that falls into these categories can vary from one jurisdiction to another and can vary between different regulatory regimes that apply to different kinds of business, so the health app manufacturer shall need to be aware of the classifications that apply to the PII processing being performed. The use of health related PII can also be subject to more stringent controls (adapted from ISO/IEC 27701:2019, 7.2.2).

5.4.1.1.2 Is data minimization applied in the health app?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Overview of PII processed and purpose e.g. from privacy statement

The app manufacturer should identify how the specific PII and amount of PII collected and processed is limited relative to the identified purposes (ISO/IEC 27701:2019, 7.4.4).

Privacy by design and privacy by default contribute to data minimization. Privacy by design ensures that processes and systems are designed such that the collection and processing (including use, disclosure, retention, transmission and disposal) are limited to what is necessary for the identified purpose. Privacy by default implies that, where any optionality in the collection and processing of PII exists, each option should be disabled by default and only enabled by explicit choice of the data subject (adapted from ISO/IEC 27701:2019, 7.4).

Data minimization shall include ensuring that:

— the app reduces data granularity and anonymizes the data on the device instead of remotely, for instance stripping image metadata [38];

— for purposes of establishing an account, the minimum necessary amount of a user's PII is collected (e.g. the information is necessary to authenticate the user, provide user support, or affect the app logic [32];

— only platform functionality and data sources essential to perform specific functions of the app are used. This includes, but is not limited to, the use of location, services, camera, microphone, accelerometer and other sensors, contact lists, calendars [32];

— the app stores the device number or IP addresses transmitted during use only to the degree needed to fulfil the application's purpose.

NOTE Data minimization is achieved if PII is only processed where it isn't reasonably feasible to carry out the processing in another manner, and anonymous data is used where possible.

EXAMPLE The use of de-identification and limiting the amount of PII that is collected indirectly, for instance through web logs, system logs, etc. (ISO/IEC 27701:2019, 7.4.1 and 7.4.4).

5.4.1.1.3 Is an appropriate retention policy established to erase or review the data stored?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Retention policy, appropriate Standard Operating Procedure

A retention policy should be in place for the PII of inactive users of the health app.

The manufacturer should develop and maintain retention schedules for information it retains, taking into account the requirement to retain PII for no longer than is necessary. Such schedules should take into account business requirements. Legal and regulatory requirements can also apply. Where such requirements conflict, a business decision needs to be taken (based on a risk assessment) and documented in the appropriate schedule (adapted from ISO/IEC 27701:2019, 7.4.7).

Procedures for how data continues to be retained and used after account closure shall be clear and understandable and give the app user the option to obtain a copy of their data [32].

The user shall be able to safely decommission and dispose of the health app, including, where appropriate, safeguarding personal and health related PII (adapted from IEC 82304-1: 2016, 8.5).

NOTE Retention policy is also referred to as storage limitation.

5.4.1.1.4 Is a privacy statement readily available to potential customers and users of the health app?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Access to the health app

The health app manufacturer shall determine the legal, regulatory and/or business requirements for when information is to be provided to the PII subject (e.g. prior to processing, within a certain time from when it is requested, etc.) and for the type of information to be provided. Depending on the requirements, the information can take the form of a notice. Examples of types of information that can be provided to PII subjects are:

- the purpose of the processing;
- contact details for the PII controller or its representative;
- the lawful basis for the processing;
- where the PII was obtained, if not obtained directly from the PII subject;
- whether the provision of PII is a statutory or contractual requirement, and where appropriate, the possible consequences of failure to provide PII;
- obligations to PII subjects, and how PII subjects can benefit from them, especially regarding accessing, amending, correcting, requesting erasure, receiving a copy of their PII and objecting to the processing;
- how the PII subject can withdraw consent;
- transfers of PII;
- recipients or categories of recipients of PII;
- the period for which the PII will be retained;
- the use of automated decision making based on the automated processing of PII;
- the right to lodge a complaint and how to lodge such a complaint;
- the frequency with which information is provided, for instance ‘just in time’ notification, organization defined frequency, etc.

The health app manufacturer shall:

- provide updated information if the purposes for the processing of PII are changed or extended (ISO/IEC 27701:2019, 7.3.2)
- inform the PII subject of any intended changes concerning the addition or replacement of PII processors, thereby giving the PII subject the opportunity to object to such changes (ISO/IEC 27701:2019, 8.5.8)];
- provide a mechanism for PII subjects to modify or withdraw their consent (ISO/IEC 27701:2019, 7.3.4).

Where appropriate, the privacy statement should be given at the time of PII collection. It should also be permanently accessible (ISO/IEC 27701:2019).

Before using select platform functions and data sources for the first time, the app manufacturer shall ensure app users are asked for permission to use the services and data sources. The manufacturer should allow the user to individually give permission for each function, data source and user tracking activity controlled by the app [32].

NOTE ISO/IEC 29184 provides information on online privacy notices and consent.

5.4.1.1.4.1 Does the privacy statement start with an accessible overview of less than 150 words?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Access to the health app

The overview shall include a description of the PII processed, purpose and retention policy.

The health app manufacturer should provide the information in a timely, concise, complete, transparent, intelligible and easily accessible form, using clear and plain language, as appropriate to the target audience. Icons and images can be helpful to the PII subject by giving a visual overview of the intended processing (ISO/IEC 27701:2019, 7.3.3).

NOTE Aim is to enable adequate understanding (privacy literacy), informed decisions and to not further increase disparities. Research in privacy policy reading behaviour for a (fictitious) social networking app suggests 3 in 4 persons do not read a policy at all. Those that do, have an average reading time of 73 seconds. Decliners read 30 seconds longer.[46] The average number of words per minute for low health literates is estimated at 120, hence the 150 words.

5.4.1.1.5 Are contracts in place with all processors and controllers of PII of the health app and associated services to ensure the level of security controls and privacy protection are as communicated to the user?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: List of processors and controllers of PII, and relevant contract clauses

The app manufacturer should have a written contract with any PII processor that it uses and should ensure that their contracts with PII processors address the implementation of the appropriate controls. The contract between the manufacturer and any PII processor processing PII on its behalf should require the PII processor to implement the appropriate controls, taking account of the information security risk assessment process and the scope of the processing of PII performed by the PII processor (adapted from ISO/IEC 27701:2019, 7.2.6).

A joint PII controller agreement can include but is not limited to (ISO/IEC 27701:2019, 7.2.7):

- purpose of PII sharing / joint PII controller relationship;
- identity of the organizations (PII controllers) that are part of the joint PII controller relationship;
- categories of PII to be shared and/or transferred and processed under the agreement;
- overview of the processing operations (e.g. transfer, use);
- description of the respective roles and responsibilities;
- responsibility for implementing technical and organizational security measures for PII protection;
- definition of responsibility in case of a PII breach (e.g. who will notify, when, mutual information);
- terms of retention and/or disposal of PII;
- liabilities for failure to comply with the agreement;
- how obligations to PII subjects are met;
- how to provide PII subjects with information covering the essence of the arrangement between the joint PII controllers;
- how PII subjects can obtain other information they are entitled to receive;
- a contact point for PII subjects.

PII transfer between jurisdictions can be subject to legislation and/or regulation depending on the jurisdiction or organization to which PII is transferred (and from where it originates). The health app manufacturer should document compliance with such requirements as the basis for transfer (ISO/IEC 27701:2019, 7.5.1).

The health app manufacturer should inform the PII subject of any transfer of PII, including transfers to suppliers, other parties and other countries or international organizations (ISO/IEC 27701:2019, 8.5.1).

5.4.1.1.6 Is opt-in the default setting for sharing PII with third parties?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Screenshots of opt-in and sources of the screenshots, and cookie statement and cookie scan report

Opt-in refers to requiring the PII subject’s consent. The consent should be:

- freely given;
- specific regarding the purpose for processing;
- unambiguous and explicit (adapted from ISO/IEC 27701:2019, 7.2.4).

Before exporting data, the app user shall be asked for permission to transmit the data with an explanation of what data is being transmitted, and to which recipients for what purposes (e.g. to servers of the app supplier, for backups, for big data analysis). Permission is requested before the first potential transmission of data. Permission is re-requested the first time any **additional** data elements are sent to an external data source when permission had previously been extended for a smaller set of data.

Permission is **not** requested at every transmission, if the scope of exported data remains unchanged [32].

This can include cookies and other tracking technologies used to share information with third parties, as well as sharing data with social networks.

NOTE 'Not applicable' indicates that no data is shared with third parties.

5.4.1.1.7 Does the app manufacturer have a person responsible for legal and regulatory compliance of processing of PII?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Name and contact details of the person responsible for legal and regulatory compliance of processing of PII. As people can change roles, a role-based e-mail address and telephone number is recommended.

The health app manufacturer shall appoint one or more persons responsible for developing, implementing, maintaining and monitoring an organization-wide governance and privacy program, to ensure compliance with all applicable laws and regulations regarding the processing of PII.

The responsible person should, where appropriate:

- be independent and report directly to the appropriate management level of the organization in order to ensure effective management of privacy risks;
- be involved in the management of all issues which relate to the processing of PII;
- be expert in data protection legislation, regulation and practice;
- act as a contact point for supervisory authorities;
- inform top-level management and employees of the organization of their obligations with respect to the processing of PII;
- provide advice in respect of privacy impact assessments conducted by the organization.

Such a person is called a data protection officer in some jurisdictions, which define when such a position is required, along with their position and role. This position can be fulfilled by a staff member or outsourced (adapted from ISO/IEC 27701:2019, 6.3.1.1).

5.4.1.1.8 Are security-incident response procedures in place-that include reporting PII breaches to the user and relevant authorities?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Security-incident response procedures

The health app manufacturer shall establish responsibilities and procedures for the identification and recording of breaches of PII. Additionally, the organization shall establish responsibilities and procedures related to notification to required parties of PII breaches, including the timing of such notifications and the disclosure to authorities, taking into account the applicable requirements (ISO/IEC 27701:2019, 6.13.1.1).

Where a breach involving PII has occurred, a record shall be maintained with sufficient information to provide for regulatory and/or forensic purposes (adapted from ISO/IEC 27701:2019, 6.13.1.5), such as in:

- a description of the incident;
- the time period;
- the consequences of the incident;
- the name of the reporter;
- to whom the incident was reported;
- the steps taken to resolve the incident (including the person in charge and the data recovered);
- the fact that the incident resulted in unavailability, loss, disclosure or alteration of PII;
- a description of the PII compromised, if known;
- if notifications were performed, the steps taken to notify PII subjects, regulatory agencies or customers.

5.4.2 Security

5.4.2.1 Have the health app manufacturer and all organizations providing associated services implemented ISO/IEC 27001 or a recognized equivalent?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Statement of applicability that covers software product and associated services, ISO/IEC 27017 and ISO/IEC 27018 in case of cloud hosting

Associated services include but are not limited to other mobile applications, cloud computing/storage and third-party Application Programming Interfaces (APIs), which are typically required to provide the health app's intended functionality.

The extent of documented information can differ from one organization to another (as listed in ISO/IEC 27001:2013, 7.5.1) due to:

- size of the organization and its type of activities, processes, products and services;
- complexity of processes and their interactions;
- competence of persons.

Certification can be considered to demonstrate implementation of ISO/IEC 27001.

EXAMPLE Other recognized standards are ISM[36] (Australia), SOC 2[34] and HITRUST[42].

5.4.2.2 Is an information security risk assessment for the health app available?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Information security risk assessment

The information security risk assessment shall:

- consider the external and internal issues that are relevant to its purpose, legal, regulatory and contractual requirements, and interfaces and dependencies between activities performed by the app manufacturer and by those that are performed by other organizations;
- identify risks and potential consequences associated with the loss of confidentiality, integrity and availability of information and the realistic likelihood of the occurrence of the risks;
- assess the applicability of control objectives and controls in the context of both risks to information security as well as risks related to the processing of PII, including risks to data subjects (adapted from ISO/IEC 27001:2013, 6.1, and ISO/IEC 27701:2019, 6.1);
- if personal health information is hosted, ensure and document backup and recovery procedures are compliant with applicable requirements [32];
- explicitly determine what risk must be addressed through software coding, hardware adaptations, and policies, and what residual risk will be accepted by the app manufacturer [32].

EXAMPLE ISO/IEC 27001:2013, Annex A provides a list of control objectives and controls that can be useful. OWASP mobile security risks top 10[49] and HL7's cMHAFF, section 2.4 on examples of risk scenario's and related controls[32].

5.4.2.3 Is a secure by design process followed?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure or policy

Where available and appropriate the security best practices for the platform should be used.

NOTE Security by design ensures that information security is designed and implemented within the development lifecycle of information systems (ISO/IEC 27701:2019, A.14.2).

EXAMPLE [38]

- Ensure correct usage of biometric sensors and secure hardware;
- Secure data integration with third party code;
- Implement user authentication, authorization and session management correctly;
- Ensure sensitive data is protected in transit;
- Obtain consent and protect privacy;
- Protect paid resources;
- Secure the backend services and the platform server and APIs;
- Identify and protect sensitive data on the mobile device;
- Protect the application from client side injections;
- Secure software distribution;
- Check device and application integrity;
- Handle runtime code interpretation correctly;
- Handle authentication and authorization factors securely on the device.

5.4.2.4 Are measures in place to ensure that all third-party software libraries and other software components for the health app are reliable and maintained?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Overview of third-party code and third-party libraries and validation of their safe functionality

App manufacturers should audit code for security issues, audit libraries and inspect any transmitted data to third-party services for privacy issues [38].

EXAMPLE

— Backdoors: Any method by which authorized and unauthorized users are able to get around normal security measures to gain root access to a computer system, network or software application;

— Untrusted software branches/forks: Branches/forks refer to duplicating software under version control to enable modifications. The modified software is later integrated to update the application. Only use branches/forks that are actively maintained by the original project team, otherwise security vulnerabilities might not be resolved and even be introduced. Check if sources are trustworthy and use tools to help assess maintenance level.

5.4.2.5 Is a process to prevent unauthorized access and modifications to the health app source code in place?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure, alternatively report or other evidence of a code-level security assessment by a CREST[37] or similar appropriate body.

The process can include following:

- Check the application integrity, check that the application and its resources are not modified:
  - use platform service (e.g. Android™ SafetyNet attestation, iOS® App Store receipt);
  - perform in-memory code integrity checks to protect against code modification and/or runtime hooking.
- Make reverse engineering harder:
  - obfuscate code;
  - encrypt data (e.g. strings) to further obfuscate application logic.
- Disable developer features:
  - disable debugging in the application settings;
  - check if the device is in developer mode if supported by platform, for instance Android™;
  - check if debugger is attached and/or if the process is being traced. On platforms with managed code check for managed and native code debuggers.

Check the device/platform integrity to ensure that the device is not modified. Prefer using platform services if available, for instance Android™ SafetyNet attestation. Only implement custom or use third party root/jailbreak detection, if platform does not offer a built-in solution [38]

The health app source code should be secured during design, development and deployment.

5.4.2.6 Are organizational measures in place to ensure PII is processed in a manner that is compatible with the explicit, legitimate purposes specified in the privacy statement?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Documentation of relevant Operating Procedures including steps taken to ensure that the procedures are followed.

NOTE ISO/IEC 27001 provides a list of appropriate organizational measures.

EXAMPLE (adapted from ISO/IEC 27001:2013, 5.1)

- Ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;
- Ensuring the integration of the information security management system requirements into the organization's processes;
- Ensuring that the resources needed for the information security management system are available;
- Communicating the importance of effective information security management and of conforming to the information security management system requirements;
- Ensuring that the information security management system achieves its intended outcomes;
- Directing and supporting persons to contribute to the effectiveness of the information security management system;
- Promoting continual improvement.

5.4.2.7 Is user authentication, authorization and session management implemented to secure access to the health app?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Access to the health app and a description of the measures taken

The health app manufacturer shall ensure (adapted from Reference [32], section 3.4.1):

- the identity of an app user is authenticated prior to any access of PII;
- the method of authentication is communicated to the app user when an app account is established;
- the app user is authorized to access a feature of the app before that feature or any associated PII is displayed. Authorization can be internal to the app or derived from an external source;
- at the request of an app user, the app terminates such that access to PII requires a new, successful authentication attempt;
- if another external health IT system (e.g. Electronic Health Record) is used, a subject's association with their real-world identity is verified, establishing that a subject is who they claim to be (identity proofing);
- if PII are displayed, the health app terminates or makes PII invisible after a period of time of user inactivity as described in the app's product information;
- if passwords are stored on the device, passwords are encrypted and never displayed as plain text;

- if access to the account exposes PII, the user is given an option to utilize strong authentication methods (e.g. multi-factor authentication and/or biometrics) in addition to passwords.

If the health app has associated services such as cloud services or back end systems, authentication and authorization should be implemented for all interfaces.

NOTE ENISA[38] is a source for measures.

5.4.2.8 Does the health app transmit and store all PII with adequate encryption?

CONDITION: 5.4.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Overview of cryptography algorithms used

Adequate encryption should include:

- generating all cryptographic keys for the health app and associated services dynamically wherever possible. Dynamic keys are one-time used to avoid compromising the encryption and the safety of the whole system;
- making use of secure containers provided by the operating system to store cryptographic keys, to avoid unauthorized unlawful disclosure or access to the user's data, impersonating as the user, for instance Keystore for Android™ and Keychain®[3] for iOS®.

Encryption paradigms should follow contemporary practices as the strength of an encryption method can degrade over time as computational methods for breaking encryption continue to evolve [32].

Data on associated services should be encrypted, if applicable.

EXAMPLE OWASP's Mobile Security Testing Guide[47] cryptography clause specifies contemporary cryptography practices.

5.4.2.9 Are security vulnerabilities reported, identified, assessed, logged, responded to, disclosed, and quickly and effectively resolved?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure, Coordinated Vulnerability Disclosure (CVD) or Responsible Disclosure, Vulnerability report

Sources of information on security vulnerabilities can include publicly available reports from authorities, as well as publications by suppliers of, for instance, operating systems and third-party software (IEC 82304-1:2016, 4.1).

The monitoring process shall at minimum include:

- informing customers and users of the health app about security vulnerabilities the manufacturer has become aware of, and of changes in regulatory requirements that impact the use of the health app (IEC 82304-1:2016, 8.4);
- coordinated Vulnerability Disclosure (CVD), a responsibility disclosure policy and active engagement with stakeholders and peers in case of a breach;

[3] Keychain® is the registered trademark of a product supplied by Apple®. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results.

- tracking updates of software libraries and other software components and to plan for their use;
- tracking of vulnerabilities in associated services, e.g. newly discovered vulnerabilities in cloud-based authentication and storage providers.

5.4.2.10 Are the security of the health app and associated services tested on a regular basis and at major changes?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure, certificate by security testing organization that specifies health app name and associated services, alternatively evidence of continuous static code testing

Testing shall assess the effectiveness of technical and organizational measures for ensuring confidentiality, integrity and availability.

The rigor of testing should be guided by the risk levels, e.g. whether PII or special categories of PII are processed and the severity and likelihood of resulting harm.

This includes automated static code vulnerability scanning solutions, PEN-testing or penetration testing and ethical hacking, i.e. the practice of testing a computer system, network or web application to find security vulnerabilities that an attacker could exploit.

Further guidance on testing can be obtained from ISO/IEC 27701, OWASP[47] and ENISA[38] and certified bodies such as CREST[37].

5.4.2.11 Is the information security policy readily available to potential customers and users?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Access to the health app

The information security policy shall (adapted from ISO/IEC 27001:2013, 5.2):

- be appropriate to the purpose of the organization;
- include information security objectives or provide the framework for setting information security objectives;
- include a commitment to satisfy applicable requirements to information security;
- include a commitment to continual improvement of the information security management system;
- be approved by management;
- be available as documented information;
- be communicated within the organization;
- be available to interested parties, as appropriate.

EXAMPLE A whitepaper on the information security policy on the consumer website.

5.5 Robust build

5.5.1 Technical robustness

5.5.1.1 Are all the health app product requirements documented?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Health app product requirements

The manufacturer shall ensure that the health app product requirements are updated as appropriate (adapted from IEC 82304-1:2016, 4.7).

NOTE 1 Further information about health app product requirements is available in IEC 82304-1:2016, Clause 4, and cMHAFF, section 3.2 [32].

NOTE 2 Health app product requirements include both use requirements and system requirements.

NOTE 3 Health app product requirements include but are not limited to the requirements documented in this document.

5.5.1.2 Is the health app developed with a software development process that covers the standards, methods and tools to be used?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure, screenshots of tools employed

EXAMPLE ISO/IEC/TR 29110-1:2016.

5.5.1.3 Is a secure coding standard followed?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Output from source code analysis tools

Secure coding standards should incorporate the following principles:

- establish coding standards and conventions;
- use safe functions only;
- use appropriate compiler and toolchain versions and secure compiler options;
- handle input and other data safely (i.e. in a restrictive, cautious way);
- use source code analysis tools to find security issues early;
- handle errors.

NOTE Secure coding aims to avoid common mistakes that might introduce vulnerabilities in development languages such as C++, Java, etc. Coding mistakes such as buffer overruns and logic flaws are a common cause for security vulnerabilities.

EXAMPLE OWASP secure coding practices[48].

5.5.1.4 Is a configuration management plan established for the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Configuration management plan

Configuration should be managed so components of the health app are consistently referenced in all project and user documentation and to enable the management of issues encountered during use. The configuration management plan should exist for the entirety of the health app life cycle (IEC 62304:2006+AMD1:2015).

5.5.1.5 Are processes in place to deal with a significant increase or spike in demand?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure

The process should ensure that the health app requirements specified in 5.5.1.1 are not compromised in case of increased demand.

The manufacturer should avoid excessive data use by the app, minimizing it as much as possible, warning users when high data usage occurs (e.g. downloads and updates) [32].

NOTE Increased demand includes increases in number of users, transactions and data volumes.

5.5.1.6 Is a validation and verification plan used for the health app?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Validation and verification plan

The validation and verification plan should cover the health app itself and also any associated products or services it is dependent upon.

The validation and verification plan shall describe what testing should be done when there is a change to the accompanying documentation, to the health app or to the platform that it runs on.

The testing should include validation that the intended use can be delivered by the health app and verification that the requirements and risk control measures have been implemented successfully.

The validation and verification team shall perform the validation activities in the intended operational environments according to the validation and verification plan (adapted from IEC 82304-1:2016, Clause 6).

All requirements, tests and test outcomes should be traceable throughout the app’s life cycle.

EXAMPLE Validation methods include inspection, analysis, analogy/similarity, demonstration, simulation, peer-review, testing or certification. Relevant information: reference to standards and other publications such as compatibility standards, regulatory authority guidance documents, and clinical literature (IEC 82304-1:2016, 6.1). The objective evidence needed for a verification can be the result of an inspection or of other forms of determination such as performing alternative calculations or reviewing documents (IEC 82304-1:2016, 3.24).

NOTE For further detail on validation, see IEC 82304-1:2016. For further detail on verification, see IEC 62304:2006+AMD1:2015.

5.5.1.7 Is a release and deployment process established?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure

The release and deployment process shall include a process for rolling back to a previous version of the health app if major issues are identified. An incremental release policy should be considered, where possible, so that the app is trialled by a limited number of users in pilot implementations before being made generally available.

When the health app has collected personal health information, the release and deployment process should guarantee continuity of data use across different versions of the app [32].

5.5.1.8 Is a maintenance process established?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Appropriate Standard Operating Procedure

The maintenance process shall involve monitoring feedback, problem resolution and change request management.

In the case of health app maintenance, the manufacturer shall inform customers and users of the availability of the updated version of the health app, and provide information about the following, where appropriate (IEC 82304-1:2016, 8.4):

- new features;
- corrected errors or faults;
- any impact on safety and/or security of the modified software;
- updates in the health app identification;
- updates in the accompanying documents.

The health app manufacturer shall (Reference [32], section 3.4.9):

- ensure re-validation takes place to the parts of the health app that have been affected by the software maintenance, taking into account the extent of the modification;
- update the validation and verification plan accordingly;
- ensure that the modified version of the health app functions with any hardware and software platform that is claimed to be supported (IEC 82304-1:2016, 8.3);
- ensure the app respects operating system level permission concerning automatic product updates;
- if automatic app updates are not enabled, ensure the app prompts the user to the availability of a new version of the app when a new version is available;
- if the user elects to not install a new version of the health app, present the consequences of not installing the new version of the app to the user, including information about support limitations for the older version of the app.

The health app manufacturer should (Reference [32], section 3.2.2):

- document measures to ensure the availability of that infrastructure if a health app relies on external supporting infrastructure (e.g. cloud-based servers) to operate;
- monitor and document conflicts or compatibility issues of the app with other apps, device features, for instance camera, or connected devices.

EXAMPLE IEC 62304:2006+AMD1:2015 provides an example of a maintenance process.

5.5.2 Interoperability

5.5.2.1 Are potential customers and users of the health app able to access the specifications and implementation guides for all the APIs?

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Regular access to specification and implementation guides

If the health app exchanges unstructured data, commonly accepted formats, e.g. Clinical Document Architecture (CDA) and Portable Document Format (PDF), should be used [32].

There can be additional costs to access the relevant standards.

While such technical details are not relevant to all users, they can for example be used for assessing compatibility of the health app with other systems in a health service.

NOTE 1 'APIs' are Application Programming Interfaces to for example external devices, websites, apps or other software.

NOTE 2 Examples of external devices include scales and blood pressure devices not native to the app.

NOTE 3 Examples of other software include Electronic Health Records, Personal Health Records and web services.

NOTE 4 Examples of suitable specifications for external devices are published by Personal Connected Health Alliance,[50] Bluetooth Low Energy (BLE), and ANT Wireless (ANT+)[35].

NOTE 5 Suitable standards for interfaces to health software are published by IEC, ISO, CEN, IEEE™[4], HL7®[6], IHE®[6], DICOM®[6] and GS1®[6].

NOTE 6 'Not applicable' indicates that the health app does not have APIs.

5.5.2.2 Are potential customers and users of the health app able to access the specifications and implementation guides for the terminology or terminologies used?

CONDITION: 5.5.2.1 Yes or No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No

EVIDENCE: Regular access to specifications and implementation guides for the terminology or terminologies used

[4] IEEE is a registered trademark of Institute of Electrical and Electronics Engineers. HL7 is the registered trademark of Health Level Seven International. IHE is the trademarks of the Healthcare Information Management Systems Society in the United States and trademarks of IHE Europe in the European Community. DICOM is the registered trademark of the National Electrical Manufacturers Association for its standards publications relating to digital communications of medical information. GS1 is a registered trademark of GS1 Switzerland.

While such technical details are not relevant to all users, they can for example be used for assessing compatibility of the health app with other systems in a health service.

NOTE Examples of suitable terminologies used for coding health information include Systematized Nomenclature of Medicine - Clinical Terms (SNOMED-CT®[5]), Logical Observation Identifiers Names and Codes (LOINC®[7]) and International Statistical Classification of Diseases and Related Health Problems (ICD).

5.5.2.3 Does the health app validate all data for the health app transferred via APIs?

CONDITION: 5.5.2.1 Yes or No

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Mechanism to ensure tested endpoint identity verification (OWASP: Android^{TM}, MSTG-Network-3, iOS®: MSTG-Network-2)

Data validation testing is the task of testing all the possible forms of input to understand if the application sufficiently validates input data before using it. Data validation testing shall include software running on associated services if applicable.

If the health app collects or receives quantitative data, the precision (accuracy, granularity) of measurements (e.g. physical activity, physiological data from connected devices) shall be documented and justified as appropriate for the intended use of the app [32].

NOTE ‘Not applicable’ indicates that the health app does not use data from other sources.

5.5.2.4 Can users obtain their health related PII by a data export to another platform?

CONDITION: 5.4.1.1.1 Yes

PURPOSE: Colour coding

RESPONSE OPTIONS: Yes/No/Not applicable

EVIDENCE: Overview health related data eligible for data export, screenshots of the functionality data export, and sources of the screenshots

Data should be exported in a standard exchangeable format.

NOTE 1 E.g. if a device and potentially platform is replaced or if the app is uninstalled in favor of another product.

NOTE 2 ‘Not applicable’ indicates that the health app does not have newly gathered health related PII.

NOTE 3 This is referred to as data portability.

[5] SNOMED CT is the registered trademark of International Health Terminology Standards Development Organization. LOINC is the registered trademark of Regenstrief Institute.

Annex A
(normative)

Health app quality label

A.1 General

The health app quality label shall conform to the requirements in A.2 to A.6.

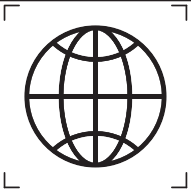
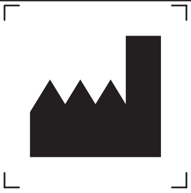
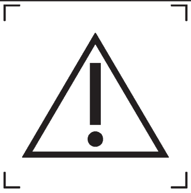
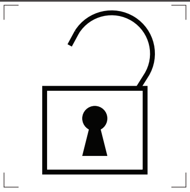
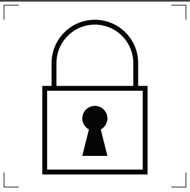
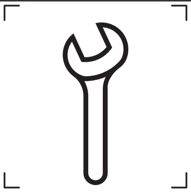
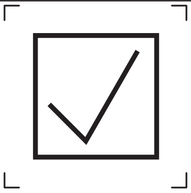
A.2 Content

The health app quality label shall contain blocks from left to right, top to bottom as indicated in Figure A.1, with icons used in the order of appearance as indicated in Table A.1:

- Flag or logo of the app assessor or the health authority or entity that commissions app assessment and Text 'Health app quality label' or a language with the same connotation;
- Dotted line;
- App icon (see 5.1.1.3), App name (see 5.1.1.2);
- Icons Operating systems or platforms the health app supports (see 5.1.1.1);
- Icon Manufacturer and App manufacturer name (see 5.1.2.1);
- Dotted line;
- Header 'Benefit of the app' or a language with the same connotation;
- Text Health benefit of this specific app (see 5.2.4.1);
- Icon Warning sign and Text Check [here] when app requires approval from a health professional before use (see 5.2.2.4) or a language with the same connotation;
- Background for quality rating blocks 'Healthy and safe', 'Easy to use', 'Secure data' and 'Robust build' with at the bottom a downward arrow;
- Header 'Healthy and safe' or a language with the same connotation;
- Healthy and safe rating block;
- Header 'Easy to use' or a language with the same connotation;
- Easy to use rating block;
- Header 'Secure data' or a language with the same connotation;
- Secure data rating block;
- Header 'Robust build' or a language with the same connotation;
- Robust build rating block;
- Header 'Overall health app quality score' or a language with the same connotation;
- Overall health app quality rating block;
- Icon Checked and Text 'App checked on [date]' or a language with the same connotation.

— Label identifier ‘ISO/TS 82304-2’

Table A.1 — Names and descriptions of icons used in the health app quality label

Icon	Title and description
	Title: Platform icon Description: On the health app quality label, to indicate that the health app supports Apple®[a], Android™ or another platform.
	Title: Web app On the health app quality label, to indicate that the health app runs in web browsers. Symbol: ISO 7000-3193
	Title: Manufacturer On the health app quality label, to identify the manufacturer of the health app. Symbol: ISO 7000-3082
	Title: Caution On the health app quality label, to indicate that the health app requires approval from a health professional for use. Symbol: ISO 7000- 0434A
	Title: Unlocking On the health app quality label: to indicate the ‘less secure data’ quality score for the health app. Symbol: ISO 60417-5570
	Title: Locking On the health app quality label: to indicate the ‘secure data’ quality score for the health app. Symbol: ISO 60417-5569
	Title: Call for maintenance On the health app quality label: to indicate the ‘robust build’ quality score for the health app. Symbol: ISO 7000-0717
	Title: Date of third-party assessment Description: On the health app quality label, to indicate the last date the health app has been assessed. Symbol: ISO 7000-1940

[a] Apple® is the registered trademark of a product supplied by Apple. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of the product named. Equivalent products may be used if they can be shown to lead to the same results

A.3 Dimensions

The label shall be at minimum 350 px wide. Where the label is printed in a larger format, it shall remain proportionate to the specifications provided.

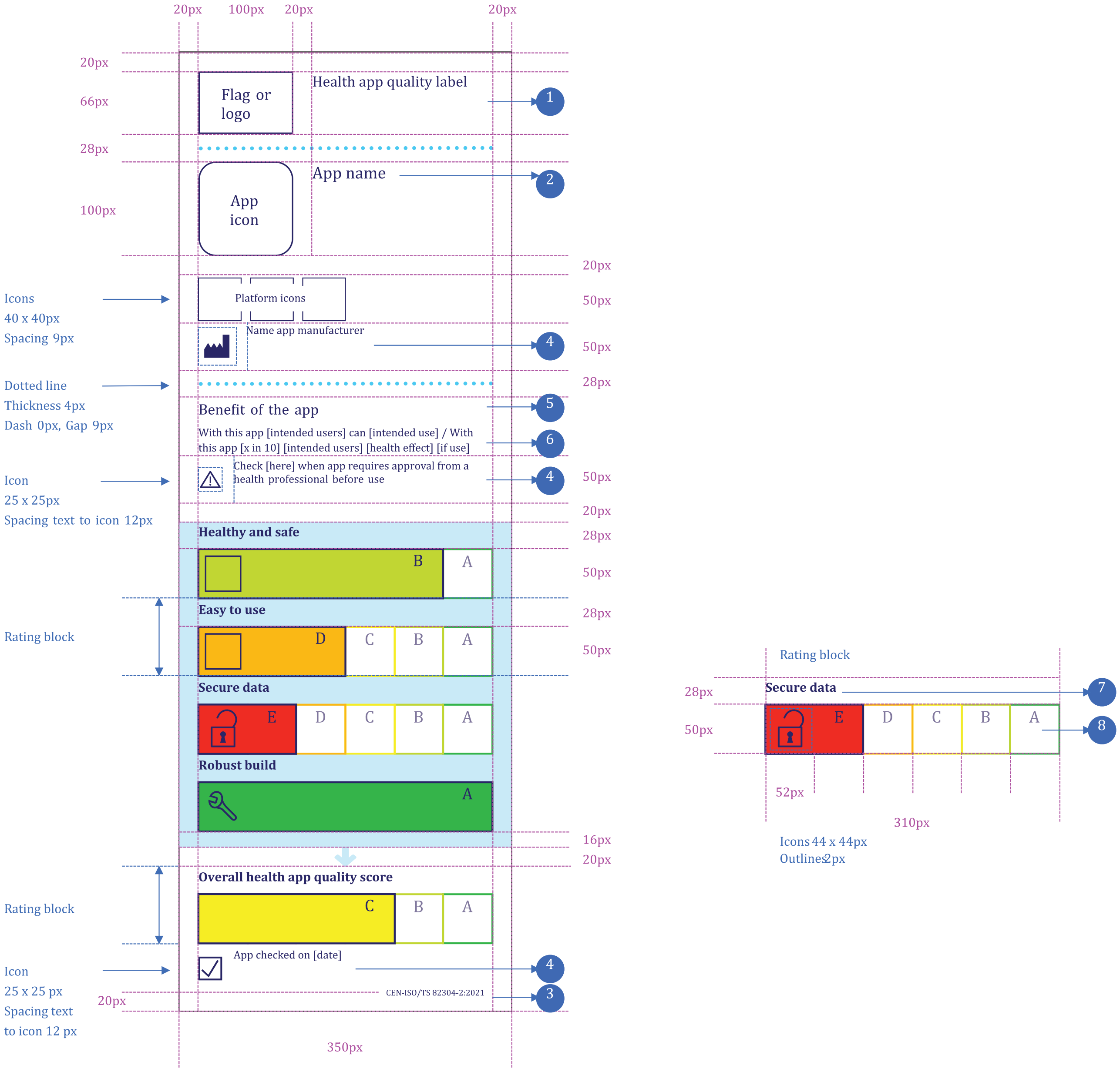


Figure A.1 — Label dimensions

A.4 Text

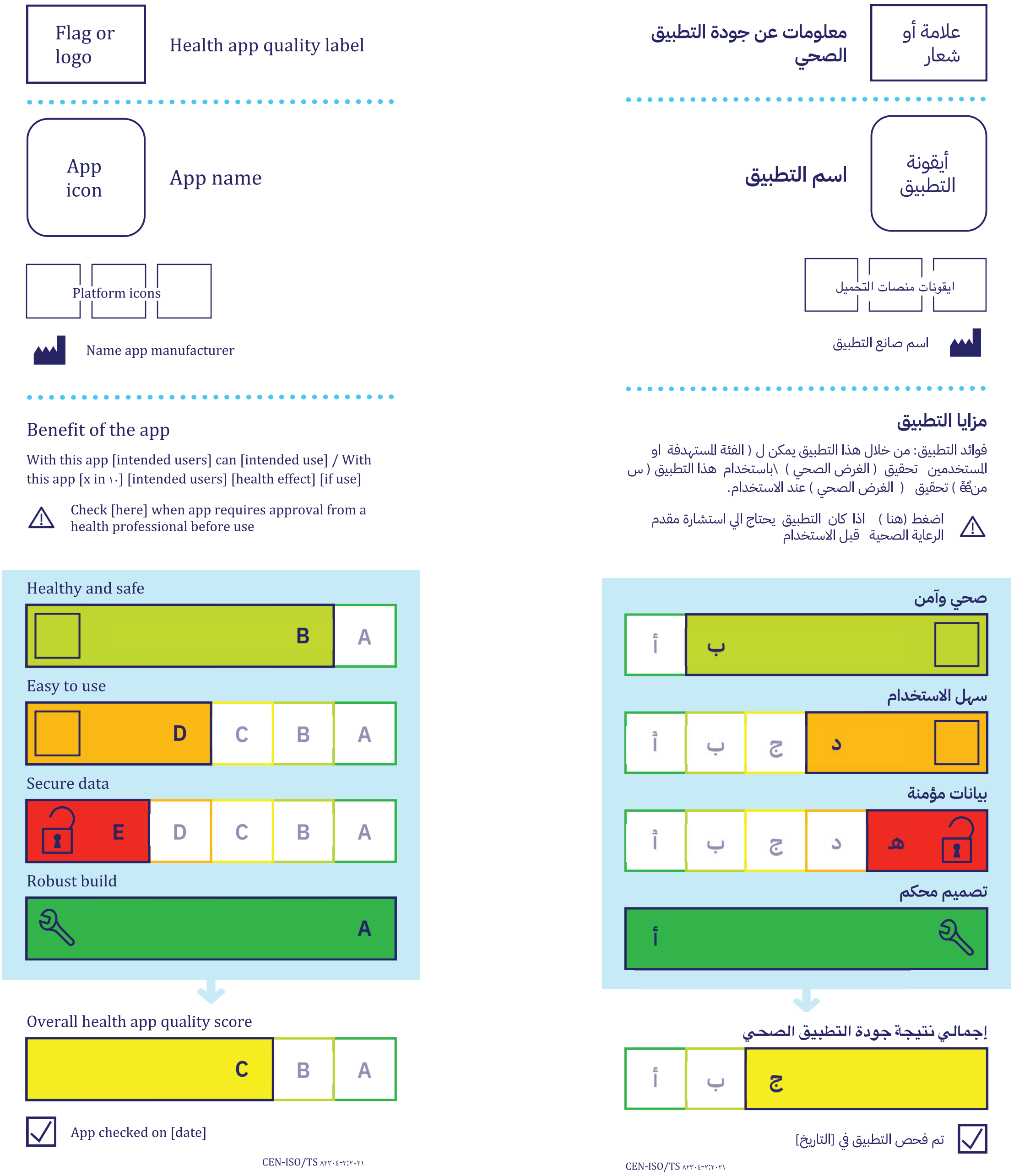
The text shall follow the requirements in Table A.2.

Table A.2 — Text requirements

	Number of (Latin) characters	Typeface	Font size	Line spacing	Alignment
1	Maximum 40 characters	Any	In the example 16px	In the example 20px	Vertical centred
2	Maximum 60 characters	IBM Plex Sans SemiBold	18px	22px	Vertical centred
3	--	IBM Plex Sans Regular	7px	9px	Vertical centred
4	Maximum 130 characters	IBM Plex Sans Regular	12px	14px	Vertical centred
5	Maximum 40 characters	IBM Plex Sans SemiBold	16px	20px	Top aligned
6	Maximum 200 characters	IBM Plex Sans Regular	12px	14px	Top aligned
7	Maximum 40 characters	IBM Plex Sans Bold	14px	16 px	Bottom aligned
8	--	IBM Plex Sans SemiBold	18px	-px	Horizontal centred Vertical centred

A.5 Languages

The label can be used with different character sets and script directions, for example Arabic right to left, within a maximum number of characters. Languages of the label and icons shall be tested with local low health literates for adequate understanding. Labels shall use the below typefaces for Latin languages and if available typefaces from the same family for non-Latin languages. Figures A.2 and A.3 provide illustrations.

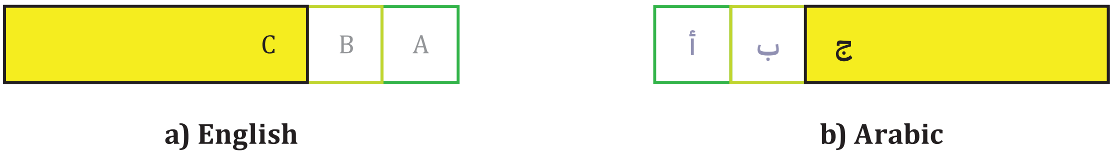

Flag or logo
Health app quality label
App icon
App name
Platform icons
Name app manufacturer
Benefit of the app
With this app [intended users] can [intended use] / With this app [x in ١٠] [intended users] [health effect] [if use]
Check [here] when app requires approval from a health professional before use
Healthy and safe
B
A
Easy to use
D
C
B
A
Secure data
E
D
C
B
A
Robust build
A
Overall health app quality score
C
B
A
App checked on [date]
CEN-ISO/TS ٨٢٣٠٤-٢:٢٠٢١
علامة أو شعار
معلومات عن جودة التطبيق الصحي
أيقونة التطبيق
اسم التطبيق
ايقونات منصات التحميل
اسم صانع التطبيق
مزايا التطبيق
فوائد التطبيق: من خلال هذا التطبيق يمكن ل (الفئة المستهدفة) او المستخدمين تحقيق (الغرض الصحي) باستخدام هذا التطبيق (س من (تحقيق (الغرض الصحي) عند الاستخدام.
اضغط (هنا) اذا كان التطبيق يحتاج الي استشارة مقدم الرعاية الصحية قبل الاستخدام
صحي وآمن
ب
أ
سهل الاستخدام
د
ج
ب
أ
بيانات مؤمنة
ه
د
ج
ب
أ
تصميم محكم
أ
إجمالي نتيجة جودة التطبيق الصحي
ج
ب
أ
تم فحص التطبيق في [التاريخ]
CEN-ISO/TS ٨٢٣٠٤-٢:٢٠٢١

a) English

b) Arabic

Figure A.2 — Labels

If the label is used in a digital marketplace or repository, the appropriate label shall be shown on the display mechanism in proximity to the price of the product. The size shall be such that the label is clearly visible and legible and proportionate to the size specified for the standard label. The label can be rendered using a nested display. The image used for accessing the label in the case of nested display, as indicated in Figure A.3, shall be a copy of the overall health app quality rating block.



a) English

b) Arabic

Figure A.3 — Nested labels

If nested display is applied, the label shall appear on the first mouse click, mouse roll-over or tactile screen expansion on the image and the sequence of display of the label shall be as follows:

a) The image referred to in Figure A.3 shall be shown on the display mechanism in proximity to the price of the product.

b) The image shall link to the label set out in Figure A.1 or a language such as displayed in Figure A.2.

c) The label shall be displayed after a mouse click, mouse roll-over or tactile screen expansion on the image.

d) The label shall be displayed by pop up, new tab, new page or inset screen display.

e) For magnification of the label on tactile screens, the device conventions for tactile magnification shall apply.

f) The label shall cease to be displayed by means of a close option or other standard-closing mechanism.

g) The alternative text for the graphic, to be displayed upon failure to display the label, shall be the overall health app quality score in a font size equivalent to that of the price.

The app manufacturer shall make the appropriate health app quality report available on the display mechanism in proximity to the price of the health app. The size shall be such that the health app quality report is clearly visible and legible. The health app quality report can be displayed using a nested display. In which case the link used for accessing the health app quality report shall clearly and legible indicate ‘Health app quality report’. If nested display is used, the health app quality report shall appear on the first mouse click, mouse roll-over or tactile screen expansion on the link.

A.6 Colour scheme

The background of the label shall be 100% white. Colours shall be in RGB, HEX or CMYK, according to Table A.3.

Table A.3 — Colour scheme

	RGB	HEX	CMYK
All text except for yet attainable scores in the rating blocks, the dotted lines and the label identifier	38 33 104	#262168	100 100 28 17
All icons	38 33 104	#262168	100 100 28 17
Outline coloured bar score	38 33 104	#262168	100 100 28 17
Yet attainable scores in the rating blocks (if score is E: A, B, C, D)	38 33 104 (opacity 50 %)	#262168 (opacity 50 %)	100 100 28 17 (opacity 50 %)
Dotted lines and vertical label identifier	77 200 239	#4DC8EF	58-0-2-0
Background square with downward arrow at the bottom	199 237 249	#C7EDF9	20-0-2-0
Colour bar A-score or outline if not yet attained	0 193 30	#00C11E	76-0-100-0
Colour bar B-score or outline if not yet attained	193 214 46	#C1D62E	29-1-100-0
Colour bar C-score or outline r if not yet attained	254 242 5	#FEF205	4-0-93-0
Colour bar D-score or outline if not yet attained	251 185 19	#FBB913	1-29-100-0
Colour bar E-score	255 29 0	#FF1D00	0-96-100-0

Annex B
(normative)

Health app quality score calculation method

The health app quality score is calculated using the following method:

— Check that all questions identified as ‘Required’ in Table B.1 are either not applicable or have been answered positively. If this is not the case, then no label or quality score shall be provided;

— For each aspect of quality (‘Healthy and safe’, ‘Easy to use’, ‘Secure data’, ‘Robust build’) take the sum of the ‘Weight’ values in Table B.1 for all the questions that have a positive answer or are not applicable. This total is the quality number for each aspect;

— Use Table B.2 to determine the quality score (A-E) that corresponds with the quality number for each aspect of quality;

— Multiply the quality number for each aspect of quality by the weight provided in Table B.3, and sum the values to obtain the overall quality number for the health app;

— Use Table B.4 to establish the overall health app quality score (A-E) that corresponds with the overall quality number for the health app.

Table B.1 — Individual quality requirements scoring table

	Weight
Healthy and safe	
5.2.1.2 Are age restrictions of the intended users or subjects of care made clear to potential customers and users?	1
5.2.1.5 Are assessments done to establish whether the health app is a medical device or in vitro diagnostic medical device, and if applicable is regulatory approval obtained before the app is made available in each country?	3
5.2.1.6 Are health professionals involved in the development of the health app?	3
5.2.1.7 Is appropriate peer reviewed scientific literature used in the development of the health app?	2
5.2.2.1 Are the health risks of the health app analysed?	Required
5.2.2.2 Are measures used to control the health risks of the health app?	1
5.2.2.3 Are the residual risks of using the health app found to be acceptable?	1
5.2.2.5 Are potential customers and users of the health app made aware of the health risks, contra-indications and limitations of use?	Required
5.2.2.6 Is a process to collect and review safety concerns and incidents for the health app maintained?	3
5.2.3.1 Are ethical challenges of the health app assessed and documented with intended users and health professionals?	1
5.2.3.2 Is the health app approved by an independent ethics advisor or ethics advisory board?	1
5.2.4.2 Are potential customers and users made aware of the health interventions applied to achieve the health benefit?	2
5.2.4.3 Are potential customers and users made aware of all financial costs to achieve the health benefit?	1
5.2.4.4 Are potential customers and users made aware of the need for support of a health professional to achieve the health benefit?	2
5.2.4.5 Is evidence available to support the health benefit of using the app?	Required

Table B.1 *(continued)*

	Weight
5.2.4.5.1 Does this evidence include peer reviewed research involving the use of this health app?	1
5.2.4.5.2 Is the level of the evidence appropriate?	2
5.2.4.6 Is there a maintenance process for the health information in the app?	1
5.2.4.6.1 Are all sources for the health information in the health app disclosed to potential customers and users?	2
5.2.4.7 Are all sources of funding of the health app disclosed to potential customers and users?	1
5.2.4.8 Is the use of advertising mechanisms disclosed to potential customers and users and are advertisements clearly distinguishable in the health app?	3
5.2.5.1 Is evidence available of a societal benefit of using the app?	1
5.2.5.1.1 Does this evidence include peer reviewed research involving the use of this health app?	1
Easy to use	
5.3.1.1 Is the health app WCAG 2.1 AA or AAA compliant?	3
5.3.1.1.1 Are reasonable measures taken to ensure that all intended users can perceive all relevant information and user interface components of the health app and related documents?	1
5.3.1.1.2 Are reasonable measures taken to ensure that all intended users can operate all relevant user interface and navigation components of the health app and related documents?	3
5.3.1.1.3 Are reasonable measures taken to ensure that all intended users can understand all relevant information and user interface components of the health app and related documents?	3
5.3.1.2 Is the health app age-appropriate?	2
5.3.2.1 Is the health app design based on an explicit understanding of users, tasks and environment?	2
5.3.2.2 Are intended users involved throughout design and development of the health app?	2
5.3.2.3 Is the design of the health app driven and refined by user-centred evaluation?	2
5.3.2.4 Are measures in place to avoid user error and reasonably foreseeable misuse of the health app?	1
5.3.2.5 Are potential customers and users provided with adequate product information about the health app?	1
5.3.2.6 Are instructions for use readily available for users?	3
5.3.2.7 Are appropriate resources available to adequately help potential customers and users who experience problems with the health app?	1
5.3.2.8 Is relevant data on the usability of the health app systematically gathered throughout its entire lifetime, in order to make regular improvements?	1
Secure data	
5.4.1.1.2 Is data minimization applied in the health app?	3
5.4.1.1.3 Is an appropriate retention policy established to erase or review the data stored?	1
5.4.1.1.4 Is a privacy statement readily available to potential customers and users of the health app?	Required
5.4.1.1.4.1 Does the privacy statement start with an accessible overview in less than 150 words?	3
5.4.1.1.5 Are contracts in place with all processors and controllers of PII of the health app and associated services to ensure the level of security controls and privacy protection are as communicated to the user?	3
5.4.1.1.6 Is opt-in the default setting for sharing PII with third parties?	3
5.4.1.1.7 Does the app manufacturer have a person responsible for legal and regulatory compliance of processing of PII?	1
5.4.1.1.8 Are security-incident response procedures in place that include reporting PII breaches to the user and relevant authorities?	3

Table B.1 *(continued)*

	Weight
5.4.2.1 Have the health app manufacturer and all organizations providing associated services implemented and documented the implementation of ISO/IEC 27001?	1
5.4.2.2 Is an Information Security Risk Assessment documented?	1
5.4.2.3 Is a secure by design process followed?	3
5.4.2.4 Are measures in place to ensure that all third-party software libraries and other software components for the health app are reliable and maintained?	1
5.4.2.5 Is a process to prevent unauthorized access and modifications to the health app source code in place and documented?	2
5.4.2.6 Are organizational measures in place to ensure PII is processed in a manner that is compatible with the explicit, legitimate purposes specified in the privacy statement?	2
5.4.2.7 Is user authentication, authorization and session management implemented to secure access to the health app?	1
5.4.2.8 Does the health app transmit and store all PII with adequate encryption?	1
5.4.2.9 Are security vulnerabilities reported, identified, assessed, logged, responded to, disclosed, and quickly and effectively resolved?	3
5.4.2.10 Are the security of the health app and associated services tested on a regular basis and at major changes?	2
5.4.2.11 Is the information security policy readily available to potential customers and users?	1
Robust build	
5.5.1.1 Are all the health app product requirements documented?	1
5.5.1.2 Is the health app developed with a software development process that covers the standards, methods and tools to be used?	3
5.5.1.3 Is a secure coding standard followed and documented?	2
5.5.1.4 Is a configuration management plan established for the health app?	1
5.5.1.5 Are processes in place to deal with a significant increase or spike in demand?	1
5.5.1.6 Is a validation and verification plan documented and used for the health app?	3
5.5.1.7 Is a release and deployment process established?	1
5.5.1.8 Is a maintenance process established?	3
5.5.2.1 Are potential customers and users of the health app able to access the specifications and implementation guides for all the APIs?	1
5.5.2.2 Are potential customers and users of the health app able to access the specifications and implementation guides for the terminology or terminologies used?	1
5.5.2.3 Does the health app validate all data for the health app transferred via APIs?	1
5.5.2.4 Can users obtain their PII by a data export to another platform?	1

Table B.2 — Numeric thresholds for each of the four aspects of quality in the label

Quality score	**A**	**B**	**C**	**D**	**E**
Healthy and safe	30 to 33	27 to 29	24 to 26	20 to 23	0 to 19
Easy to use	23 to 25	20 to 22	18 to 19	15 to 17	0 to 14
Secure data	32 to 35	28 to 31	25 to 27	21 to 24	0 to 20
Robust build	18 to 19	16 to 17	14 to 15	12 to 13	0 to 11

Table B.3 — Weight of the four aspects of quality in Overall health app quality score

Quality aspect	Weight
Healthy and safe	5
Easy to use	1,5
Secure data	2,5
Robust build	1

Table B.4 — Numeric thresholds overall health app quality score

Quality score	A	B	C	D	E
Overall health app quality score	279 to 309	248 to 278	217 to 247	186 to 216	0 to 185

Annex C
(informative)

Rationale

This document covers health and wellness apps, whether or not they are regulated as medical devices. In this it follows the same approach as IEC 82304-1, which has a scope of ‘health software’.

The title of this document mentions ‘health and wellness apps’, rather than ‘health apps’, which is the term used throughout the document. The terms ‘health app’ and ‘health and wellness app” are synonyms. The title was chosen to reflect the categories that exist in widely used app stores and libraries, and to make it clear that it is not just dealing with medical or clinical apps, and apps that are endorsed by health professionals or healthcare organizations. The scope also includes apps that are used to improve physical, mental or emotional health and wellbeing. The term ‘health app’ has been used throughout the document for brevity, and to be consistent with the use of ‘health software’ and in IEC 82304-1, rather than ‘health and wellness software’.

This document applies to all health and wellness apps, whether or not they are regulated as medical devices. Research in the Netherlands evaluating a selection of health apps found that 79 % of these health apps were not judged to be medical devices according to the EU’s Medical Device Regulation.[67]

Every health app is health software as defined in IEC 82304-1, and any health software that is an app is a health app as defined in this document. For a further discussion of the scope of health software see IEC 82304-1:2016, Annex A. The boundary between software that is considered to be an app, and software that is not an app is unclear and changes over time. This document can be used with products that are put on the market as health apps and with any health software that is placed on the market as an app.

This document considers the quality characteristics and information required to identify a health app described in UNI/TR 11708.

The quality characteristics for the ‘Quality in use’ model from ISO/IEC 25010:2011, 3.2, informed the development of this document. These are: Effectiveness, Efficiency, Satisfaction and Risks Mitigation. A subset of the characteristics from the product quality model in ISO/IEC 25010, 3.3, were also taken into account. These are: Functional suitability, Usability and accessibility, Interoperability, Reliability, Security, and Authenticity.

The document has also been informed by characteristics of data quality defined in ISO/IEC 25012 such as: Confidentiality, Credibility, Accuracy, Traceability, Completeness, Precision, Understandability, Accessibility, Availability and Recoverability.

This document has been developed alongside the HL7® Consumer Mobile Health Application Functional Framework (cMHAFF).[32] Where possible, both documents use the same definitions and criteria. However, there are differences in the granularity and focus of the criteria, and so a simple and direct mapping between the criteria is not possible in the current versions of the specifications.

Annex D
(informative)

Product safety and lifecycle process recommendations

D.1 General

This annex provides additional guidance for the application of IEC 82304-1 and relevant clauses from IEC 62304 to health apps. It does not add to or modify those requirements.

NOTE 1 IEC 82304-1 defines the requirements for health software product safety and contents of user documentation ('accompanying documents') of health software and so applies to health apps.

NOTE 2 IEC 62304 defines the software lifecycle processes that can be undertaken and documented when developing health software. A number of clauses in IEC 62304 are included as requirements for health software in IEC 82304-1, and so also apply to health apps.

D.2 Product Safety Requirements from IEC 82304-1

D.2.1 General requirements and initial risk assessment

This subclause provides additional recommendations in IEC 82304-1:2016, 4.1.

When documenting the intended use of the health app, the app manufacturer should address the following questions:

a) Who are the intended users of the app?

b) Who are the subjects of care of the app?

c) What problem is the app trying to solve?

d) What are the health and wellness outcomes that can be achieved?

e) What are (scenarios of) typical uses of the app?

All requirements identified by the manufacturer should be traceable throughout the app project life cycle in accordance with ISO/IEC/IEEE 90003.

D.2.2 Health software product use requirements

This subclause provides additional recommendations in IEC 82304-1:2016, 4.2.

Health app use requirements identified by the manufacturer. The health software use requirements should address the following questions and aspects:

a) General aspects:

   1) What data is the app intended to process?

   2) Explicit limitations relating to the requirements or use of the health app.

b) Support and maintenance requirements for the anticipated life of the health app.

c) The impact on users of discontinuing support for the app and planning for this. The impact of withdrawing the app from app repositories or other distribution channels.

d) Functional requirements of the app should be determined using case studies and user stories, and should include information about the app's relevance to the following types of care, specifically how the app enhances or inhibits such care:

   1) self-directed care;

   2) informal care;

   3) professional care.

e) Age-appropriate functionality should be considered.

f) Interface requirements should address the compatibility of the app with different platform configurations and the ways that information collected or used by the app can be reused, under appropriate privacy controls.

g) User interface requirements should consider accessibility for different types of users, and how using the app might fit in with related activities that the user performs.

h) App load and response times, and other time related behaviours should be addressed and cover both the performance of the app itself, and the supporting infrastructure, such as web services that the app can rely on.

i) The app manufacturer should research current compliance regulations governing, for example medical devices, data protection and other relevant standards, and include these processes in the requirements. Requirements stated by the applicable regulations should also be included in the analysis. Among others the following methods should be applied:

   1) a review of existing publications, including academic research on user needs and practices published in specialist magazines, conference proceedings and journals;

   2) interviews with representatives of all intended user groups, to understand how intended users currently achieve the purpose intended for the app.

D.2.3 System requirements

The system requirements for the health app should consider the following, as appropriate:

a) If the app is intended for use by children, then the content should be appropriate, if not then the app publisher should take steps to make it available only to the intended users. Apps can be used by children in a variety of ways, including alone, under supervision, or indirectly with an adult mediating between the child and the app. The requirements analysis should take this into account where relevant.

   NOTE 1 Many platforms can provide facilities to support managing distribution of age-restricted apps in a consistent way.

b) For apps that can be used on a device that has intermittent network connectivity, the requirements should address how this is likely to impact the use of the app.

   NOTE 2 This can highlight associated risks to track (see Clause 6).

c) Documented alternatives for the user if the app is temporarily or permanently not available, such as using paper notes should be addressed.

d) App load and response times, and other time related behaviours should be addressed.

e) Requirements for confidentiality, data integrity, non-repudiation, accountability and authenticity should be addressed.

f) If the health app shares data that is intended to be anonymized, the app manufacturer should document how anonymity will be maintained, taking into account the ways that the data can be combined with other data and contextual information. The assumption should be that information subjects are indirectly identifiable unless the app publisher can show otherwise. Where the information subject is indirectly identifiable, the data should be treated as personal data.

g) Standards and industry guidance should be used for health information where the app shares information or is used alongside other information systems.

h) An effective mechanism should be provided for uninstalling the app and if appropriate, making data collected by the app available to the user so that the app can be replaced.

i) If appropriate, how the user can transfer the app and associated data onto another device or platform should be described, or the app should be made usable on multiple devices with the same data.

j) Requirements for upgrading the app should be considered, including what mechanisms are needed to inform the user that upgrades are available. In some cases, the app might require the user to regularly check for and install upgrades in order to continue using the app. The benefits of ensuring that current content and functionality is available should be weighed against the risks that this sometimes causes the app to be unavailable for its intended use.

k) The system requirements should take account of reasonable demands for reliability, performance and scalability

l) The system requirements should include mechanisms for detecting when performance is outside of the acceptable range, so that the user and/or app publisher can take appropriate action.

m) The user interface for the app should include a way to access the app's privacy statement.

n) The app should ensure that personal information collected by the app is kept secure, and that it is processed according to the privacy statement.

o) If advertising is delivered through or alongside the app, there is a risk that the advertising could pop-up, obscure, interfere with or be mistaken for information provided by the app. health apps should be designed in a way that such issues do not arise when health information is being displayed on the user's device.

p) Where the user is prompted to enter data, implausible values should be tested for and handled appropriately, for example by prompting the user to confirm.

q) Where there are calculations made in the app, implausible results should be tested for and handled appropriately, for example by informing the user.

r) The health app should include tests for the configuration of the platform that the app is running on, so that the user can be informed if the platform is not supported.

s) The installation process of the health app should verify that:

   1) the installation is taking place on a supported platform and the platform version identifier. A health app might only function as intended if other apps or services upon which it is dependant are available. If this is the case, then this should be explicitly included in the requirements, with appropriate behaviours defined for when the apps or services are not available. It should be stated if there are other apps or services which can add functionality to the app if available. If there are any such apps or services, then the following information should be included in the requirements:

      i) version information;

      ii) functionality from the app or service that is likely to be supported;

      iii) which parts of the app or service API are likely to be used;

   NOTE For example, a health monitoring app could support posting information to some GP information systems if there is a connector for the GP system available to the app. The product description might state which GP systems are supported so that the user can make an informed decision.

2) that any required apps or services are available;

3) if there are required items missing then:

   i) the installation process should install the missing components if possible;

   ii) if this cannot be done immediately as part of the installation process then an informative message should be displayed to the user, with any installed components removed;

4) the user's device returned to the state that it was in before the installation was attempted.

t) Miscellaneous:

1) A health app should take advantage of the features of the selected platform, where possible, to provide a consistent user experience and to minimize the need for reinvention of functionality. The design should take into account the user needs, and the advantages and disadvantages of such reuse should be considered by the app manufacturer in the context of the intended use for the app;

2) Consider country-specific measurement units;

3) Memory and processor power requirements should be addressed;

4) Data storage requirements, whether directly accessible in the app platform, or available as networked resources should be addressed.

D.2.4 Health software product use requirements and health software product system requirements

This subclause provides additional recommendations in IEC 82304-1:2016, 4.4.

Any functional requirements discovered during the design phase should be added to these documents as applicable.

D.2.5 Software life cycle processes

This subclause provides additional recommendations in IEC 82304-1:2016, Clause 5.

IEC 82304-1:2016, Clause 5 requires the application of IEC 62304+AMD1:2015, Clauses 5 to 8. Subclause 4.3 provides further details on the application of these clauses.

D.2.6 Product validation

This subclause provides additional recommendations in IEC 82304-1:2016, Clause 6.

The app manufacturer should retain all protocols, results and evidence of testing in accordance with IEC 82304-1:2016, 6.5, including, clinical benefits. During testing evidence should be collected to validate any clinical benefits that the app's intended use delivers.

The app manufacturer should test each iteration of the health app with all relevant user groups. Data collected from all user tests should be collated, analysed and the results used to inform the final quality gate decision as to whether the app is fit for purpose and can be released in accordance with IEC 62304+AMD1:2015,4.2.

Validation should apply to both the app and accompanying documentation.

The app should be tested on all the platforms that it is planned to be released on.

The validation plan should describe what testing is to be done when there is a change to the accompanying documentation, app or to a platform that it runs on.

All Health software product use requirements should be tested as early as possible in the app project, and include the following methods:

a) a review of existing publications, including academic research on user needs and practices published in specialist magazines, conference proceedings and journals;

b) the review of wireframes and prototypes of the app;

c) evaluating similar apps that are available in the target app repository or other app repositories;

d) field testing of the app.

NOTE 1 Where an iterative methodology is used, field testing of early releases can be used to inform the requirements for subsequent releases of the app.

NOTE 2 The number of users able to use early versions of the app can be controlled by issuing activation codes if the app repository does not provide other means for the app publisher to restrict access to a limited group of test users.

For each of the requirements defined in 4.2, test results should be documented.

D.2.7 Product identification and accompanying documents

This subclause provides additional recommendations in IEC 82304-1:2016, Clause 7.

The app manufacturer should ensure the integrity of the accompanying documentation. For example, modification of the content during its publication by digital distribution services should be prevented.

NOTE 1 Instructions for use includes documents that the user is expected to be available to the user. Technical description is material that is relevant for example for admin, installation, etc.

A privacy statement should be provided as part of the instructions for use.

Personal data that is used or collected by the app should be described in the privacy statement document. This includes information about the user, the subjects of care or wellbeing, or other subjects.

The privacy statement should describe:

— the information to be captured or used by the app;

— whether the information is likely to be stored (on or off a mobile device);

— the sharing of any personal data including sharing with other apps or medical app repositories.

— where any stored information is held – takes into account backups, information synchronized between devices and information on incomplete transactions;

— what triggers the removal of personal data that is no longer relevant to the intended use of the app;

— what happens to personal data when the user choses to delete the app. If not all data is deleted, this should be made clear in the Privacy Statement.

The instructions for use should describe how the user is able to control the sharing of data.

This should be included in requirements for use: how the user should be informed about and be able to manage.

Where the intended use and design of a health app is based on existing clinical evidence, the evidence that supports claims or propositions of any medical or health benefits by using the app, should be made available in the health software description, where appropriate.

NOTE 2 For example, for mental health apps, an explicit reference to any underlying psychological approach employed might be useful to the intended user.

D.3 Product life cycle requirements from IEC 62304+AMD1:2015

D.3.1 Software development standards, methods and tools planning

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 5.1.4.

The requirements of IEC 62304+AMD1:2015, 5.1.4 should also be applied to class A and class B softwares.

D.3.2 Documentation planning

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 5.1.8.

The following project documentation should be created and maintained, if applicable, throughout the app project to provide a basis for governance during the project and supporting evidence upon completion:

— credentials – name and credentials of all human and/or institutional providers of information, including dates at which credentials were received.

— testing – a test plan should be created and maintained. The manufacturer should retain all protocols, results and evidence of testing. During testing, evidence should be collected to validate any clinical benefits that the app's intended use delivers.

NOTE 1 Documents relating to testing might be made available for contractual, regulatory or legal reasons.

NOTE 2 Such evidence might also be of use when tracking down faults that might have been introduced into the app during development or maintenance.

NOTE 3 Regulations can have impacts on how design decisions are documented.

D.3.3 Software configuration management planning

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 5.1.9.

Configuration management should be undertaken so that components of the app are consistently referenced in all project and user documentation, and to enable the management of issues encountered during use.

The configuration management plan should exist for the entirety of the app project life cycle.

NOTE 1 This can be a document created specifically for the project, a section within another project document such as a quality plan, or it can be a policy document that applies to many projects and products.

The configuration management plan should include, as a minimum, the following:

— a definition of the types of configuration items that are managed for the app;

NOTE 2 Examples of possible component types include: app screens, software modules, resource files, documents, document fragments, externally maintained apps, web services, risk register entries and app requirements.

NOTE 3 A component, for example, can be a document that includes a reference to a collection of document fragments.

— for each component type there should be a way to name or identify configuration items that are instances of that type;

NOTE 4 Many components can change without requiring a new identifier to be issued. In this case, a version identifier can be issued. For example, the welcome screen for an app might be changed as a result of feedback from users. If the welcome screen is reused across multiple apps, then a new version identifier can be issued. If it is only used on one app, then it might be sufficient to track the version identifier for the app as a whole.

- for each component type the configuration management plan should describe the criteria for issuing new component identifiers, and component version identifiers, and for describing how and where they should be used.

D.3.4 Software unit implementation

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 5.5.

For each of the requirements defined in IEC 62304+AMD1:2015, 5.2, test results should be documented. These tests should be used to verify that the app meets the requirement.

D.3.5 Software release

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 5.8.

An incremental release policy should be considered, where possible, so that the app is trialled by a limited number of users in pilot implementations before being made generally available.

D.3.6 Analyse change requests

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 6.2.3.

Proposed changes should be carefully assessed to identify the potential impact on:

- functional requirements such as safety and security related functions, compliance with technical standards and interoperability;
- non-functional requirements such as performance/scalability and usability;
- the intended use, user processes and training;
- project time scales.

D.3.7 Change control

This subclause provides additional recommendations to IEC 62304+AMD1:2015, 8.2.

Change requests to the app should be associated with new requirements or one or more problem reports identified in accordance with the software problem resolution process (IEC 62304+AMD1: 2015, Clause 9).

The approach taken for verifying changes should be designed to provide renewed assurance that any important safety, security or functional properties of the app are not adversely affected by the changes.

D.4 Product characteristics

Product characteristics should follow the following recommendations:

- The design should include mechanisms for detecting when performance is outside of the acceptable range, so that the user and/or app publisher can take appropriate action;
- The design should include tests for the configuration of the platform that the app is running on, so that the user can be informed if the platform is not supported;
- The user interface for the health app should include a way to access the health app's privacy statement;
- If advertising is delivered through or alongside the health app, there is a risk that the advertising could pop-up, obscure, interfere with or be mistaken for information provided by the health app. Health apps should be designed in a way that such issues do not arise when health information is being displayed on the user's device;

- Where the user is prompted to enter data, implausible values should be tested for and handled appropriately, for example by prompting the user to confirm;
- Where there are calculations made in the health app, implausible results should be tested for and handled appropriately, for example by informing the user;
- The functionality that is dependent upon the underlying platform, and so might need to be changed when the app is supported on a different platform, should be designed as a separate component and that can be replaced without affecting the rest of the app code.

For example if location information is needed, a ‘location’ component can be defined that provides a consistent interface for the rest of the app code, to whatever underlying platform services are used to obtain the location information. A modular design should be used.

The installation process of the health app should verify that:

- the installation is taking place on a supported platform and the platform version identifier;
- that any required apps or services are available.

If required items are missing:

- the installation process should install the missing components if possible;
- if this cannot be done immediately as part of the installation process, then an informative message should be displayed to the user, with any installed components removed.

Annex E
(informative)

Application profile – Contact tracing apps

E.1 General

E.1.1 Background

During a serious epidemic, it is important to trace people who have been in contact with patients of the infectious disease. Tracing contacts enables warning those people about a potential infection, even if they do not have any symptoms. They can provide information about control measures, such as the need for quarantine or getting tested, and monitoring these contacts regularly for symptoms. Contact tracing has traditionally been done with interviews of diagnosed individuals. Contact tracing apps can help trace such contacts. Apps can potentially support more rapid, efficient and effective contact tracing, compensating for our individual limits in recalling contacts and having contact details of these contacts, e.g. fellow passengers in public transport.

The impact of contact tracing apps on population health is dependent on the proportion of the population using it. The use of the app is typically voluntary. People are expected to use them only if they believe that these apps are useful for themselves, their society or both and that their privacy is sufficiently protected. Thus, the protection of the privacy of the users is a very important requirement for these apps. To expand the potential user base and be as inclusive as possible, the app should also be user friendly and accessible to people with disabilities, all platforms and older devices.

These apps are typically sponsored by national or regional governmental organizations or health authorities.

E.1.2 Typical operation of a contact tracing app

Although there are variations in contact tracing apps, their typical operation is as follows.

The user installs the app on his/her mobile phone. During the installation, the app generates an ID number for the user. This ID number is typically registered in a central database in an anonymized form, either during the installation of the app or when the user reports an infection in the app. During the installation, the app typically gives some basic information about the infection for which the app has been designed.

When an app user is near another app user, their smartphones store the other contact’s ID using encrypted communication. The duration of the contact needs to be sufficiently long (e.g. 15 minutes or more) and sufficiently close (e.g. 2 meters or less) to be registered. Being in a closed environment with a case, a third risk factor, is not something apps can currently detect.

If an app user gets a positive confirmation of an infection, the app user enters this information voluntarily into the app.

The app will retrieve the IDs of the contacts at risk of being infected.

Contacts at risk are informed and further information of recommended actions is given.

The IDs of the contacts that took place too long ago for an infection to be likely, are disposed of.

The app users have the right to stop the use of the app at any given time and have all their recorded information removed from their smartphone and central databases.

The application profile is based on the above scenario.

E.2 Guidance for contact tracing apps

E.2.1 This clause provides additional guidance when considering contact tracing apps.

E.2.2 (Subclause 5.1.2.1): If the contact tracing app is put on the market by a health maintenance organization, a government agency or an agency such as a third-party administrator, this is the app manufacturer. The creation and maintenance of the health app can be sub-contracted to an app development organization.

E.2.3 (Subclause 5.2.1.7): There can be limited peer reviewed literature available early in the outbreak, in which case it can be acceptable to use peer reviewed literature about similar infections, and evolving guidance from regional centres for disease prevention and control.

E.2.4 (Subclause 5.2.2.1): Examples of hazards include:

- the contact tracing app fails to register encounters;
- the app fails to correctly store infection status;
- there is a delay in providing infection status;
- users do not carry around their phone all the time or forget to charge their phone;
- the app displays outdated recommended actions;
- follow up information in the app is misinterpreted.

E.2.5 (Subclause 5.2.4.1): An example of how to phrase the health benefit for a contact tracing app is ‘With this app, anyone can anonymously log encounters that can pose a risk in spreading [subclause 5.2.1.3 health issue] and be promptly alerted for adequate follow up if other users they have encountered tested positive.’

E.2.6 (Subclause 5.2.4.2): The technology used, for example the Apple® and Google interoperable Exposure Notifications application programming interface, will typically be included in the description of the health intervention.

E.2.7 (Subclause 5.2.4.5): Health apps for contact tracing is a new area and there can be a lack of evidence of efficacy prior to deployment. Feasibility studies, simulations mimicking real life conditions, pilots and post market research with adequate ethical approval are among the measures to consider to fill this void prior to full rollout. Taking the time to run a pilot can accelerate successful wide scale update [41].

E.2.8 (Subclause 5.3.2.1): The design of the contact tracing app will typically avoid excessive power consumption and take account of the devices, platforms and versions used in different segments of the population.

E.2.9 (Subclause 5.3.2.4): Foreseeable misuse of a contact tracing app will typically include the user reporting that they are infected when this is not true. This can be mitigated by requiring that a verifiable test result identifier be provided.

E.2.10 (Subclause 5.3.2.5): The product information will typically make it clear to the user how the contact tracing app functions when the user moves between countries or regions.

E.2.11 (Subclause 5.4.1.1): Contact tracing apps do collect potentially identifiable personal information.

E.2.12 (Subclause 5.4.1.1.2): Data minimization will typically include:

- efforts to limit or exclude the use of location data in the detection of contacts, as location data can be used to identify individuals when combined with other available information;
- avoiding the requirement for users to register their use of the contact tracing app;
- frequently changing the anonymous ID of the user to protect their identity by reducing the number of contacts associated with each anonymous ID;
- limiting the information centrally held to the anonymous IDs generated by the contact tracing app. In particular the MAC address (media access control address) or IP address (internet protocol address) of the device is typically not needed since the contact tracing app can poll the central registry periodically to obtain any relevant alerts;
- careful consideration of any audit logs and similar activity records created by either the contact tracing app itself, or other services that it connects to. Audit logs will typically not include PII.

E.2.13 (Subclause 5.4.1.1.4): For contact tracing apps that operate in more than one region or country, the privacy statement will typically make clear how crossing borders affects the handling of PII.

E.2.14 (Subclause 5.4.1.1.6): When a person reports he or she is infected, contacts are typically notified of this fact without disclosing the identity of the infected individual. Sharing the identity of potentially infected individuals is expected to be a significant barrier to adoption and from an ethical point of view a risk for stigmatization.

E.2.15 (Subclause 5.4.2.2): The information security risk assessment will typically take into account the risk that the user can be identified when they seek additional information through the app after having received a contact warning from the app.

E.2.16 (Subclause 5.4.2.8): The identifiers generated by the contact tracing app are considered to be PII as they can facilitate data linkage. They will typically be generated using state-of-the-art cryptographic processes.

E.2.17 (Subclause 5.4.2.10): For contact tracing apps security testing will typically include testing by an external security testing organization, with the appropriate certificate being provided as evidence.

E.2.18 (Subclause 5.5.1.1): The product requirements for contact tracing apps will typically include:

- the ability to change the criteria for detecting significant contact. Examples of such criteria include the distance between individuals and the time that they are in close contact;
- a ‘Return to normal’ function to stop collecting contact data for all users of the contact tracing app.

E.2.19 (Subclause 5.5.1.6): Verification will typically include test result evidence that the distance measurement between the mobile phones works appropriately.

E.2.20 (Subclause 5.5.2.1): The documentation for the APIs will typically include an account of the protocols used, such as the Decentralized Privacy-Preserving Proximity Tracing (DP-3T) protocol, Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT) protocol, Temporary Contact Numbers (TCN) Protocol, or Blue trace protocol.

E.2.21 (Subclause 5.5.2.3): A contact tracing app will typically use endpoint identity verification to establish the identity of a central server if that is part of the contact tracing solution, and the server will similarly verify that the connection has come from an approved contact tracing app.

Annex F
(informative)

Ethical considerations in health apps

Health data is particularly sensitive information. It can identify individuals and reveal highly personal details of people’s lives. Tracking health data can be necessary for the general wellbeing of people (e.g. to track the spread of contagious diseases) or to adequately diagnose and treat diseases. How health apps collect and use data can have profound implications for the individual and society as a whole. The development and governance of health apps therefore requires careful ethical consideration.

While this document focusses on the responsibilities of app manufacturers, it is important to note that the adherence to ethical principles is a shared responsibility between app manufacturers, deployers and end-users. Each party has to take appropriate and well-defined steps within their control. Some cases even can require the general public or policy makers at regional or national level to be involved.

There are many ethical theories. The three mainstream theories are deontology, consequentialism and virtue ethics. Companies and institutions can use one or a combination of such theories. The High-Level Expert Group (HLEG) on Artificial Intelligence [40] has used the deontology framework to identify seven ethical principles for Artificial Intelligence. Although not all health apps apply artificial intelligence (AI), these ethical principles can also apply to other health apps.

HLEG developed a Fundamental Rights Impact Assessment (FRIA) and an Assessment List for Trustworthy AI (ALTAI). Tables F.1 and F.2 show the areas covered by the quality and reliability criteria set out in this document, with an indication of the relevant sections in this document.

Table F.1 — Mapping of Fundamental Rights Impact Assessment (FRIA) and values on quality and reliability criteria in this document

Fundamental Rights Impact Assessment (FRIA)	Relevant section in Clause 5
1. Discrimination	5.2.3 Ethics 5.2.4 Health benefit
2. Rights of the child	5.2.1 Health requirements 5.2.2 Health risks
3. Protection of personal data	5.4 Secure data
4. Freedom of expression and information and/or freedom of assembly and association	5.2.4 Health benefit 5.5.1 Technical robustness

Table F.2 — Mapping of ethical principles and values on quality and reliability criteria in this document

Ethical principles or values of Assessment List for Trustworthy AI (ALTAI)	Relevant section in Clause 5
1 Human agency and oversight	
Human agency and autonomy	5.2 Healthy and safe 5.3.2 Usability 5.4.1 Privacy
Human oversight	5.2.2 Health risks 5.2.4 Health benefit

Table F.2 *(continued)*

Ethical principles or values of Assessment List for Trustworthy AI (ALTAI)	Relevant section in Clause 5
2 Technical robustness and safety	
Resilience to attack	5.2.2 Health risks
	5.4.2 Security
General safety	5.2.2 Health risks
	5.2.5 Societal benefit
	5.3.2 Usability
	5.4.2 Security
	5.5.1 Technical robustness
Accuracy	5.2.2 Health risks
	5.2.4 Health benefit
	5.3.2 Usability
Reliability, fallback plans and reproducibility	5.2.2 Health risks
	5.2.4 Health benefit
	5.5.1 Technical robustness
3 Privacy and data governance	
Privacy	5.4 Secure data
Data governance	5.2.2 Health risks
	5.4 Secure data
4 Transparency	
Traceability	5.2.2 Health risks
	5.2.4 Health benefit
	5.5 Robust build
Explainability	5.2.1 Health requirements
	5.2.4 Health benefit
	5.3 Easy to use
Communication	5.2.2 Health risks
	5.2.4 Health benefit
	5.3.2 Usability
5 Diversity, non-discrimination and fairness	
Avoidance of unfair bias	5.2.1 Health requirements
	5.2.2 Health risks
	5.2.3 Ethics
	5.3.2 Usability
	5.4.2 Security
Accessibility and universal design	5.2.3 Ethics
	5.2.5 Societal benefit
	5.3 Easy to use
Stakeholder participation	5.3.2 Usability
6 Societal and environmental wellbeing	
Environmental well-being	5.2.3 Ethics

Table F.2 *(continued)*

Ethical principles or values of Assessment List for Trustworthy AI (ALTAI)	**Relevant section in Clause 5**
Impact on work and skills	5.2.1 Health requirements
	5.2.2 Health risks
	5.2.3 Ethics
	5.2.5 Societal benefit
	5.3.2 Usability
Impact on society at large or democracy	5.2.3 Ethics
	5.2.5 Societal benefit
7 Accountability	
Auditability	5.2.1 Health requirements
	5.2.3 Ethics
	5.5.1 Technical robustness
Risk management	5.2.2 Health risks
	5.2.3 Ethics
	5.2.4 Health benefit
	5.4.2 Security

Annex G
(informative)

Potential uses of this document

G.1 Health app manufacturer

This document can be used throughout the lifecycle of the health app, including but not limited to the following:

- design: The app manufacturer can determine during the design phase of the project how they intend to be able to answer the assessment questions, and what supporting evidence they will collect. This can be done in collaboration with potential customers and users;
- development: The manufacturer can use the assessment questions as input to the software development plan;
- validation: The manufacturer can use the assessment questions to establish the quality and reliability of the health app. In addition, a health app assessment organization can do an external assessment;
- installation, maintenance and disposal: The assessment questions include processes that the app manufacturer can undertake to ensure the quality and reliability of the health app after it is put on the market;
- business development: Health apps are used in a wider digital health technology and healthcare ecosystem, and a commitment to using this document can be used to build trust and establish business partnerships;
- marketing and sales: Application of this document can be used to show potential customers and users the level of quality and reliability of the health app.

G.2 Health app assessment organizations

App assessment organizations can:

- use this document to assess health apps and issue health app quality labels and health app quality reports for a global market;
- provide advice and consultancy to health app manufacturers to improve the quality and reliability of their health apps;
- provide complimentary assessment services, such as gathering and analysing user reviews.

G.3 Specification development organizations

Specification development organizations can:

- develop profiles of this document for particular use cases. Annex E is an example of such a profile;
- develop additional context-specific assessment questions for aspects of quality and reliability that are not included in this document. For example, there can be assessment questions that cover national or regional interoperability frameworks, or local legislation. Such additional questions will not impact the calculation method for the health app quality score but can be communicated to potential customers and users alongside the label and report specified in this document.

G.4 Potential customers and users

Potential customers and users can:

- communicate their quality and reliability requirements to potential manufacturers of health apps. This can be done by setting minimum health app quality scores, or by requiring that specific assessment questions are answered positively;
- use the health app quality label or health app quality report to determine whether a health app meets their requirements for quality and reliability. The levels of quality and reliability required can vary depending upon the context;
- use the health app quality label and health app quality report in the process of selecting health apps to be included in clinical guidelines, care pathways and care contracts.

G.5 Digital marketplace provider

A digital marketplace provider such as app stores and repositories can require that a health app has a health app quality label issued by a trusted app assessment organization to qualify for their health and wellness section. This would reduce the reputational and other risks associated with including health apps of unknown quality and reliability on the marketplace.

G.6 National and regional authorities

National and regional authorities can require that any health app put on the market within their jurisdiction has a health app quality label issued by a trusted app assessment organization.

G.7 Person or organization recommending health apps

Health app quality labels and reports can be used for or in the process of recommending health apps, avoiding the risk to recommend health apps of unknown quality. For example, individuals, journalists, or organizations representing patients or consumers can make recommendations for a specific health app, or a ‘top ten’ list of health apps.

Bibliography

[1] ISO 639-3, *Codes for the representation of names of languages — Part 3: Alpha-3 code for comprehensive coverage of languages*

[2] ISO 9000:2015, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 9001:2015, *Quality management systems — Requirements*

[4] ISO 9241-11:2018, *Ergonomics of human-system interaction — Part 11: Usability: Definitions and concepts*

[5] ISO 9241-210:2019, *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems*

[6] ISO 13940:2015, *Health informatics — System of concepts to support continuity of care*

[7] ISO 14907-1:2020, *Electronic fee collection — Test procedures for user and fixed equipment — Part 1: Description of test procedures*

[8] ISO 14971:2019, *Medical devices — Application of risk management to medical devices*

[9] ISO/TR 16982:2002, *Ergonomics of human-system interaction — Usability methods supporting human-centred design*

[10] ISO 20282-1:2006, *Ease of operation of everyday products — Part 1: Design requirements for context of use and user characteristics*

[11] ISO/TS 27790:2009, *Health informatics — Document registry framework*

[12] ISO 81001-1:2021, *Health software and health IT systems safety, effectiveness and security — Part 1: Principles, concepts, and terms*

[13] ISO/IEC Guide 51:2014, *Safety aspects — Guidelines for their inclusion in standards*

[14] ISO/IEC Guide 63:2019, *Guide to the development and inclusion of aspects of safety in International Standards for medical devices*

[15] ISO/IEC/TR 20007:2014, *Information technology — Cultural and linguistic interoperability — Definitions and relationship between symbols, icons, animated icons, pictograms, characters and glyphs*

[16] ISO/IEC 21827:2008, *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)*

[17] ISO/IEC 25010:2011, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

[18] ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

[19] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*

[20] ISO/IEC 29100:2011, *Information technology — Security techniques — Privacy framework*

[21] ISO/IEC/TR 29110-1:2016, *Systems and software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 1: Overview*

[22] ISO/IEC 29184, *Information technology — Online privacy notices and consent*

[23] ISO/IEC/IEEE 90003, *Software engineering — Guidelines for the application of ISO 9001:2015 to computer software*

[24] ISO/IEC/IEEE 9945:2009, *Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7*

[25] ISO/IEEE 11073 (all parts), *Health informatics — Device interoperability*

[26] IEC Guide 120:2018, *Security aspects - Guidelines for their inclusion in publications*

[27] IEC 62304:2006, *Medical device software — Software life cycle processes*

[28] IEC 62366-1:2015, *Medical devices — Part 1: Application of usability engineering to medical devices*

[29] IEC 82304-1:2016, *Health software — Part 1: General requirements for product safety*

[30] BS PAS 277:2015, *Health and wellness apps. Quality criteria across the life cycle. Code of practice*

[31] IEEE, IEEE standard computer dictionary: a compilation of IEEE standard computer glossaries. New York: Institute of Electrical and Electronics Engineers; 1990

[32] HL7 *Consumer Mobile Health Application Functional Framework (cMHAFF)*, Release 1

[33] UNI/TR 11708, *Health Informatics - Criteria to identify APPs in the wellness, social and health context*

[34] AICPA *SOC 2® - SOC for Service Organizations: Trust Services Criteria* [viewed 2020-09-07]. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html

[35] ANT+. *What is ANT+* [viewed 2020-09-07]. https://www.thisisant.com/consumer/ant-101/what-is-ant

[36] Australian Signals Directorate, 2020. Australian Government Information Security Manual (ISM), [viewed 2020-09-07]. https://www.cyber.gov.au/acsc/view-all-content/ism

[37] CREST, 2020. Assurance in Information Security [viewed 2020-09-07]. https://www.crest-approved.org/

[38] ENISA, 2019. Smartphone Guidelines Tool [viewed 2020-09-13]. https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smartphone-guidelines-tool

[39] European Commission, European Innovation Partnership on Active and Healthy Ageing, 2020. Blueprint [viewed 2020-09-13]. https://ec.europa.eu/eip/ageing/blueprint_en

[40] European Commission, High Level Expert Group on Artificial Intelligence, 2018. Ethics guidelines for trustworthy AI, [viewed 2020-09-07]. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[41] Farronato C., Iansiti M., Bartosiak M., Denicolai S., Ferretti L., Fontana R. *How to get people to actually use contact-tracing apps*. https://hbr.org/2020/07/how-to-get-people-to-actually-use-contact-tracing-apps

[42] Health Information Trust Alliance (HITRUST) *HITRUST Common Security Framework.* https://hitrustalliance.net/hitrust-csf/

[43] Morrison L, Muller I, Yardley L et al. , The person-based approach to planning, optimising, evaluating and implementing behavioural health interventions. The European Health Psychologist*,* 2018; **20**:464–9.

[44] NHS Digital 2018. *DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems.* https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and

-notifications/standards-and-collections/dcb0129-clinical-risk-management-its-application-in-the-manufacture-of-health-it-systems

[45] National Institute for Health and Care Excellence (NICE) 2019. *Evidence standards framework for digital health technologies.* https://www.nice.org.uk/Media/Default/About/what-we-do/our-programmes/evidence-standards-framework/digital-evidence-standards-framework.pdf

[46] Obar JA, Oeldorf-Hirsch A, The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 2020; **23**(1),128-147.

[47] OWASP *OWASP Mobile Security Testing Guide.* https://owasp.org/www-project-mobile-security-testing-guide/

[48] OWASP *OWASP Secure Coding Practices-Quick Reference Guide*. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/migrated_content

[49] OWASP 2020. *OWASP Top Ten.* https://owasp.org/www-project-top-ten/

[50] Personal Connected Health Alliance *Personal connected health*. https://www.pchalliance.org/

[51] UNICEF *Communicating with children (Guideline 1A)*, https://www.unicef.org/cwc/cwc_58605.html

[52] W3C, 2018. *Web Content Accessibility Guidelines (WCAG) 2.1* https://www.w3.org/TR/2018/REC-WCAG21-20180605/

[53] WHO 1948. *World Health Organization, Preamble to the Constitution of the World Health Organization as adopted by the International Health Conference, New York, 19-22 June, 1946; signed on 22 July 1946 by the representatives of 61 States* (Official Records of the World Health Organization, no. 2, p. 100) and entered into force on 7 April 1948

[54] WHO, 2016. *Monitoring and evaluating digital health interventions: A practical guide to conducting research and assessment.* https://www.who.int/reproductivehealth/publications/mhealth/digital-health-interventions/en/

[55] WHO 2018. *Classification of digital health interventions v1.0 (WHO/RHR/19.06)*. https://www.who.int/reproductivehealth/publications/mhealth/classification-digital-health-interventions/en/

[56] WHO 2020. *Research – Overview.* https://www.who.int/health-topics/research/

[57] Xcertia, 2019. *mHealth App Guidelines.* https://www.himss.org/sites/hde/files/media/file/2020/04/17/xcertia-guidelines-2019-final.pdf

[58] ISO/IEC 27017, *Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*

[59] ISO/IEC 27018, *Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*

[60] ISO 13131, *Health informatics — Telehealth services — Quality planning guidelines*

[61] ISO/IEC 29100:2011/Amd 1:2018, *Information technology — Security techniques — Privacy framework — Amendment 1: Clarifications*

[62] ISO/IEC/IEEE 9945:2009/Cor 1:2013, *Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7 — Technical Corrigendum 1*

[63] ISO/IEC/IEEE 9945:2009/Cor 2:2017, *Information technology — Portable Operating System Interface (POSIX®) Base Specifications, Issue 7 — Technical Corrigendum 2*

[64] IEC 62304:2006/AMD1:2015, *Medical device software — Software life cycle processes — Amendment 1*

[65] IEC 62366-1:2015/AMD1:2020, *Medical device software — Software life cycle processes — Amendment 1*

[66] European Commission 2014. *Health inequalities and eHealth report.* https://digital-strategy.ec.europa.eu/en/library/commission-publishes-four-reports-ehealth-stakeholder-group

[67] Drongelen A. van et al. 2018. *Apps under the medical device legislation*. RIVM. https://www.rivm.nl/publicaties/apps-under-medical-devices-legislation-apps-onder-medische-hulpmiddelen-wetgeving

Anteckningar/Notes

Anteckningar/Notes

Anteckningar/Notes

sis Svenska Institutet för Standarder

Globala lösningar för ett smartare samhälle

SIS är en del av ISO och CEN som är nätverk av experter som arbetar med att skapa internationella standarder. Hos oss kan aktörer ta initiativ och samverka för best practice som främjar Sveriges konkurrenskraft och ger smart och hållbar samhällsutveckling. SIS samverkar med alla delar av det svenska samhället, som till exempel industri, akademi, offentlig sektor och frivilligorganisationer.

SIS projektleder det svenska arbetet med att ta fram standarder. Vi verkar för ökat svenskt inflytande i internationella samarbeten och för att best practice sprids och tillämpas i Sverige. Vi erbjuder också utbildningar, tjänster och produkter som hjälper våra kunder att utveckla sina verksamheter och skapa samhällsnytta med hjälp av standarder.

Vill du veta mer eller bidra till att skapa smarta globala lösningar, kontakta oss per telefon eller besök **sis.se**

Svenska institutet för standarder
104 31 Stockholm
Tel 08 - 555 523 10
kundservice@sis.se
sis.se

Tryckt på miljövänligt papper