FinJeHeW Finnish Journal of eHealth and eWelfare

SCIENTIFIC PAPERS

VERTAISARVIOITU
KOLLEGIALT GRANSKAD
PEER-REVIEWED
www.tsv.fi/tunnus

Digi-HTA, assessment framework for digital healthcare services: information security and data protection in health technology – initial experiences

Jari Jääskelä [1], Jari Haverinen [2,3], Rauli Kaksonen [1], Jarmo Reponen [3,4], Kimmo Halunen [1], Teemu Tokola [1], Juha Röning [1]

[1] Biomimetics and Intelligent Systems Group, University of Oulu, Oulu, Finland; [2] Finnish Coordinating Center for Health Technology Assessment (FinCCHTA), Oulu, Finland; [3] FinnTelemedicum, Research Unit of Medical Imaging, Physics and Technology, Faculty of Medicine, University of Oulu, Oulu, Finland; [4] Medical Research Center Oulu, Oulu University Hospital and University of Oulu, University of Oulu, Oulu, Finland

Jari Jääskelä, Biomimetics and Intelligent Systems Group, University of Oulu, Pentti Kaiteran katu 1, FI-90570 Oulu, FINLAND. Email: jari.jaaskela@oulu.fi

Abstract

It is well-known that security issues in medical devices, services and applications have potentially catastrophic consequences. To avoid compromising patient data or information systems, it is essential that healthcare services and products meet the relevant information security and data protection requirements. For these reasons, the Digi-HTA assessment includes information security and data protection assessment domains. The outcome of the Digi-HTA process is a recommendation that decision-makers can use during the procurement process. We present results and experiences from the first assessments made in the Digi-HTA process.

We have assessed six products so far and multiple assessments are in progress. The results indicate that healthcare product manufacturers have found the process useful, and usually, the manufacturers have had to improve the security of their product during the Digi-HTA process to get a favourable recommendation for their product. The assessment processes have taken longer than expected due to shortcomings and ambiguities in the provided self-assessment forms, and due to feedback cycles and meetings prompted by assessment findings. Of the six assessed products, four received a green light in information security and data protection, whereas two have received a yellow light due to issues that were not fixed during the process. In addition to shortcomings in adhering to best practices, we have also found exploitable security issues.

Keywords: health technology assessment, telemedicine, cyber security

Introduction

The term *health technology* covers all kinds of treatment methods to solve health problems and to improve the quality of life, such as medicines, medical devices, and healthcare and medical systems. Health technology assessment (HTA) is an evidence-based evaluation of health technologies. Purpose of the HTA is to support decision-makers in decisions relating to the introduction of new health technologies. [1]

One example of how HTA can inform decision-makers was the Managed Uptake of Medical Methods (MUMM) program previously used in Finland [2]. The MUMM program provided recommendations for health technologies and the recommendations used a three-tier traffic light model to inform decision makers.

Information for HTA reports will be collected in a systematic, transparent, unbiased, and robust manner by using a multidisciplinary process [3]. The full HTA reports cover nine domains: (1) the health problem and current use of technology; (2) description and technical characteristics of the new technology; (3) safety assessment; (4) clinical effectiveness; (5) economic evaluation, typically cost-effectiveness analysis or cost-utility analysis; (6) ethical analysis; (7) organizational aspects; (8) social aspects; and (9) legal aspects [3,4]. However, it is not possible to make such comprehensive HTA reports in all cases, but information is needed faster and with a lighter procedure, such as by using the mini-HTA method [5]. The mini-HTA questionnaire was developed by Danish HTA experts and is used in Finland to perform rapid HTA assessments [5,6].

The increasing amount of novel digital health technologies (DHT) pose new challenges on how to comprehensively apply HTA activities in their assessment [7-9]. However, a lot of determined work has been done in many countries to ensure that HTA takes into account the requirements of DHT products [10-12]. In some countries the assessment of DHT applications has also been combined with a national reimbursement model, such as in the DiGA process in Germany [13]. However, it should be noted that in addition to mHealth application the term DHT covers several different digital technologies, such as artificial intelligence (AI) and robotics solutions and combinations of many digital technologies [8,14]. In order to support the evidence-based introduction of new and innovative digital technologies in Finnish healthcare, the Digi-HTA method was developed and published in 2019 [8]. Since then, Digi-HTA process has been part of day-to-day HTA activities of the Finnish Coordinating Center for Health Technology Assessment (FinCCHTA) for DHT products and published recommendations can be found on the FinCCHTA website [15].

Traditionally, HTA has been focusing mainly on effectiveness, cost, and safety of health technology, as in the MUMM program. However, during the development of Digi-HTA, it was noted that product usability and accessibility, as well as information security and data protection, are also key domains to be included in the DHT assessments [8]. The same trend can be seen in other European countries. For example, European mHealth HUB has recently evaluated available HTA frameworks for mHealth and they stated that information security and data protection issues are somewhat considered in the majority of the frameworks [10]. If a DHT is insecure or does not follow data protection requirements, it will more likely expose organizations and end-users to major risks, such as financial consequences, health risks or even death than a DHT which takes these issues into consideration.

It is also important to keep in mind that HTA is not the only tool that organizations can use in their procurement process to take information security into account. As an example, the European union agency for cybersecurity (ENISA) has created a guideline for how to take cybersecurity into account during procurement of healthcare services [16]. Another source for security requirements that can be included in the procurement is the OWASP Application Security Verification Standard (ASVS) [17].

In this article, we will focus on the information security and data protection assessment domains of Digi-HTA. We have performed information security and data protection assessments using the Digi-HTA criteria during 2020 and 2021. The process produces a recommendation for each assessed DHT. Organizations can use the recommendation in the procurement process. This article first explains the HTA process for healthcare products. Then, we will introduce the Digi-HTA framework, and the information security and data protection criteria used in this framework [18], which were developed in the Kyber-Terveys project. Finally, we will discuss our findings, compare it to other similar HTA processes and discuss how the process could be improved in the future. The abstract of this article was originally published the eHealth2021 conference [19].

Digi-HTA assessment process

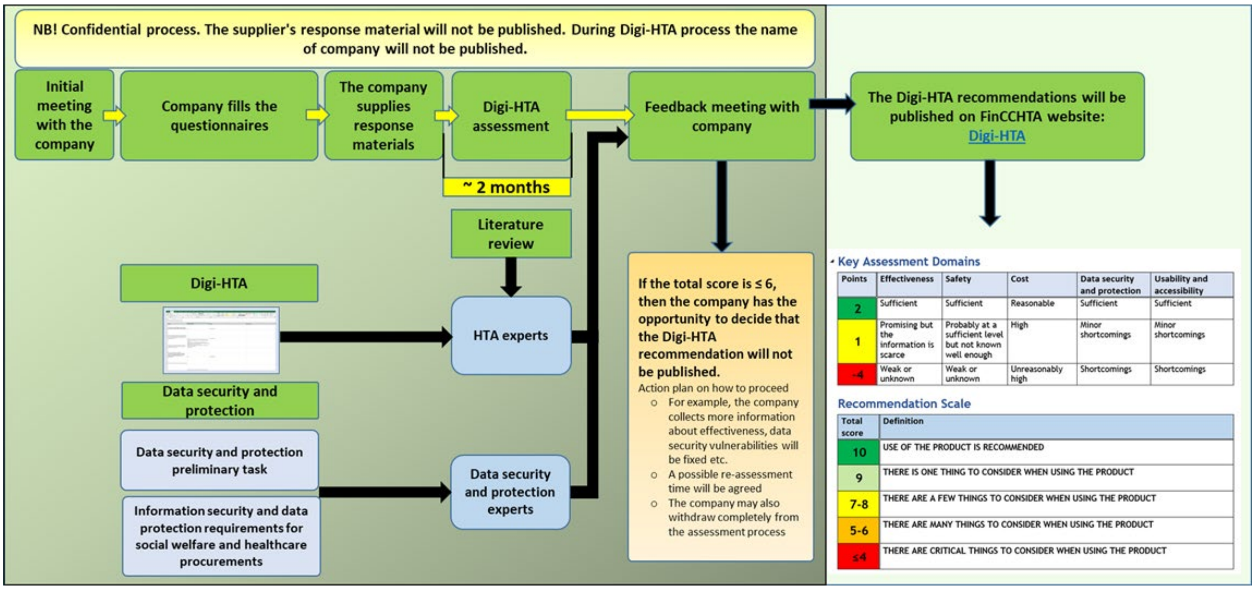
The overall workflow of the Digi-HTA process is shown in Fig 1. There is no service fee for the companies who participate in the process. In this section we will focus on the security and data protection assessment domains, see [8] for a more detailed description of the whole Digi-HTA process.

After the kick-off meeting, the company manufacturing the DHT product fills out the security and data protection self-assessment form. This form is based on the criteria developed for healthcare procurements in the Kyber-Terveys project and published on the Finnish national cybersecurity centre (NCSC-FI) website [18]. The criteria has been derived from the industry best practices and standards. The company decides which requirements are relevant for their product and provides sufficient evidence for these requirements. In addition, the company fills out a preliminary task with information about the architecture and data flow within the system and what kind of personal and health data it stores and processes. The response material will be checked by the auditor. The auditor will create more specific questions about the product for the company to answer if the assessment of the product requires more information or evidence.

The information security and data protection requirements in the criteria range from organization and management security requirements, such as those defined in the ISO27001 standard (for example, security awareness training and risk management) to product technical security requirements, such as role-based access control, support for multi factor authentication (MFA) and use of secure data communication channels, such as HTTPS (hypertext transfer protocol secure). Most of the data protection requirements in the criteria are derived from the regulation, most notably from the general data protection act (GDPR). Table 1. presents the overview of the common information security and data protection requirements. This list highlights the requirements that are relevant to most of the products that undergo the

Digi-HTA process and what evidence the Digi-HTA auditor reviews regarding these requirements.

Recommendation is the outcome of the Digi-HTA process. Digi-HTA recommendations use a three-tier traffic light model in five key domains of assessments. Based on these five key domains, a final statement and overall score is given the entire product [8]. The traffic light model is the modified version of the approach previously used in the MUMM program recommendations [2]. After the recommendation draft has been written, the auditors will have a feedback meeting with the company in which the recommendation is discussed. If the product is going to receive a total score of six or less, the company can drop-out of the process in order to have time to fix the issues. In this case the recommendation will not be published.


NB! Confidential process. The supplier's response material will not be published. During Digi-HTA process the name of company will not be published.
Initial meeting with the company
Company fills the questionnaires
The company supplies response materials
Digi-HTA assessment
~ 2 months
Feedback meeting with company
The Digi-HTA recommendations will be published on FinCCHTA website: Digi-HTA
Literature review
Digi-HTA
HTA experts
Data security and protection
Data security and protection preliminary task
Information security and data protection requirements for social welfare and healthcare procurements
Data security and protection experts

If the total score is ≤ 6, then the company has the opportunity to decide that the Digi-HTA recommendation will not be published.

Action plan on how to proceed

- For example, the company collects more information about effectiveness, data security vulnerabilities will be fixed etc.
- A possible re-assessment time will be agreed
- The company may also withdraw completely from the assessment process

Key Assessment Domains

Points	Effectiveness	Safety	Cost	Data security and protection	Usability and accessibility
2	Sufficient	Sufficient	Reasonable	Sufficient	Sufficient
1	Promising but the information is scarce	Probably at a sufficient level but not known well enough	High	Minor shortcomings	Minor shortcomings
-4	Weak or unknown	Weak or unknown	Unreasonably high	Shortcomings	Shortcomings

Recommendation Scale

Total score	Definition
10	USE OF THE PRODUCT IS RECOMMENDED
9	THERE IS ONE THING TO CONSIDER WHEN USING THE PRODUCT
7-8	THERE ARE A FEW THINGS TO CONSIDER WHEN USING THE PRODUCT
5-6	THERE ARE MANY THINGS TO CONSIDER WHEN USING THE PRODUCT
≤4	THERE ARE CRITICAL THINGS TO CONSIDER WHEN USING THE PRODUCT

Figure 1. Digi-HTA assessment process.

Table 1. Overview of common security requirements and evidence that is reviewed by the Digi-HTA auditor.

Category	Requirement	Evidence
Information security risk management	• Comprehensive security risk assessment	• Security risk assessment documents
Data protection & GDPR	• System shall have the capability to encrypt data using a method that is strong according to current standards • All sensitive data shall be stored and located within the EEA • Vendor must be in the EEA • Customer owns the collected data • System must comply with GDPR • All personal data must be located within EEA • Vendor must direct all inquiries from authorities to the customer and wait for response • Customer owns the personal data, it must not be used for development or testing purposes	• Data Protection Assessment (including data protection risk assessment) • Privacy policy • How data is protected at-rest • Data-flow diagram • List of 3rd party services that process personal data
Security testing	• Security testing must be included as part of software/solution development	• Documentation about security testing practices
Update management	• Vendor shall run all relevant security patches regularly	• Documentation about software update practices
Authentication & Authorization	• The system has the capability to use and enforce strong passwords according to current standards • All stored passwords shall be hashed using a method designed for passwords that is strong according to current standard. If this is not possible, passwords must be encrypted. • The system shall have capability to use and enforce multi-factor authentication • System shall have capability to enforce two-way authentication of all system-to-system connections. • The system shall support common identity federation protocol • The system shall follow the principle of least privilege	• Documentation about the authentication system and what secondary controls it supports • Documentation about how the system supports configuring roles to restrict access
System monitoring	• System shall alert when the performance level is endangered • Vendor shall document how the system is monitored and managed • Vendor shall log and report to customer any security compromise immediately after detection • Logging system must provide reliable information that enables tracing malicious use	• Documentation about system monitoring practices
Logging	• Vendor shall have processes that enable generating logs about audit data access activity • System shall have capability to transfer logs to centralized logging database • Vendor shall log both successful and unsuccessful login attempts • Admin operations must be logged reliably • Activities concerning personal data must be logged reliably	• Documentation about logging practices • How the logs are protected and audited

Hardening	• Vendor shall have an up-to-date hardening guide • Vendor shall ensure that only required ports and services are enabled • Vendor shall remove or disable all unused system accounts	• Hardening documentation
Interface security	• Vendor shall provide a method for exchanging data using a secure communication channel • Vendor system shall have the capability to exchange data using open standard communication data formats	• How data is protected in-transit • Data-flow diagram • What protocols and data formats the system uses

Results

Both the quantity and variety of DHT products is increasing in all kinds of healthcare services. This trend is also visible in the products that have undergone or are involved in the Digi-HTA assessment process: there is considerable diversity in the technological solutions as well as the different end users' groups. The intended purpose of the products may be e.g., the self-assessment of symptoms, to support care or to monitor the Activities of Daily Living (ADL). So far, all the products involved in the Digi-HTA process have included an mHealth, web-based or desktop application. The reviewed products have included robotic devices, measurement sensors, communication devices, and artificial intelligence algorithms. The different DHT products and their application areas that have gone through the Digi-HTA assessment process or are already involved in the assessment process are shown in Table 2. Most of the products utilize the SaaS (software-as-a-service) delivery model and therefore do not require on-premise installations. However, sometimes the products also have an option for on-premise deployment because some organizations want to deploy services on-premise instead of on cloud.

Table 2. The different DHT products that have gone through or are involved in the Digi-HTA assessment process.

Area of healthcare services	Intended purpose	Digital healthcare technology (DHT) solution	End users
Specialized care	Intelligent digital service to monitor patients' symptoms remotely	mHealth application	Patients
		Web-based application	
		Web-based application Integrated artificial intelligence (AI) algorithm to improve the functionality of the product	Healthcare professionals
	Digital service to support remote monitoring in a hospital environment	Monitoring device	Healthcare professionals
		Web-based application mHealth application	Healthcare professionals
Rehabilitation	Exoskeleton robotic solution to support rehabilitation	Robotic device	Patients
		mHealth application	Healthcare professionals
Home care	Digital platform to monitor the status of home care patients	Sensors and communication devices to monitor the Activities of Daily Living (ADL)	Older adults
		mHealth application	Elderly relatives
		mHealth application	Healthcare professionals
		Web-based application	
	Medicine dispensing robot solution to support care	Robotic device	Older adults
		mHealth application	Healthcare professionals
		Web-based application	
Primary care	Digital service to support self-monitoring for the symptoms of patients and to provide personalized care	mHealth application	Patients
		Web-based application	Healthcare professionals
		Integrated AI algorithm to improve the functionality of the product.	
	Remote measuring and monitoring of health status of patients	mHealth application	Patients
		Measuring and monitoring device with wireless connection	
		Web-based application	Healthcare professionals

We have published six recommendations so far and two have opted out of the process. Eighteen companies have indicated their willingness to participate in the Digi-HTA assessment process. Four of these companies have provided their response material and an assessment of these products is ongoing. Usually, manufacturers have been very cooperative. A couple of times we have had to discuss with the manufacturers about which risks are relevant and whether risks are mitigated to an acceptable level.

The assessment of a product usually takes about 10 - 30 work hours including writing the recommendation, meetings, and other communication. However, the process from kick-off to publication usually spans over multiple quarters. This is mainly due to delays in the evidence material delivery, and due to the shortcomings and ambiguities in the provided self-assessment forms.

Table 3. presents published Digi-HTA assessments and traffic lights for each key assessment domain as well as the overall recommendation for the products. Of the six assessed products, four received a green light in information security and data protection, whereas two have received a yellow light due to issues that were not fixed during the process. Even though the purpose of the assessment process is not to do security testing, but to confirm if the product and manufacturer follow the relevant best practices defined in the assessment criteria, we have also found some security issues. For example, one product which later dropped out of the process had access credentials to the backend infrastructure hardcoded into the mobile application. A malicious actor could have read them and thus gained an access to the personal and health data stored in the database. Another product had some insecurely designed features and used risky cryptographic algorithms.

Table 3. Published Digi-HTA assessments.

Product	Effectiveness	Safety	Cost	Information security and data protection	Usability and accessibility	Overall recommendation
Medicine dispensing robot solution	🟨	🟩	🟩	🟩	🟩	🟩
Exoskeleton robotic solution to support rehabilitation	🟨	🟩	🟩	🟨	🟩	🟨
Intelligent digital service to monitor patients' symptoms remotely	🟩	🟩	🟩	🟩	🟨	🟩
Robotic solution to support rehabilitation	🟨	🟩	🟩	🟨	🟩	🟨
Digital platform to monitor the status of home care patients	🟨	🟩	🟩	🟩	🟨	🟨
Digital service platform for home care	🟨	🟩	🟩	🟩	🟩	🟩

Discussion

Digi-HTA information security and data protection assessment process is based on the information security and data protection criteria developed in the Kyber-Terveys project. The auditor works in collaboration with the manufacturer to determine which requirements are relevant to their product and if they meet the requirements to a satisfactory level in relation to the risks. The audit is based on the evidence provided by the manufacturer. The process does not include penetration testing, code reviews, or other technical audit activity to determine if the security controls and other security requirements are implemented correctly. Because of this, the process will not catch the majority of the implementation issues, such as an incorrect implementation of access control policy.

The purpose of the Digi-HTA assessment is to inform the decision-makers how well the product meets the security requirements defined in the assessment criteria. While the criteria used in the assessment is based on best practices and standards, it is not comprehensive. Even if the criteria would be comprehensive that would not guarantee that the product is secure. The purpose of security requirements is to try to minimize the identified risks to an acceptable level. In addition, the security control or procedure should be implemented correctly, otherwise it does not mitigate the risk as expected. As already mentioned, implementations of technical requirements are not reviewed in this process. While the framework requires that the manufacturer has procedures for security testing, it does not currently set strict requirements for the testing. For these reasons, it is also essential that manufacturers perform security testing, penetration testing, and other security improvement activities themselves. For example, these activities could include use of SCA (software component analysis) or SAST (static application security testing) tools or yearly external penetration testing.

Digi-HTA is not the only one HTA process with information security and data protection aspects. NHS in the UK reviews mobile health applications. They are using the Digital Technology Assessment Criteria (DTAC) [11]. For information security and data protection this criteria leverages the NHS Data Security and Protection Toolkit [20]. They also provide detailed guides for auditors on how to review the evidence which Digi-HTA currently does not have. In this process they also require that the developer provides an external penetration test report which is not a mandatory requirement in Digi-HTA currently.

Another HTA process, is the DiGA [13], which includes an information security and data protection checklist that the manufacturer must fill-out. Even though GDPR permits processing of data outside the EU under the Articles 45 and 46, DiGA forbids this explicitly. When they have identified a very high need for data protection, they require a penetration test report from the manufacturer as does the to the DTAC in the UK.

The Digi-HTA recommendation should only be used as a pre-filter and not as a replacement for other procurement security practices. Organizations should always include their security and data protection requirements in the procurement because a generic framework cannot include every requirement that the customers may need, or they may accept less risks in general. Therefore, they may require stricter security controls and procedures from the manufacturers. Secondary security controls, such as multi factor authentication (MFA) is one common example of this kind of security control. Instead of incorporating these kinds of requirements into the traffic light assessment, we bring up these kinds of things to consider in the recommendation body text. For these reasons, the IT department should always be involved in procurement to ensure that the necessary security expertise is present. We also recommend that organizations take a look at the guideline created by the European union agency for cybersecurity (ENISA) for how to take cybersecurity into account during procurement of healthcare services [16].

Currently some organizations in Finland require that the product has a Digi-HTA recommendation in their request for proposal. In addition to meeting this requirement, manufacturers can also use the recommendation in their public marketing material.

The manufacturer should be aware of what security requirements the customers expect them to fulfil. For this, the manufacturer can use a publicly available list of security requirements, such as the criteria used in this assessment process, the guide created by ENISA [16] and the Application Security Verification Standard [17] created by the OWASP foundation.

We are iteratively improving the assessment process by collecting feedback via surveys. In August 2021, we updated the recommendation structure to be more informative and to include information about what accredited certifications the product and the manufacturer have. It is also important to keep in mind that the certification may not cover everything, for example, the manufacturer may have only certified their support department for ISO 27001. The assessment criteria will be improved upon continuously as we discover new requirements that should be added to the criteria. We are also considering creating guidelines for auditors on how to review the evidence provided by the manufacturers. Detailed audit guides enforce consistent audit quality across multiple assessments and would make onboarding and training new auditors into the assessment process easier.

Acknowledgements

The development and launch of the Digi-HTA framework happened in the project called Oulu DigiHealth Knowledge Hub funded by the Regional Council of Northern Ostrobothnia (funding from the European Regional Development Fund).

FinCCHTA is funded by the Northern Ostrobothnia Hospital District. Digi-HTA information and data protection assessment activity is funded by the Finnish National Emergency Supply Agency.

Conflict of interest statement

None.

References

[1] World Health Organization. Health technology assessment [Online]. Copenhagen: WHO Regional Office for Europe [cited 17 October 2021]. Available from: https://www.euro.who.int/en/health-topics/Health-systems/health-technologies-and-medicines/policy-areas/health-technology-assessment.

[2] Sihvo S, Ikonen T, Mäkelä M. Implementing health technology assessment-based recommendations in Finland: Managed uptake of medical methods. Int J Technol Assess Health Care. 2017 Jan;33(4):430-433. https://doi.org/10.1017/S0266462317000587

[3] European Network for Health Technology Assessment (EUnetHTA). Assessment FAQ. What is health technology assessment (HTA)? [Online].

EUnetHTA; 2018 [cited 5 December 2021]. Available from: https://www.eunethta.eu/ja3services/submission-guidelines/submissions-faq/.

[4] Gyldmark M, Lampke K, Ruof J, Pöhlmann J, Hebborn A, Kristensen F. Is The Eunethta Hta Core Model® Fit for Purpose? Evaluation From an Industry Perspective. Int J Technol Assess Health Care. 2018 Jan;34(5):458-463. https://doi.org/10.1017/S0266462318000594

[5] Danish National Board of Health. Introduction to Mini-HTA – a management and decision support tool for the hospital service. [Online]. Copenhagen; The National Board of Health, Danish Centre for Evaluation and Health Technology Assessment 2005 [cited 5 December 2021]. Available from: http://www.sst.dk/~/media/47C62A769EBC4E80A153F986C5348F55.ashx.

[6] Räsänen P, Hytönen M, Pakarinen S, Blom M. Menetelmäarvioinnista tukea päätöksentekoon. Lääkärilehti. 2021;45(76):2660-2662.

[7] Vis C, Bührmann L, Riper H, Ossebaard H. Health technology assessment frameworks for eHealth: A systematic review. Int J Technol Assess Health Care. 2020 Jun;36(3):204-216. https://doi.org/10.1017/S026646232000015X

[8] Haverinen J, Keränen N, Falkenbach P, Maijala A, Kolehmainen T, Reponen J. Digi-HTA: Health technology assessment framework for digital healthcare services. FinJeHeW 2019;4(11):326-341. https://doi.org/10.23996/fjhw.82538

[9] Alami H, Lehoux P, Auclair Y, De Guise M, Gagnon M, Shaw J, et al. Artificial Intelligence and Health Technology Assessment: Anticipating a New Level of Complexity. J Med Internet Res. 2020 Jul 7;22(7):e17707. https://doi.org/10.2196/17707

[10] European mHealth Hub. D2.1 Knowledge Tool 1. Health Apps Assessment Frameworks. [Online]. European mHealth Hub; 2020 [cited 17 October 2020]. Available from: https://mhealth-hub.org/download/d2-1-knowledge-tool-1-health-apps-assessment-frameworks-pending-ec-approval.

[11] NHSX. Digital Technology Assessment Criteria (DTAC). [Online]. NHSX; 2021 [cited 17 October 2021] Available from: https://www.nhsx.nhs.uk/key-tools-and-info/digital-technology-assessment-criteria-dtac/.

[12] Bundesministerium der Justiz und für Verbraucherschutz. Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung (Digitale Gesundheitsanwendungen-Verordnung - DiGAV). [Online, In German]. Bundesministerium der Justiz und für Ver-braucherschutz; 2020 [cited 17 October 2021]. Available from: https://www.gesetze-im-internet.de/digav/BJNR076800020.html.

[13] Federal Institute for Drugs and Medical Devices. The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users [Online]. Bonn: Federal Institute for Drugs and Medical Devices (BfArM); 2021 [cited 17 October 2021]. Available from: https://www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.html.

[14] Zion Market Research. Global mHealth Apps Market Will Reach USD 111.1 Billion By 2025: Zion Market Research [Online]. Zion Market Research; 2019 [cited 17 October 2021]. Available from: https://www.globenewswire.com/news-release/2019/01/24/1704860/0/en/Global-mHealth-Apps-Market-Will-Reach-USD-111-1-Billion-By-2025-Zion-Market-Research.html.

[15] FINCCHTA. Digi-HTA [Online]. Oulu University Hospital, FINCCHTA; 2021 [cited 17 October 2021]. Available from: www.digi-hta.fi.

[16] ENISA. Procurement Guidelines for Cybersecurity in Hospitals [Online]. The European Union Agency for Cybersecurity (ENISA); 2020 [cited 17 October 2021]. Available from: https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services.

[17] OWASP. OWASP Application Security Verification Standard [Online]. OWASP; 2020 [cited 17 October 2021]. Available from: https://owasp.org/www-project-application-security-verification-standard/.

[18] TRAFICOM, Finnish National Emergency Supply Agency. Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset [Online]. TRAFICOM; 2019 [cited 17 October 2021]. Available from: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/sosiaali-ja-terveydenhuollon-hankintojen-tietoturva-ja.

[19] Jääskelä J, Tokola T, Halunen K, Röning J. Digi-HTA, assessment process for digital healthcare services and products: information security and data protection in health technology - initial experiences. In: Suomen telelääketieteen ja eHealth seura ry. eHealth2021. The 26th Finnish National Conference onTelemedicine and eHealth “eHealth in a Lifecycle.” [conference proceedings]. Finnish Society of Telemedicine and eHealth (FSTeH) publication 1/2021. Oulu: Grano Oy; 2021 p. 38.

[20] NHS. Data Security and Protection Toolkit. [Online]. NHS; 2021 [cited 16 October 2021]. Available from: https://www.dsptoolkit.nhs.uk/.