Funded by the European Union – NextGenerationEU

Comparison report of Digi-HTA and NordDEC

JARNO SUOMINEN[1]

PAULA VEIKKOLAINEN[2]

RAULI KAKSONEN[3]

JARI HAVERINEN[1, 2]

[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

Funded by the European Union – NextGenerationEU

Table of Contents

Funded by the European Union – NextGenerationEU

Version	Date and name of the version updater	Description of the update
1.0.	13.1.2023 Jarno Suominen, Paula Veikkolainen	Baseline version
1.1	28.2.2023 Jarno Suominen, Paula Veikkolainen, Rauli Kaksonen, Jari Haverinen, Paul Weston, Fiona Costello, Ben Philips	The stakeholders addressed in this report have been consulted regarding their view on the conclusions of this report.

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. NordDEC is an evaluation framework that combines parts of the assessment criteria of different evaluation models, providing requirements for the specification of mobile and desktop applications within healthcare [4]. The purpose of this document is to summarize the results of the comparative analysis of the two evaluation methods. The goal is to produce transparent and reliable reference material that compares the NordDEC technical specification and the Digi-HTA evaluation framework.

The 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. With regard to the regulatory basis, the safety, performance, risks and benefits of medical devices are strongly regulated before market access. This strong regulation-based approach can serve to create the impression that market penetrated solutions are uniformly applicable. However, market access in itself does not guarantee the effectiveness or applicability of a device [5, 6]. The same applies to wellness technology, in which regulation is clearly at a lower level compared to medical devices. Furthermore, to assess and qualify digital solutions, the harmonization of assessment criteria is essential, so the open market does not become siloed between countries. It is in the shared interest of manufactures, users, and assessment bodies that digital solutions and mobile apps in the social, health, and welfare sectors are evaluated using uniform criteria to support decision-making, while taking into account the needs of technology companies and citizens. The assessment criteria should not silence innovations or research, but support them to ensure a high standard of quality. From this point of view, modularized and unified assessment methods support high-quality apps without creating additional market restrictions.

The analysis is divided into two parts: the first part focuses on the general parts of the frameworks and the second part on the cybersecurity and data protection requirements. A comparison by category is presented in the following sections. The middle column "Both" summarizes the requirements shared by both documents. The stakeholders addressed in this report have been consulted regarding their view on the conclusions of this report. This comparison work was conducted in 09/2022-01/2023 and 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 evaluation methods

The modular way of thinking embodied in the comparison helps clear a pathway to avoiding overlapping evaluation burden. As a key finding, it is recognized that the criteria offer different application areas and points of view. Digi-HTA looks at digital solutions from a high-level perspective with strictly limited attention to detail, whereas NordDEC divides the entities into smaller pieces, building the end result on specific details. The level of the Digi-HTA evaluation aims at national level advisory activities, whereas NordDEC intends to cover the commercialisation of the product across the Nordic countries.

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

1. NordDEC focuses on mobile and web applications whereas Digi-HTA also includes hardware devices and software synergies in its scope.

2. In both Digi-HTA and NordDEC, the evaluation process is based on materials provided by the vendor providing the product or service. Nevertheless, NordDEC conducts background research based on the documents that are openly available beforehand. On the other hand, Digi-HTA supports the evaluation with its own additional literature review process.

3. The main differences between the two assessments entities focus on the areas of Privacy, Security, Effectiveness, Ethics, Usability, Accessibility, Costs, Interoperability, Technical Stability and final visualization of the assessment results. In addition Digi-HTA also includes robotics and artificial intelligence in its assessment areas. These individual assessment areas are not found in both assessment frameworks and thus are not included in this analysis. It is also valuable to understand that NordDEC combines various parts of the assessment criteria of different evaluation models rather than creating new assessment criteria.

4. As a method, NordDEC supports the assessment process through modularity, as it is built on web-based user interface which helps create half-automated assessment reports. The assessment criteria of Digi-HTA are at the moment built on Excel and the reports are compiled manually. Both approaches provide a detailed assessment report.

Product

Digi-HTA[1]	Both	NordDEC[4]
Evaluates Technology Readiness Level (TRL) of the product. Includes whether the product meets the electrical safety requirements for medical devices (EN 60601-1) Includes whether the use of the product requires strong electronic identification. Assesses what sort of support or training is necessary the end user. Distinguishes whether the medical device follows the Medical Device Directive or Medical Device Regulation.	What the intended purpose of the product is and what problem / intervention it is used for. Product manuals must be provided as separate document. Distinguishes between wellness apps and medical devices. If the product is a medical device the Declaration of Conformity document has to be provided. Takes into account Medical Device Regulation and FDA approval. If the product is not classified as a medical device, it must be justified why not. Takes into account what kind of support is available for the user/patient. Capability to assess products at different stages of readiness.	Multiple questions seeking evidence of an appropriate professional being involved in the product's design and development. E.g. "Is a suitably qualified professional involved in the development team of the App?" Specific questions regarding provided support and forum. (e.g. moderated forum, time to response) Which Evidence Standard Framework (ESF) does the product belong to and whether the evidence is appropriate. Several questions related as to whether and how the developer has considered the nature of the *Health IT System* (e.g. system architecture, messaging, data migration, business process impact, intended use and clinical scope).

Effectiveness

Digi-HTA	Both	NordDEC
Highlights clinical benefits. Emphasises other measurable indicators such as cost-effectiveness and efficiency gains for healthcare organisation besides the medical and functional evidence. Also assesses cases when there is no evidence available and the reasons behind such situations. Also investigates if there are any ongoing studies.	Both emphasize the type and number of evidence of the benefit. Includes evidence on behavioural/ lifestyle changes as their own question/question category. Takes into account recommendations/endorsement(s) from relevant bodies/institutions. Apps with more complex functionality and higher risk require more evidence.	Includes specific questions intended to evaluate the quality of the related studies (sample size, p-value, comparator). Specific questions assessing the number of available evidence. Based on NICE Digital Health Technologies Framework (Tiers).

Safety

Digi-HTA	Both	NordDEC
Is the manufacturer aware of the product register and Manufacturer Incident Report supervised by Finnish national officer Fimea?	Evaluates risks, possible side effects, or other undesirable effects associated with using or misusing the product.	Is the App/Solution in scope for a clinical safety assessment?
	Gives value to research evidence available related to safety. Requires naming a responsible person (CSO) for handling Manufacturer Incident Reports.	Evaluates the competence of the responsible person (CSO) and if the person played an active part in the clinical safety process. Gives value to publishing the risk management process.
	Requires a risk analysis and a deployment of the analysis.	
	Requires a documentation of process for patient / customer safety events.	

Costs

Digi-HTA	Both	NordDEC
What kind of lifecycle costs does the product incur on the acquiring organisation?	Costs for end users.	-
Requires evidence of cost-effectiveness.	Source of income of the application presented related to the app.	

Technical Stability

Digi-HTA	Both	NordDEC
Reference to the IEC 62304 life cycle process standard. History of down time / impairment time during last 6 months and how are downtime situations to be handled. How are end-users informed about product updates?	Cover (with nearly identical questions): - Change audits - Testing process - Rollback capacity - Proactive monitoring of faults - Decommissioning of product	Requires evaluation of whether the provided evidence regarding product testing is sufficient, assesses used testing standards, details and tools. Includes multiple questions assessing people / roles that are involved in the testing process.
	Both acknowledge error (DigiHTA) / fault (NordDEC) situations and their handling.	Documented roadmap of future product development.
	Both acknowledge potential updates (DigiHTA) / future development roadmap (NordDEC) of the product	

Usability and accessibility

Digi-HTA	Both	NordDEC
Electronic feedback channel for users to submit accessibility feedback with reply available in 14 days.	Is an accessibility statement available for the product? [7, 8] *(In NordDEC only for web apps)*	Gives value to detailed parts of usability such as notifications, change of presentation themes and different functional buttons, e.g. search button, home button.
Emphasis on Finnish national restrictions: Act on the Provision of Digital Services?	Is there a statement within the app outlining compliance with any current recognized app design standards? E.g. Has the product been evaluated against WCAG 2.1 AA, AAA? Value the evidence of user involvement in testing the product. What accessibility features does your product support? Does the app take into consideration people with disabilities such as hearing or seeing difficulties? How have the product's users been taken into consideration in the product's text (clear, concrete language; the avoidance of professional jargon)? How is the user supported in using the product? Is the product a native or a web-based app? Has the functionality of the product been tested with screen readers or other assistive technologies?	Has the app been designed to work on mobile devices and tablets? Does the app inform the user how to manage notification settings for convenience/privacy?

Interoperability

Digi-HTA	Both	NordDEC
Can the data contained in the product be exported in a commonly used or standard format?	Does the product use interfaces to access the website or other software?	Is there a way for the user to confirm that the data input is accurate?
Emphasis on Finnish national interoperabilities such as Kanta PHR.	Does the product connect with any health or wellness devices?	Emphasis on NHS interoperabilities.
Can the data contained in the product be exported in a commonly used or standard format?		
Are proprietary formats used to store and transfer data?		
Are the definitions of the original proprietary formats openly available?		
Does the product use interfaces to access other companies' services?		
If yes, list those interfaces. Does the product use data from other systems via interfaces?		
If yes, can the data produced by others be separated in the system?		

3. Comparison of information security and data protection

This part compares the technical content of two cyber security requirements documents:

1. Nordic Digital Health Evaluation Criteria - NordDEC (hereinafter NordDEC), Adam McCabe, Last updated 15 June 2022, 12:33[4]

2. Digi-HTA version of the HTA TT Information Security and Data Protection Requirements.XLSX (Soten hankintojen tietoturva- ja tietosuojavaatimukset) 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:

3. NordDEC has many requirements/questions about clinical evidence of medical efficacy, which is relevant for the Digi-HTA overall assessment, but not considered in this report about information security.

4. NordDEC focuses heavily on private data security, which is expected to be documented in detail in the *Data Protection Impact Assessment* (DPIA). There are many detailed and overlapping questions concerning the DPIA.

5. NordDEC does not, in a real sense, include an assessment of the security of the product deployment, administration, hardening, interface security, used cryptography, security updates, etc. These seem to be out of the scope of NordDEC.

A comparison by category is presented in the following sections. The middle column "Both" summarises the requirements shared by the documents. The requirements unique for each document are summarized in the left- and right-hand columns.

1. Product requirements

Security design

Digi-HTA[1]	Both	NordDEC[4]
Detailed requirements for architecture documentation including network security architecture, data flows, data classes, user and administrator roles, SEED integration, etc.	Architecture design required. Minimal application permissions.	-

Secure programming

Digi-HTA	Both	NordDEC
-	-	External review using the OWASP Mobile Application Security Verification Standard

Delivery & deployment

Digi-HTA	Both	NordDEC
Vendor must provide system hardening guidelines, including firewall, and tools to check proper system deployment. The system must not use default passwords.	-	-

Administration

Digi-HTA	Both	NordDEC
Requirements for secure administration, integration with external security systems, and other similar requirements.	-	-

Interface security

Digi-HTA	Both	NordDEC
Firewall requirements. Removal of unused services, ports, accounts, debug interfaces, and software. Limit on external connections, wireless security. Must tolerate security scanning.	-	-

Authentication

Digi-HTA	Both	NordDEC
Ability to integrate with identity federation, password setting configuration, limit shared accounts, smart cards, encrypted passwords. Two-way authentication of components.	User must be authenticated; additional auth. security is good.	-

Access control

Digi-HTA	Both	NordDEC
User access control, user groups and roles. Safety Integrated system (SIS) access control.	-	Preferences for sharing data with others

Security hardware

Digi-HTA	Both	NordDEC
SIS security.	-	-

Backend security

Digi-HTA	Both	NordDEC
Separation of users in multi-tenant cloud systems.	-	Does app connect to external Internet APIs (e.g. for advertising). Web security requirements.

Cryptography

Digi-HTA	Both	NordDEC
Use of strong and contemporary encryption, updated as required. Password encryption. Centralised digital key management, X.509 certificates.	Data must be encrypted in transit.	-

Data protection

Digi-HTA	Both	NordDEC
-	Comprehensive requirements / questions about personally identifiable information (PII).	A LOT of questions about Data Protection Impact Assessment (DPIA)?

Service availability

Digi-HTA	Both	NordDEC
Key management and response or reporting of events must not interfere with normal operation.	-	-

Failure security

Digi-HTA	Both	NordDEC
-	-	-

Audit logging

Digi-HTA	Both	NordDEC
Logging to enable regulatory handling and forensics of data breaches. Centralised log database and list of items to log. Integration with SIEM. Logs can be provided to customer upon request.	-	-

Intrusion detection

Digi-HTA	Both	NordDEC
Document how security is monitored and managed. Alerts, malware protection, application whitelisting.	Is the system monitored?	-

Incident response

Digi-HTA	Both	NordDEC
Requirements for backup and restore scheme, technology and tools.	-	-

System updates

Digi-HTA	Both	NordDEC
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.	-	Can rollback to previous version?

Usability of security

Digi-HTA	Both	NordDEC
Provide user documentation. Automatically lock-out/hide PII after inactivity.	-	Evidence of user involvement in design and testing? User notifications? On-line support.

Life-cycle requirements

Vendor security

Digi-HTA	Both	NordDEC
Vendor organization must implement security measures, personnel are informed and trained on security. Data in bankruptcy situations, obligation to notify customer of personnel, subcontractor or consultant changes. Use access control lists.	Use qualified staff.	Data Protection Officer (DPO).

Policies & laws

Digi-HTA	Both	NordDEC
Vendor must direct authority data requests to the customer.	GDPR and other privacy laws must be followed.	A lot of questions about Data Protection Impact Assessment (DPIA)!

Development process

Digi-HTA	Both	NordDEC
Secure 3rd party components. Customer documentation security, must review plans with customer.	Secure development processes, change management. Security testing including penetration testing.	Independent expert involvement.

Security requirements

Digi-HTA	Both	NordDEC
-	Perform risk analysis.	Roadmap of future development.

Security standards

Digi-HTA	Both	NordDEC
-	Use security standards.	-

Vulnerability management

Digi-HTA	Both	NordDEC
Monitor vulnerabilities and report them appropriately. Support mitigation of vulnerabilities	Confidential data breach handling. Accept reports from outsiders.	-

User communication

Digi-HTA	Both	NordDEC
Provide user with timely information about security risks, vulnerabilities, updates, etc.	-	-

Funded by the European Union – NextGenerationEU

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] Nordic Digital Health Evaluation Criteria - NordDEC. (2022). Updated 15th of June 2022. [cited 13 January 2023]. Available https://confluence.external-share.com/content/7a7e9bac-472b-49ad-a8e4-d1fd13b95199

[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 13 January 2023]. 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 13 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 13 January 2023]. 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 13 January 2023].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 13 January 2023]. 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