FINCCHTA | Digi HTA

FACULTY OF TECHNOLOGY UNIVERSITY OF OULU

FACULTY OF MEDICINE UNIVERSITY OF OULU

Funded by the European Union – NextGenerationEU

Comparison report of Digi-HTA and CEN/ISO TS 82304-2:2021

JARNO SUOMINEN[1]

PAULA VEIKKOLAINEN[2]

MERJA VOUTILAINEN[1]

JARI HAVERINEN[1, 2]

RAULI KAKSONEN[3]

[1]Finnish Coordinating Center for Health Technology Assessment (FinCCHTA), Oulu University Hospital, Oulu, Finland
[2]FinnTelemedicum, Research Unit of Health Sciences and Technology, Faculty of Medicine, University of Oulu, Oulu, Finland
[3]Biomimetics and Intelligent System Group, Faculty of Technology, University of Oulu, Oulu, Finland

23.01.2023

Finnish Coordinating Center for
Health Technology Assessment, FinCCHTA

Funded by the European Union – NextGenerationEU

Version	Date and name of the version updater	Description of the update
1.0	30.09.2022 Jarno Suominen, Paula Veikkolainen, Rauli Kaksonen, Merja Voutilainen, Jari Haverinen	Baseline version
1.1	23.01.2023 Jarno Suominen, Paula Veikkolainen, Rauli Kaksonen, Merja Voutilainen, Jari Haverinen, Petra Hoogendoorn	The stakeholders addressed in this report have been consulted regarding their view on the conclusions of this report.

FinCCHTA
CC BY-NC-ND 4.0
2023

Finnish Coordinating Center for
Health Technology Assessment FinCCHTA
P.O. Box 10 , Fi-90029 OYS, Finland
fincchta.fi

Table of Contents

1.Background

Digi-HTA is a health technology assessment (HTA) method developed for digital products and services for social, health care and well-being services [1-3]. It is used to assess the suitability of a product or service for the use of customers, professionals and organizations in the sector. CEN/ISO TS 82304-2:2021 is an assessment framework that provides requirements for the specification for a health app quality label [4]. The purpose of this document is to summarize the results of the comparative analysis of the two assessment methods. The goal is to produce transparent and reliable reference material that compares CEN/ISO TS 82304-2:2021 and the Digi-HTA assessment framework.

Comparison workflow was driven by the on-going rise of digital health technologies and the increasing demand for high quality and comprehensive assessment of mHealth, artificial intelligence and robotics solutions. On regulatory basis, the safety, performance, risks and benefits of medical devices are strongly regulated before market access. Strong regulation-based approach can create the impression that market penetrated solutions are uniformly applicable. However, market access in itself does not guarantee the effectiveness or applicability of the device [5, 6]. The same applies to wellness technology, in which regulation is clearly at a lower level compared to medical devices. In addition to assess and qualify digital solutions the need for harmonization of assessment criteria is essential so the open market is not siloed between countries. It is a shared interest of manufactures, users and assessment bodies that digital solutions and mobile apps in the social, health and welfare sectors are evaluated with uniform criteria to support decision making while taking into account the needs of technology companies and citizens. The assessment criteria should not silent innovations or research but support them to ensure quality on high standard. From this point of view modularized and unified assessment methods support quality apps without additional market restriction.

The analysis is divided into two parts: the first part focuses on the general parts of the frameworks, and the second part on the information security and protection requirements. A comparison by category is presented in the following sections. The middle column "Both" summarizes the requirements shared by both documents. The requirements unique for each document are summarized in the left- and right-hand columns. CEN/ISO TS 82304-2:2021 includes four questions that are required. The stakeholders addressed in this report have been consulted regarding their view on the conclusions of this report. Comparison work was done in 08/2022-12/2022 and it is part of Finnish Recovery and Resilience Plan which is funded by the European Union -NextGenerationEU funding.

2. Comparison of the general parts of the assessment methods

In modular way of thinking, comparison cleared the pathway of avoiding overlapping evaluation burden. As a key observation, it is recognized that the criteria between these two evaluation methods support each other. The categorized differences between the two assessments entities focus on the areas of cost effectiveness, interoperability and visualization of the assessment results. In addition CEN/ISO TS 82304-2:2021 features ethics as its own assessment area. Digi-HTA features robotics and artificial intelligence as their own assessment areas. These individual assessment areas are not found in both assessment frameworks and thus are not included in this analysis. It should be clarified that there are multiple similar assessment criteria in between. However, similar criteria can be written in many ways from different perspectives.

Summary of the differences in the general parts of the frameworks:

1. Digi-HTA brings up the organization’s and end-user’s perspective on its assessment framework from the viewpoint of HTA (Health Technology Assessment) while CEN CEN/ISO TS 82304-2:2021 emphasizes the end-user point of view.

2. CEN/ISO TS 82304-2:2021 focuses on mobile applications, whereas Digi-HTA focuses on covering also wide range of digital health technologies including hardware devices with embedded software integrations.

3. In both Digi-HTA and CEN/ISO TS 82304-2:2021, the assessment process is based on materials provided by the vendor providing the product or service. However, Digi-HTA supports the assessment with its own additional literature review process.

4. The main differences between the two assessments entities focus on the areas of cost-utility, interoperability and visualization of the assessment results

Product

Digi-HTA [1]	Both	CEN ISO/TS 82304-2:2021 [4]
Technology readiness level (TRL) of the product. When will the finished product be available and what is the FDA classification of the product?	A description of the product, general information on the product and for which platforms the product is available	Are potential customers and users provided with adequate product information about the health app?
Questions related to electrical devices	Information about the product's CE approval, and whether the product is a medical device (MDD/MDR)	
Is the product already in use elsewhere in Finland or worldwide and if so, where and for how long has it been?	The intended use of the product, information about maintenance processes and product support for end-users. Information about the instructions and where to find them	

Effectiveness

Digi-HTA	Both	CEN ISO/TS 82304-2:2021
Explanation of any missing evidence of clinical benefits or system/organizational effects	Description of the product's health benefits and the evidence + the evidence of its effectiveness	Whether all sources for the health information in the health app disclosed to potential customers and users
Whether there are any ongoing studies to investigate the product's effectiveness in Finland or in other countries	Description of the product's effects on users' actions and the evidence available	Whether there a maintenance process for the health information in the app
Whether there any ongoing studies to investigate the product's effectiveness in Finland or in other countries	Is the level of the evidence appropriate	
Level of evidence for system effectiveness requires peer reviewed publications	Is evidence available of a societal benefit of using the app	
Institutions that recommend the product attached with the recommendations		

Funded by the European Union –
NextGenerationEU

Safety

Digi-HTA	Both	CEN ISO/TS 82304-2:2021
Whether the provision of erroneous guidance can be ruled out or rendered unlikely	Are potential customers and users of the health app made aware of the health risks, contra-indications and limitations of use? Have the health risks of the app been analysed and what the risks are?	Are measures in place to control the health risks of the health app and are the residual risks of using the app found to be reasonable?
Whether any product-related customer safety events been reported and who is the responsible person in the company for handling Manufacturer Incident Reports	Is there any research evidence available related to safety, including links to public results or attached reports, and are there any undesirable effects associated with misuse of the product?	Describe whether the health app requires approval from a health professional before use
National references for safety supervision	Has the product undergone a risk analysis and what is the company's process to handle customer safety events? Are there any risks associated with using the product? Assessment risks, possible side effects, or other undesirable effects associated with using or misusing the product. Process to handle safety incidents and concerns.	Gives value to informing customers about the safety and risks Are health professionals involved in the development of the health app? Is the health app approved by an independent ethics advisor or ethics advisory board?

Costs

Digi-HTA	Both	CEN ISO/TS 82304-2:2021
Accurate information on the formation of costs and the amount of costs for both the organization and the end-users, the maintenance cost for the organization and the uncertainty factors associated with the costs	Costs for the end-users	Are potential customers and users made aware of all financial costs to achieve the health benefit and are all the sources of funding and the use of advertising mechanism disclosed to the customers and users?

Technical Stability

Digi-HTA	Both	CEN ISO/TS 82304-2:2021
Do software/system updates cause downtime in the use of the product and how are they handled?	Is the health app developed with a software development process that covers the standards?	Is a validation and verification plan used for the health app?
IEC 62304 - no reference to year of issuance or amendments	Is a configuration management plan established for the health app?	IEC 62304-1:2016
	Description of the company's testing process and how the company is handling error messages	Is a maintenance process established and are measures in place to avoid use error and reasonably foreseeable misuse of the health app, and is a secure coding standard followed?
	How do you implement software/system updates for your product?	Are potential customers and users provided with adequate product information. and are processes in place to deal with a significant increase or spike in demand?
	Does the company have the capacity to roll back to previous versions of the product and do they have a process to proactively monitor the running of systems and system components to automatically identify faults and technical issues?	
	How the company informs the end-user or organization using the product about the updates and whether software/system updates cause downtime in the use of the product	

Interoperability

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
What specific user interfaces are used to access Electronic Patient Records (EPR), website or other software, and in which format can the data contained in the product be exported?	Can the data contained in the product be exported in a commonly used or standard format?	Are potential customers and users of the health app able to access the specifications and implementation guides for the terminology or terminologies used?
Are proprietary formats used to store and transfer data?	Mention of possible connection with other health or wellness devices	Can users obtain their health related Personally Identifiable Information (PII) by a data export to another platform and does the health app validate all data for the health app transferred via Application Programming Interfaces (API)?

Usability and accessibility

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Is an accessibility statement available for the product? [7, 8]	Suitability of the product for different user groups and possible restrictions for different user groups	Is the design of the health app driven and refined by user-centred assessment, is the app age-appropriate, and is there a usability assessment plan including controls?
Electronic feedback channel for users to submit accessibility feedback with reply available in 14 days.	Requirements of Web Content Accessibility Guidelines (WCAG) 2.1 level AA compliancy	
	How the product has been tested on real user groups and has the functionality of the product been tested with screen readers or other assistive technologies	Are any ethical issues with the health app assessed with the intended users and health professionals?
	How is the accessibility developed and evaluated and what accessibility features does the product support?	Are measures in place to avoid user error and reasonably foreseeable misuse of the health app?
	Is it possible to have a demo version of the product for testing during the deployment process, and does the product follow the design guidelines for the platform?	
	Has the product undergone an accessibility assessment and if so, who carried it out, and is the product a native iOS or Android app?	
	What changes have been made to the product based on user feedback	

3. Comparison of information security and data protection

The goal of this part is to compare the technical content of two cyber security requirement documents:

- CEN ISO/TS 82304-2:2021 Health software - Part 2: Health and wellness apps - Quality and reliability, August 2021 [4]
- Digi-HTA version of the HTA TT Information Security and Data Protection Requirements.XLSX (Information security and data protection requirements for social welfare and healthcare procurements) v1.3 (last version history entry is v.1.0.8, 17/12/2021) The latter document is not identical to the one provided at the Traficom website (v. 1.0.2) [9]. There is a separate comparison document.

The comparison is based on product requirement categories presented in the article "Common cybersecurity requirements in IoT standards, best practices, and guidelines" [10]. Summary of the differences:

1. CEN/ISO TS 82304-2:2021 is focused on mobile applications while Digi-HTA covers the whole IT system. The former has very few requirements beyond applications. If requirements for the system are desired, Digi-HTA provides much broader coverage.
2. CEN/ISO TS 82304-2:2021 has many requirements for usability which are to some extent related to security. Digi-HTA requirements have no specific usability focus.
3. The other differences are not major. However, as with comparing any other security standards, the details vary and implementing one does not mean that the other is covered.

Product requirements

Security design

Digi-HTA [1]	Both	CEN/ISO TS 82304-2:2021 [4]
Detailed requirements for architecture documentation including network security architecture, data flows, data classes, user and administrator roles, security information and event management (SIEM) integration, etc.	Must be secure by design	One generic question: "Is a secure-by-design process followed?"

Secure programming

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	-	Requirement to have a secure programming standard. Use of proper compilers and other tools

Delivery & deployment

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Vendor must provide system hardening guidelines, including firewall, and tools to check proper system deployment. The system must not use default passwords.	Must specify the conditions for secure use	Vendor provides a list of security-related warnings and notices

Administration

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Requirements for secure administration, integration with external security systems, and other similar requirements.	-	-

Interface security

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Firewall requirements. Removal of unused services, ports, accounts, debug interfaces, and software. Limit on external connections, wireless security. Must tolerate security scanning.	-	Validate received data

Authentication

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Ability to integrate with identity federation, password setting configuration, limit shared accounts, smart cards. Two-way authentication of components	Strong user authentication, e.g. multi-factor or biometric. Encrypted passwords and automated logout. Authentication of external connections.	User authentication before proceeding with support requests involving handling of Personally Identifiable Information (PII).

Access control

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
SIS (Safety Integrated System) access control, user groups and roles	Access control of users	-

Security hardware

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
SIS security	-	-

Backend security

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Separation of users in multi-tenant cloud systems. (Many other requirements handled under other topics)	-	-

Cryptography

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Centralised digital key management, X.509 certificates	Use of strong and contemporary encryption, updated as required. Password encryption	-

Data protection

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
PII must be stored in EU and the storage location documented. PII shall not be used in development	Protect PII and comply with regulations. Provide the user control over their own PII. Multi-vendor/data processor responsibilities documented. Protect data in transit and at rest. Use data export standards. Decommissioning	Data retention policy. Stored PII must be minimized and/or anonymized. Age-appropriate user data handling.

Service availability

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Key management and response or reporting of events must not interfere with normal operation	-	Ensure functionality in case of increased demand. Document measures to ensure availability

Failure security

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	-	Coding standard must cover error handling

Audit logging

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Centralised log database and list of items to log. Integration with SIEM. Logs can be provided to customer upon request	Logging to enable regulatory handling and forensics of data breaches	-

Intrusion detection

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Document how security is monitored and managed. Alerts, malware protection, application whitelisting	-	-

Incident response

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Detailed requirements for backup and restore scheme, technology and tools	Back-up and restore personal data	-

System updates

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
The vendor shall provide tools for secure updating. Updates as agreed with customer. Must update all parts of the system	Inform users of availability of new versions	Work with OS update systems. Incremental delivery and rollback to previous version.

Usability of security

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	Automatically lock-out/hide PII after inactivity. Provide user documentation	User-centric usability, accessibility requirements. Support service for users

Life-cycle requirements

Vendor security

Digi-HTA [1]	Both	CEN/ISO TS 82304-2:2021 [4]
Data in bankruptcy situations, obligation to notify customer of personnel, subcontractor or consultant changes. Use access control lists	Vendor organization must implement security measures, personnel are informed and trained on security	Implement ISO/IEC 27001 or equivalent. Participation of top-level management, responsible person for PII and legal compliance

Policies & laws

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Vendor must direct authority data requests to the customer.	GDPR and other privacy laws must be followed.	-

Development process

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
Customer documentation security, must review plans with customer	Secure development processes, change management, handling of 3rd party components, security testing including penetration testing	Protect source code, data validation testing, usability testing

Security requirements

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	Perform risk analysis	-

Security standards

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	Use security standards	-

Vulnerability management

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	Monitor vulnerabilities and report them appropriately. Support mitigation of vulnerabilities	-

User communication

Digi-HTA	Both	CEN/ISO TS 82304-2:2021
-	Provide user timely information about security risks, vulnerabilities, updates, etc.	-

References

[1] Haverinen, J., Keränen, N., Falkenbach, P., Maijala, A., Kolehmainen, T., & Reponen, J. (2019). Digi-HTA: Health technology assessment framework for digital healthcare services. Finnish Journal of EHealth and EWelfare, 11(4), 326–341. https://doi.org/10.23996/fjhw.82538

[2] Jääskelä, J., Haverinen, J., Kaksonen, R., Reponen, J., Halunen, K., Tokola, T., & Röning, J. (2022). Digi-HTA, assessment framework for digital healthcare services: information security and data protection in health technology – initial experiences. Finnish Journal of EHealth and EWelfare, 14(1), 19–30. https://doi.org/10.23996/fjhw.111776

[3] Haverinen, J., Turpeinen, M., Falkenbach, P., & Reponen, J. (2022). Implementation of a new Digi-HTA process for digital health technologies in Finland. International Journal of Technology Assessment in Health Care, 38(1), E68. https://doi.org/10.1017/S0266462322000502

[4] International Organization for Standardization. (2021). Health software -part 2: health and wellness apps—quality and reliability (ISO/TS 82304-2). [cited 30 September 2022]. Available https://www.iso.org/standard/78182.html

[5] European Parliament. (2021). Regulation (EU) 2021/2282 of the European Parliament and of the Council of 15 December 2021 on health technology assessment and amending Directive 2011/24/EU. [cited 30 September 2022]. Available https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32021R2282

[6] Annunen K.; Lukkarila A. (2023). Added Value that Digi-HTA Assessment Brings to Digital Health Technology Products Compared to the Requirements of the Medical Device Regulation. [cited 11 January 2023]. Available https://urn.fi/URN:NBN:fi:amk-2022123131709

[7] European Parliament. (2016). Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies. [cited 30 September 2022]. Available https://eur-lex.europa.eu/legal-content/GA/ALL/?uri=CELEX:32016L2102

[8] Act on the Provision of Digital Services 306/2019. (2019). [cited 30 September 2022]. Available https://www.finlex.fi/en/laki/kaannokset/2019/en20190306

[9] National Cyber Security Centre Finland, NCSC-FI. (2019). Information security and data protection requirements for social welfare and healthcare procurements, version 1.0.6-20191202. [cited 30 September 2022]. Available https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/information-security-and-data-protection-requirements-social

[10] Kaksonen, R., Halunen, K. & Röning, J. (2022). Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines. In Proceedings of the 7th International Conference on Internet of Things, Big Data and Security - IoTBDS 2022; ISBN 978-989-758-564-7: 149-156. https://doi.org/10.5220/0011041700003194