ISO/TS 82304-2:2021 (E)

Health software — Part 2: Health and wellness apps—Quality and reliability

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

3.1 General terms
3.2 Terms relating to apps
3.3 Terms relating to risk management

4 Health app assessment process

4.1 Quality assessment
4.2 Quality requirements
4.3 Health app quality report
4.4 Health app quality evidence pack
4.5 Health app quality label

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?
5.1.1.2 What is the name of the health app?
5.1.1.3 Provide the health app icon, if available.
5.1.1.4 In which languages is the health app available?
5.1.1.5 Provide health app access instructions for the app assessment organization.
5.1.2 App manufacturer
5.1.2.1 What is the name of the health 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.
5.2 Healthy and safe
5.2.1 Health requirements
5.2.1.1 Who are the intended users of the health app?
5.2.1.2 Are age restrictions of the intended users or subjects of care made clear to potential customers and users?
5.2.1.3 For which health issue(s) and/or health need(s) is the health app intended?
5.2.1.4 What is the intended use of the health app?
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?
5.2.1.6 Are health professionals involved in the development of the health app?
5.2.1.7 Is appropriate peer reviewed scientific literature used in the development of the health app?
5.2.2 Health risks
5.2.2.1 Are the health risks of the health app analysed?
5.2.2.2 Are measures in place to control the health risks of the health app?
5.2.2.3 Are the residual risks of using the health app found to be acceptable?
5.2.2.4 Describe when the health app requires approval from a health professional before use.
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?
5.2.2.6 Is a process to collect and review safety concerns and incidents for the health app maintained?
5.2.3 Ethics

5.2.3.1 Are ethical challenges of the health app assessed with intended users and health professionals?
5.2.3.2 Is the health app approved by an independent ethics advisor or ethics advisory board?
5.2.4 Health benefit
5.2.4.1 Describe the health benefit of using the app.
5.2.4.2 Are potential customers and users made aware of the health interventions applied to achieve the health benefit?
5.2.4.3 Are potential customers and users made aware of all financial costs to achieve the health benefit?
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?
5.2.4.5 Is evidence available to support the health benefit of using the app?
5.2.4.5.1 Does this evidence include peer reviewed research involving the use of this health app?

5.2.4.5.2 Is the level of the evidence appropriate?
5.2.4.6 Is there a maintenance process for the health information in the app?
5.2.4.6.1 Are all sources for the health information in the health app disclosed to potential customers and users?
5.2.4.7 Are all sources of funding of the health app disclosed to potential customers and users?
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?
5.2.5 Societal benefit
5.2.5.1 Is evidence available of a societal benefit of using the app?
5.2.5.1.1 Does this evidence include peer reviewed research involving the use of this health app?

5.3 Easy to use
5.3.1 Accessibility
5.3.1.1 Is the health app WCAG 2.1 AA or AAA compliant?
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?
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?
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?
5.3.1.2 Is the health app age-appropriate?
5.3.2 Usability
5.3.2.1 Is the health app design based on an explicit understanding of users, tasks and environment?
5.3.2.2 Are intended users involved throughout design and development of the health app?
5.3.2.3 Is the design of the health app driven and refined by user-centred evaluation?
5.3.2.4 Are measures in place to avoid use error and reasonably foreseeable misuse of the health app?
5.3.2.5 Are potential customers and users provided with adequate product information about the health app?
5.3.2.6 Are instructions for use readily available for users?
5.3.2.7 Are appropriate resources available to adequately help users who experience problems with the health app?
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?
5.4 Secure data
5.4.1 Privacy
5.4.1.1 Does the health app process Personally Identifiable Information (PII)?
5.4.1.1.1 Does the health app process health related PII?
5.4.1.1.2 Is data minimization applied in the health app?
5.4.1.1.3 Is an appropriate retention policy established to erase or review the data stored?
5.4.1.1.4 Is a privacy statement readily available to potential customers and users of the health app?
5.4.1.1.4.1 Does the privacy statement start with an accessible overview of less than 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?
5.4.1.1.6 Is opt-in the default setting for sharing PII 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?
5.4.1.1.8 Are security-incident response procedures in place-that include reporting PII breaches to the user and relevant authorities?
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?
5.4.2.2 Is an information security risk assessment for the health app available?
5.4.2.3 Is a secure by design process followed?
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?
5.4.2.5 Is a process to prevent unauthorized access and modifications to the health app source code in place?
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?
5.4.2.7 Is user authentication, authorization and session management implemented to secure access to the health app?
5.4.2.8 Does the health app transmit and store all PII with adequate encryption?
5.4.2.9 Are security vulnerabilities reported, identified, assessed, logged, responded to, disclosed, and quickly and effectively resolved?
5.4.2.10 Are the security of the health app and associated services tested on a regular basis and at major changes?
5.4.2.11 Is the information security policy readily available to potential customers and users?
5.5 Robust build
5.5.1 Technical robustness
5.5.1.1 Are all the health app product requirements documented?
5.5.1.2 Is the health app developed with a software development process that covers the standards, methods and tools to be used?
5.5.1.3 Is a secure coding standard followed?
5.5.1.4 Is a configuration management plan established for the health app?
5.5.1.5 Are processes in place to deal with a significant increase or spike in demand?
5.5.1.6 Is a validation and verification plan used for the health app?
5.5.1.7 Is a release and deployment process established?
5.5.1.8 Is a maintenance process established?
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?
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?
5.5.2.3 Does the health app validate all data for the health app transferred via APIs?
5.5.2.4 Can users obtain their health related PII by a data export to another platform?

Annex A (normative) Health app quality label

A.1 General
A.2 Content
A.3 Dimensions
A.4 Text
A.5 Languages
A.6 Colour scheme

Annex B (normative) Health app quality score calculation method

Annex C (informative) Rationale

Annex D (informative) Product safety and lifecycle process recommendations

D.1 General
D.2 Product Safety Requirements from IEC 82304-1
D.2.1 General requirements and initial risk assessment
D.2.2 Health software product use requirements
D.2.3 System requirements

D.2.4 Health software product use requirements and health software product system requirements
D.2.5 Software life cycle processes
D.2.6 Product validation
D.2.7 Product identification and accompanying documents
D.3 Product life cycle requirements from IEC 62304+AMD1:2015
D.3.1 Software development standards, methods and tools planning
D.3.2 Documentation planning
D.3.3 Software configuration management planning
D.3.4 Software unit implementation
D.3.5 Software release
D.3.6 Analyse change requests
D.3.7 Change control
D.4 Product characteristics

Annex E (informative) Application profile – Contact tracing apps

E.1 General
E.1.1 Background
E.1.2 Typical operation of a contact tracing app
E.2 Guidance for contact tracing apps

Annex F (informative) Ethical considerations in health apps

Annex G (informative) Potential uses of this document

G.1 Health app manufacturer
G.2 Health app assessment organizations
G.3 Specification development organizations
G.4 Potential customers and users
G.5 Digital marketplace provider
G.6 National and regional authorities
G.7 Person or organization recommending health apps

Page count: 78