Funded by the European Union – NextGenerationEU

Comparison report of Digi-HTA and DiGAV ordinance

VOUTILAINEN MERJA[1]
KAKSONEN RAULI[2]
HAVERINEN JARI[1, 3]

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

14.4.2023
Finnish Coordinating Center for Health Technology Assessment

Version	Date and name of the version updater	Description of the update
1.0	12.12.2022 Merja Voutilainen	Baseline version
1.1	24.1.2023 Merja Voutilainen, Rauli Kaksonen	Cyber security
1.2	30.1.2023 Jari Haverinen, Merja Voutilainen	The comparison of the general parts
1.3	14.4.2023 Jari Haverinen	A new version based on updated version of DiGAV

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

Table of Contents

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

1. Background

Digi-HTA is a health technology assessment (HTA) method developed for digital products and services in social, health care, and well-being in Finland [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. The perspectives of the assessment include effectiveness, costs, safety, data protection and security, and usability and accessibility. In addition to these, issues affecting the introduction of a digital product are examined, such as the treatment process and IT changes.

The Digital Health Applications Ordinance (DiGAV) is the ordinance on the procedure and requirements for assessing the reimbursability of digital health applications in statutory health insurance in Germany. DiGAV evaluates digital health applications classified as a medical device, but it does not apply to well-being applications. At the time of writing, only risk class I and IIa medical devices can be included in the assessment process, but classification will be expanded to include medical devices up to class IIb. Every digital health application (Digitale Gesundheitsanwendungen, DiGA) needs to be successfully assessed by the *Governmental Institute for Drugs and Medical Devices (BfArM)* in order to be listed in the directory of reimbursable DiGA. In the application, the manufacturer specifies whether it is applying for permanent inclusion in the DiGA directory or temporary inclusion. The details of this process are regulated in the DiGAV, which is examined in this report. [4]

The purpose of this document is to summarize the results of the comparative analysis of Digi-HTA and DiGAV. The goal is to produce transparent and reliable reference material in the comparison work.

The comparison workflow was driven by the on-going rise of digital health technologies (DHTs) and the increasing demand for high quality and comprehensive assessment of mHealth, artificial intelligence (AI) 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 the DHT classified as a medical device [5,6]. The same applies to digital 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 requirements. A comparison by category is presented in the following sections. The middle column "Both" summarizes the requirements shared by both sets of criteria. The requirements unique for each set of criteria are summarized in the left- and right-hand columns. This comparison work was conducted in 08/2022-04/2023 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 assessment methods

Summary of the most important considerations in the comparison of Digi-HTA and DiGAV:

1. The product assessed in DiGAV must be a CE marked medical device. Digi-HTA can assess non-medical devices as well.
2. DiGAV assesses only digital health applications, which may include mobile applications, browser-based applications, standard software, software as a service solutions, etc. DiGA may also include hardware components such as sensors, but the main functionality should be digital. Digi-HTA also focuses on covering the wide range of DHTs including hardware devices with embedded software integrations, for example robotic solutions.
3. In Digi-HTA and DiGAV, the key assessment domains were named differently. This comparison report has been implemented based on the domains used by Digi-HTA.
4. In both assessment models, the assessment of the product takes about 2-3 months.
5. The Digi-HTA assessment process is free of charge for the companies, while BfArm charges companies for the assessments.
6. Since DiGaV is based on a German legislation, additional regulations regarding administrative procedure are also mentioned separately in it.

Digi-HTA also has robotics and artificial intelligence as additional domains of assessment, but these are not found in DiGAV. Therefore, they are excluded from this comparison.

Product

Digi-HTA [1]	Both	DiGAV [4]
Information about product maturity level: Technology Readiness Level (TRL) of the product. If the product has not yet been released, when will the finished product be available?	General information about the product, its functionalities and supported platforms.	CE marking is prerequisite for the product to be eligible for assessment and introduced into the reimbursement process. Risk classes I or IIa included.
Information about the CE-marking of the product. A declaration of conformity document is required for CE marked products.	Information about the intended purpose and intended users of the product.	Consumer protection. The manufacturer should provide to the user of a digital health application all the information needed to make a usage decision on the sales platform or on the application's website. • Functions and features • The compatibility of the digital health application with systems and devices • The medical purpose of the digital health application • Information about all costs for end-user is transparently communicated
Is the product classified as a medical device according to MDD or MDR? If so, what risk class? Does the product have FDA approval?	The exclusion criteria for use of the product. Note that in Digi-HTA, this is covered under the usability and accessibility domain, but in DiGAV, is part of the safety domain.	Digital health applications shall be free of advertising.
In addition, products classified as non-medical devices can be assessed. In those cases, a manufacturer provides a rationale document clarifying why the product is not classified as a medical device.	Information about product support. Digi-HTA covers end-users and healthcare organizations. DiGAV covers mainly the end-user. In DiGAV, German-language support for end-users is mandatory.	If applicable, information about medical institutions and organizations that participated in the development of the digital health application.
Information about if the product is intended to replace current healthcare services and if so, what services?	Operating instructions for end-users.	If health information will be offered for the patient, is the information appropriate and up-to-date?
Information about if the product is already in use elsewhere in Finland or worldwide and if so, where and for how long?	Are instructions or support available for healthcare service providers to ensure fluent introduction of the product?	If applicable, information about the notified body involved in the conformity assessment procedure in accordance with the applicable medical device legislation.
Information about company's post-market surveillance plans.		Information about the minimum duration of use of the digital health application deemed necessary by the manufacturer
If the product is battery-operated, what are the charging, idle and operating times?		

Effectiveness

In DiGAV, the digital health application should provide positive patient-relevant health effects; either a medical benefit, or patient-relevant structural and procedural improvements in care. Correspondingly, in Digi-HTA, in addition to the positive health effects that are significant for the patient, benefits that are significant for the operation of the healthcare organization are assessed as well. In DiGAV, the studies must be carried out in Germany. If studies are conducted outside Germany, their transferability to the German healthcare context must be proven. A country of origin of studies is not specified

in Digi-HTA. The transferability to the Finnish healthcare context will be investigated on a case-by-case basis.

Digi-HTA	Both	DiGAV
Description of effectiveness from the perspective of healthcare organizations or system, and the availability of evidence to support it. Explanation for any missing evidence about the clinical benefits, behavioral changes or system/organizational effects. Information about ongoing studies to investigate the product's effectiveness in Finland or in other countries. Information about any institutions (e.g., another country's HTA agency) that recommend the product.	Description of the product's health benefits, and the availability of evidence to support of it. Description of the product's effects on users' actions or behavior favorable for their health, and the availability of evidence to support it.	Patient-relevant improvement of structure and processes in healthcare, which supporting the health behavior of patients or better integrating the processes between patients and healthcare providers.

Safety

Both Digi-HTA and DiGAV require appropriate measures to guarantee product safety. In DiGAV, the necessary measures are mentioned in the regulation at a more general level, while in Digi-HTA the questions are more specific. DiGAV states in § 3 that "*Proof of safety and suitability for use is, in principle, considered to be provided by the declaration of conformity document for products classified as medical devices. The BfArM may carry out additional tests on justified reasons. To that end, it may require the manufacturer of the digital health application to provide the necessary documentation, in particular the declarations and certificates necessary for the conformity assessment procedure.*" DiGAV also requires that the patient be clearly informed about possible risks when using the product and how they can be avoided.

Digi-HTA	Both	DiGAV
What is the company's process to handle customer safety events (deviations/errors, safety incidents, close calls or adverse events)? Is a risk analysis available for the product and will it be updated regularly? Have any product-related customer safety events been reported, and who is the responsible person in the company for handling Manufacturer Incident Reports? National references for safety supervision.	Is there any evidence available related to safety of the product? The company provides links to public results or attaches available documents (e.g., the declaration of conformity document) to response materials. Does the manufacturer implement appropriate measures to improve patient safety? Are there any undesirable effects associated with misuse of the product?	The manufacturer should clearly indicate for which users and indications the digital health application should not be used, if there are any restrictions. The user of the digital health application should be informed about possible risks and the necessary measures to reduce or avoid them. In connection with critical measurement values or analysis results, the digital health application clearly indicates for end-user the need to consult a doctor or other

Has it been ensured that there are no errors in the product instructions or that their occurrence has been made as unlikely as possible?		healthcare service provider. The digital health application recommends the end-user to stop using it if the aforementioned critical condition is detected. Consistency conditions are defined in the digital health application for all values entered by the end-user or collected via the connected medical devices or sensors or taken from other external sources The error messages of the digital health application are clear and informative.

Costs

In Germany people covered by the statutory health insurance are entitled to use DiGA prescribed by a physician or psychotherapist. DiGAs are reimbursed by health insurance companies. BfArM charges fees and expenses for individually attributable public services in accordance with the provisions mentioned in the ordinance. A vendor of digital health application can define free pricing for a one-year preliminary period. Pricing negotiations will be started after a permanent listing in the DiGA directory. There is no reimbursement system linked to Digi-HTA in use in Finland at the time of writing. The costs for the end-user and the service provider have been detailed in the Digi-HTA assessment.

Digi-HTA	Both	DiGAV
Economic evidence will be assessed. Accurate information on the formation of costs and the amount of costs for the end-users. What kind of initial costs does the introduction of the product impose on the organization, including changes to buildings or facilities, a need for new devices and software, as well as needed training? Information about the maintenance costs (e.g., monthly service fee) to the organization for the use of the product. The uncertainty factors of the costs.		Economic evidence will not be assessed. Information about all costs is transparently communicated for end-user.

Technical Stability

Digi-HTA	Both	DiGAV
Reference to IEC 62304 life cycle process standard. Description about the product's testing process. Information about company's process for handling the error messages. How the company informs the end-user or organization using the product about the updates and do software/system updates cause downtime in the use of the product? Has there been any downtime or impairment time in the use of the product during the last six months?		Is the digital health application robust against malfunctions and operating errors? Possible malfunctions and operating errors have been listed • Sudden power outage will not result in loss of data • Sudden loss of internet connection will not result in loss of data • The digital health application checks the plausibility of measurements, inputs and other data from external sources • The digital health application includes functions for testing and/or calibrating connected medical devices and sensors

Usability and accessibility

Both Digi-HTA and DiGAV assess the availability and the accessibility of the product from the end-user point view. If a digital application for healthcare professionals exists in the digital solution under assessment, this will be assessed by Digi-HTA as well. Digi-HTA refers to the Finnish national legislation requirements for accessibility if those are applicable to the product under assessment [8].

Digi-HTA	Both	DiGAV
The development of the usability and accessibility of the product should be a continuous process that can be influenced based on customer feedback. The manufacturer should clearly indicate for which users and indications the product should not be used, if there are any restrictions. Refers to WCAG 2.1 AA accessibility guidelines. Has an accessibility assessment been conducted for the product? Is there an accessibility statement available for the product, which describes possible deficiencies in accessibility? [7,8] Is an electronic feedback channel available for users to submit	The product has been tested with users representing the real end-users of the product. In the design of the product, the design guidelines of the mobile application platform have been followed. Mobile app platform accessibility features will be supported. The product offers accessibility for people with disabilities.	Is the digital health application easy and intuitive to use?

accessibility feedback? Does the company respond to accessibility feedback within 14 days?

Interoperability

Digi-HTA	Both	DiGAV
Information about whether the product has interfaces to websites, other software, other companies' services, electronic patient records or Finnish Kanta services. Information about the data formats used in any such interfaces • 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? If so, are the definitions of the original proprietary formats openly available?	Does the product support ISO/IEEE 11073 PHD compliant interfaces in connections with health or wellness devices?	The digital health application must allow the end-user to export therapy-relevant extracts of the data collected via the digital health application in human-readable and printable form, so that they can use them for their own purposes or pass them on to a physician. The digital health application must allow the end-user to export the data collected from the digital health application in a machine-readable, interoperable format so that the end-user or a third party authorized by the insured person can further process these data via other digital products. Requirement from 1 January 2024 onwards: The digital health application must enable data processed by the digital health application to be transferred to the electronic health record at any time with the end user's consent. Are the standards and profiles used to ensure the interoperability of the digital health application published and can they be used in a non-discriminatory manner?

3. Comparison of the cybersecurity

The goal of this task is to compare the technical content of two cybersecurity requirement documents:

- 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)
- Digital Health Applications Ordinance - DiGAV requirements. (Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV) [4]. Issue date: 08.04.2020, last change 22.9.2021. Machine translated from German to English by Google search.

The former 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]. All in all, the coverages provided by the two security requirement collections are quite similar. DiGAV has 158 individual requirements in 22 category groups and Digi-HTA 241 requirements in 23 category groups. The differences are relatively small.

It is important to understand that the comparison concerns the *categories* of security requirements and not the detailed content of the requirements themselves. For example, are there security requirements for *Interface Security* or *Authentication*? Even within a category, the practical requirements may quite different. This is unfortunate, but as there is no consensus on the best way to implement cybersecurity, the requirements vary between standards.

Security design

Digi-HTA [2]	Both	DiGAV [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.	Careful with personal data.	Use standard components for authentication. Web services running in limited accounts. Validate data from external systems.

Secure programming

Digi-HTA	Both	DiGAV
-		-

Delivery & deployment

Digi-HTA	Both	DiGAV
The vendor must provide system hardening instructions, including firewall, and tools to check proper system deployment. The system must not use default passwords.	Secure by default.	Installation conditions for sensors.

Administration

Digi-HTA	Both	DiGAV
Requirements for secure administration, integration with external security systems, and other similar requirements.		Administration of sensors.

Interface security

Digi-HTA	Both	DiGAV
Firewall requirements. Removal of unused ports, accounts, debug interfaces, and software. Limit external connections, wireless security. Tolerate security scanning.	Protective measures, removal of unused services.	Files are removed after use. User uploads secured. Input validation and prevention of injection vulnerabilities. No security parameter leaks.

Authentication

Digi-HTA	Both	DiGAV
	Authentication is required. Central authentication function. Strong user authentication, e.g., multi-factor or biometric. Encrypted passwords and automated logout. Authentication of external connections.	

Access control

Digi-HTA	Both	DiGAV
	Access control of users, must use user roles.	

Security hardware

Digi-HTA	Both	DiGAV
Safety integrated system (SIS) security.		-

Backend security

Digi-HTA	Both	DiGAV
Separation of users in multi-tenant cloud systems.		Web-server-specific requirements.

Cryptography

Digi-HTA	Both	DiGAV
Centralized digital key, management, X.509 certificates. Possibility to update encryption algorithms.	Use of strong and contemporary encryption. Password encryption.	

Data protection

Digi-HTA	Both	DiGAV
Personally identifiable information (PII) shall not be used in development.	PII must be stored in the EU. PII must be protected and regulations complied with. Users must be provided with control over their own PII. Multi-vendor/data processor responsibilities documented. Protect data in transit and rest. Use data export standards. Decommissioning.	Minimize handled PII.

Service availability

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

Failure security

Digi-HTA	Both	DiGAV
-		Errors must be handled properly.

Audit logging

Digi-HTA	Both	DiGAV
Integration with SIEM. Logs can be provided to customer upon request.	Logging of security-related events must be done securely.	-

Intrusion detection

Digi-HTA	Both	DiGAV
Alerts, malware protection, application whitelisting.	Monitor logs.	Denial of service (DOS) protection.

Incident response

Digi-HTA	Both	DiGAV
Requirements for Backup and Restore scheme, technology and tools.	-	Resetting of sensors to secure state.

System updates

Digi-HTA	Both	DiGAV
Vendor shall provide tools for secure updating. Updates agreed with customers. Update all parts of the system.	Inform users of the availability of new versions.	

Usability of security

Digi-HTA	Both	DiGAV
	Automatically lock-out/hide PII after inactivity. Provide security-related user documentation.	

Life-cycle requirements

Vendor security

Digi-HTA [1]	Both	DiGAV [4]
Data in bankruptcy situations, obligation to notify customer of personnel, subcontractor or consultant changes. Use access control lists.	Th vendor organization must implement security measures, personnel are informed and trained on security.	Vendor must implement ISO 27001 as specified.

Policies & laws

Digi-HTA	Both	DiGAV
PII storage locations must be documented. The vendor must direct authority data requests to the customer.	GDPR and other privacy laws must be followed.	A privacy plan is required. A data retention policy is required. Policies must be readily available for users and users must be informed of them. Stored PII data must be minimized. Visibility of PII must be limited also within the vendor's system.

Development process

Digi-HTA	Both	DiGAV
Customer documentation security, review plans with customer. Security testing.	Secure development processes, change management, handling of 3rd party components, penetration testing. Bill of materials (BOM) is required.	Vendor must have a procedure to check effectiveness of processes.

Security requirements

Digi-HTA	Both	DiGAV
Safety requirements	Perform risk analysis.	Perform structured protection requirement analysis with given damage scenarios. Requirements for sensor installation.

Security standards

Digi-HTA [2]	Both	DiGAV [4]
	Use security standards.	

Vulnerability management

Digi-HTA	Both	DiGAV
Monitor vulnerabilities and report them appropriately. Support mitigation of vulnerabilities.	Alert users.	Observe public vulnerability information.

User communication

Digi-HTA	Both	DiGAV
Inform customers about vulnerabilities.	Provide users with timely information about security updates.	Notify users about password resets.

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] Digital Health Applications Ordinance - DiGAV requirements. (Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV). Cited 23 January 2023. Available from: https://www.gesetze-im-internet.de/digav/BJNR076800020.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 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