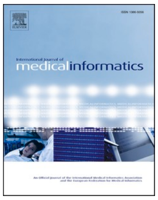
International Journal of Medical Informatics 177 (2023) 105141

Contents lists available at ScienceDirect

International Journal of Medical Informatics

journal homepage: www.elsevier.com/locate/ijmedinf



Review article

Apps in healthcare and medical research; European legislation and practical tips every healthcare provider should know

Sebastiaan L. van der Storm [a,b,c,*,1], Marilou Jansen [a,b,c,1], Henriëtte A.W. Meijer [a,b,c], Esther Z. Barsom [a,b,c], Marlies P. Schijven [a,b,c,*]

[a] Amsterdam UMC location University of Amsterdam, Surgery, Meibergdreef 9, Amsterdam, the Netherlands
[b] Amsterdam Gastroenterology and Metabolism, Amsterdam, the Netherlands
[c] Amsterdam Public Health, Digital Health, Amsterdam, the Netherlands

ARTICLE INFO

Keywords:
Mobile applications
Medical apps
Health apps
Safety
Legislation
Data privacy
Medical device

ABSTRACT

Background: The use of apps in healthcare and medical research is increasing. Apps in healthcare may be beneficial to patients and healthcare professionals, but their use comes with potential risks. How to use apps in clinical care is not standard part of medical training, resulting in a lack of knowledge. As healthcare professionals and their employers can be held accountable for the wrongful use of medical apps, this situation is undesirable. This article addresses the most important European legislation regarding medical apps from the perspective of healthcare providers.

Methods: This review provides an overview of current and changing regulations, focusing on apps used in healthcare and medical research. Three topics are discussed: 1) the relevant European legislation and its enforcement, 2) the responsibilities and liability of the medical professional when using these apps, and 3) an overview of the most practical considerations medical professionals should know when using or building a medical app.

Results: When using and developing medical apps, data privacy must be guaranteed according to the GDPR guidelines. Several international standards make it easier to comply with the GDPR, such as ISO/IEC 27001 and 27002. Medical Devices Regulation was implemented on May 26, 2021, and as a result, medical apps will more often qualify as medical devices. The important guidelines for manufacturers to comply with Medical Devices Regulation are ISO 13485, ISO 17021, ISO 14971 and ISO/TS 82304–2.

Conclusion: The use of medical apps in healthcare and medical research can be beneficial to patients, medical professionals, and society as a whole. This article provides background information on legislation and a comprehensive checklist for anyone wanting to start using or building medical apps.

1. Background

The use of mobile applications (‘apps’) has gained solid ground in healthcare. Currently there are over 400.000 health apps available on app stores worldwide. [1] Health and welness apps can be defined as apps operating on smartphones that process health-related data or information, as medical apps are considered to be used for medical or clinical purposes. [2] Medical apps may thus facilitate not only patients, but also healthcare professionals (HCPs), their institutions, and society as a whole. Medical apps can aid in access to, distribution, exchange, management and maintenance of information and even facilitate clinical decision making. [3] An important benefit of using an app on a personal mobile device is the possibility of (inter-)connectivity. The use of apps on mobile devices enables the use of integrated sensors like the gyroscope, accelerometer, camera or microphone. [4] Although the use of apps in healthcare and medical research can be convenient and may improve quality of care, there are associated risks. Before using or developing an app, it is important to decide what objective needs to be met and to investigate if the app is truly the best and a reliable solution. Wrongful use of an app, or rightful use in the wrong context, is potentially harmful. [5] This is especially applicable to medical apps that fail to provide any evidence of its effectiveness or safety. [6].

[*] Corresponding authors at: Box 22660, 1105 AZ Amsterdam, the Netherlands.
E-mail addresses: s.vanderstorm@amsterdamumc.nl (S.L. van der Storm), m.p.schijven@amsterdamumc.nl (M.P. Schijven).

[1] Shared first authorship.

https://doi.org/10.1016/j.ijmedinf.2023.105141
Received 7 April 2023; Received in revised form 27 June 2023; Accepted 2 July 2023
Available online 3 July 2023

How to critically appraise an app or how to use an app responsibly, is not a standard part of the medical curriculum. As a result, HCPs including medical researchers, often lack knowledge of the safe use of medical apps. This is an unwanted scenario, as HCPs can be held accountable for the wrongful use of nonconfirmative medical apps. Although this problem has existed for longer, the social-cultural discussion has been accelerated by both the covid-19 pandemic as well as the implementation of the Medical Device Regulation (MDR). [7] MDR safeguards stringent requirements for technical development, validation, quality surveillance, and manufacturing.

This study serves three purposes. First, to provide an overview of current and relevant European legislation applicable to medical apps and the institutes responsible for legal enforcement. Second, this study gives an overview of responsibilities and liabilities relevant to the medical professional who use medical apps. Finally, to provide the reader with a framework to critically appraise existing medical apps including a comprehensive checklist for those building and/or using medical apps. Several studies on the safe use of medical apps have been published, however most of them focus on the framework provided by the FDA. [8,9] To our knowledge, this is the first study to focus on the contemporary European regulations.

2. Part Ia: European legislation

2.1. General Data Protection Regulation

In several apps, personal data is used as input and sometimes even as output. For example: the covid-19 status of someone passing through the street, including the date and time of the encounter. Using or processing personal data has to be done in compliance with the General Data Protection Regulation (GDPR). [10] The GDPR was adopted on April 14th 2016 and came into effect on May 25th 2018. The GDPR is a regulation on data protection, based on the principle that the individual is and remains the owner of their data. The GDPR unifies law on European level superseding the Data Protection Directive 95/46/EC. [11].

Most patient data qualifies as special personal data. Under the GDPR the processing of health data is prohibited, unless one of the exceptions in Article 9 of the GDPR is applicable. [10,12] For example; the subject - in this scenario the patient - gives unambiguous consent to use their data and the reasons for processing the data outweigh the risks related to processing the data. It is necessary to have appropriate protection measures when processing data. The GDPR rests upon pillars like the 'Data protection by default' and 'Data protection by design' principles (Art. 25 of the GDPR). [10].

Sometimes, data is only used temporarily as input to generate output, such as a risk score, prognostic value, or therapeutic advice. It is important to keep in mind that software manufacturers, or the hosts of the server where the data is processed, can have temporary access when processing data and as a result becoming the data processor. [9] As an organization or health institution providing a medical app (defined as the data controller), it is important to have a *data processing agreement* with the processor in place. [10,13].

It is also possible that data is stored longer or even permanently. Data storage usually takes place on a server, which is sometimes owned by the health institution itself. However, commercial applications often rely on third parties to facilitate use of apps and the related data storage. The server where data is stored must be compliant with the requirements formulated within the GDPR, see Table 1. Companies offering data storage in compliance with the GDPR can be recognised by certain certifications. These certifications are granted for a standardized period by certifying bodies if companies comply with the standards published by the International Organization for Standardization (ISO) or International Electrotechnical Commission (IEC). ISO/IEC developed and published worldwide standards for the GDPR requirements. Examples of such certifications include ISO/IEC 27001 for information security management. ISO/IEC 27002 provides control mechanisms for creating the information security as described in ISO 27001.

Table 1
Requirements for data collection, processing and storage according to the GDPR.

Requirements for personal data collection, proccesing and storage	
Lawfulness, fairness and transparency	Personal data should be processed in a lawful, fair and transparent manner
Limited purpose	Personal data should only be collected for a specified use
Confidentiality and integrity	Personal data should be processed according to the appropriate security level and should be protected against unauthorized access, accidental loss, destruction or damage
Data minimisation	The collection of personal data should be limitied, only data relevant to accomplish the specific purpose should be collected
Storage limitation	Data should not be stored longer than needed to accomplish the specified use
Accuracy	Personal data should be accurate and kept up to date when applicable

Not all software manufacturers have experience building in medical apps and their associated specific guidelines regarding the protection of patient data. Therefore, it is advisable to work with a software manufacturer who is experienced in working in the medical app domain or to involve someone to oversee the project and advise on requirements. The Data Protection Officer of an institute can serve as a starting point. [10].

2.2. Medical Device Regulation

The Medical Device Regulation (MDR) came into force on May 26th 2021, after a prolonged transit period of four years in total. [7,14] The MDR is effective in all members of the European Economic Community (EEC), including Switzerland, Norway, Iceland,Liechtenstein and excluding Great-Britain. The MDR replaced the Medical Device Directive (MDD) (93/42/EEC). [15] As the MDD was a European directive, its implementation in national laws varied among members of the EEC. Legislation became non-transparent, making it difficult and time-consuming for manufacturers to release new products onto the market, and regulation of medical devices was problematic. The new MDR should improve transparency, decrease time from innovation to market and provide a better overview of available medical devices.

As a HCP, the MDR is important to be aware of, as health apps easily meet the definition of a medical device. According to the MDR, 'medical device' means:

"any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:

— diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,

— diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,

— investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,

— providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations…".

(Fragment of the official definition of a medical devices as provided in the MDR) [15].

In the new regulation, software is specifically addressed. Software includes all programs and other operating information used by a hardware device. Software can be stand-alone, such as a computer program or a medical app, or part of a medical device such as an infusion pump. If an app is defined as a medical device, it must meet corresponding standards to ensure safety, quality and performances. One of the required standards is the application of CE-marking.

2.2.1. CE-marking

The manufacturer is responsible for determining the risk class of the medical app and for the application of the Conformité Européenne (CE)-marking.The mark guarantees that the medical device is in concordance with the MDR and that the appropriate conformity assessment procedures have been followed in order to determine so. The CE-marking is valid in all members of the EEC. It is important to note that it is a compliance mark, and not a quality mark. Every medical device has an intended purpose, wherefore it was specifically designed by the manufacturer. The conformity assessment procedure is specifically followed for the intended purpose; therefore, the CE-mark is only applicable for the intended purpose.

The conformity assessment procedure depends on the risk class to which the medical device belongs. Class I indicates the lowest risk and class III indicates the highest risk. To determine the risk category of a medical device, the manufacturer should follow the “Implementing rules” in chapter II and the “Classification rules” in chapter III of Annex VIII of the MDR. If a medical device belongs to risk class I, the manufacturer itself can assess the new medical device and apply CE-marking when all requirements from the conformity assessment are met. Whenever a medical device belongs to any other risk class, only a relevant Notified Body (NB) can perform the conformity assessment procedure. Notified bodies are designated organisations to assess the conformity of products, and in this specific scenario, medical devices. The member states of the European Union can designate an organisation within their own state. The Nando-database (New approach notified and designated organisations) lists all notified bodies that are designated to perform conformity assessment procedures according to the MDR. [16] It is important to realise, that products that were already on the market under the MDD will not be revoked, however they should meet the MDR when the current CE-marking expires.

3. PART Ib: Enforcement

3.1. Enforcement of the GDPR

The GDPR provides rules that are directly applicable in all Member States as of May 25th 2018. Under the previous Data Protection Directive (DPD), each EU Member State had to transpose the directive into internal law, resulting in differences in the enforcement of these laws (Art. 4, DPD). [9] Enforcement of the GDPR is facilitated by the European Data Protection Board (EDPB). This board consists of 28 Data Protection Authorities (DPA’s) from all Member States and the European Data Protection Supervisor (EDPS). The EDPS is appointed by a joint decision of the European Parliament and the Council for a five-year term. The current term started on December 6th 2019. [17] Under the GDPR, it is possible for the national DPA’s to make binding decisions including the option to impose a fine (Art. 83 and 84 GDPR). The national DPA’s handle reports of data breaches, they can mediate in disputes between data processors and controllers, but they can also undertake their own research. [10].

3.2. Enforcement of the MDR

The NB’s and Competent Authorities (CA’s) as indicated by the European Commission are entrusted with the enforcement of the MDR. One of the topics of MDR is the increased post-market surveillance. This implies that the manufacturer should continue to meet requirements during the entire lifecycle of the product. NB’s and CA’s can perform an unannounced audit to enforce the MDR (Chapter 7, Art. 80, 90). In many cases annual performance and safety reporting will be mandatory. [15] It is important to note, that only manufacturers of medical devices with risk II and higher are audited by NB’s. NB’s can implement their own audit processes, however, they are required to follow the ISO 17021 standard for the MDR. Most NB’s will create a quality management system (QMS) following the ISO 17021, ISO 14971 and ISO 13485 standard (see Table 2). [18,19] The aforementioned standards are not legally valid on their own, however they provide guidelines for the practical implementation of the MDR.

To keep track of all available medical devices and to improve coordination between EU member states, every medical device should have an Unique Device Identifier (UDI) and be registered within the European database on medical devices (EUDAMED). [20].

Wrongly applying or not applying CE-marking, or uncomplying to the standards for post market surveillance, is ground for penalization. The most common reasons for failing an audit are: providing an incomplete search strategy, providing an incomplete audit trail, using ad hoc processes, questionable data integrity and providing non-transparent documentation. The NB usually gives the manufacturer an opportunity to revise documentation and visit again, sometimes even several times. When standards are not met after the re-audit, a manufacturer can be fined and ultimately, the NB can decide that CE-marking should be revoked. Consequently, the medical device should then be withdrawn from the market.

4. Part II: Responsibility and liability of the end-user

The manufacturer is the legal person responsible for compliance with the GDPR and the MDR of an app. However; any person, organization or company that puts a name or trademark on a medical device is stated as the manufacturer. In healthcare it is imaginable that a HCP has an idea for an app and then starts looking for a manufacturer. In large healthcare organisations, this may be facilitated in-house, but in smaller organisations this may be an external party. In the first scenario, the healthcare organisation is also the manufacturer. In the second scenario, where the app was built by an external party, the issue of who is deemed the manufacturer is more complex. For example, when the healthcare organization publishes an externally built app in the app stores, it is the healthcare organisation who legally becomes the manufacturer. When a healthcare organization uses a preexisting app, but rebrands the app to match the corporate identity, the healthcare organization might become the manufacturer as well. In those scenario’s it is important to be aware of the responsibilities attached to being the manufacturer, or legally transfer them to the organization or party that actually built the app. [21].

When considering using a pre-existing app it is important to realise that the HCP using or advising the medical app can be held responsible when any harm occurs to the end user. Imagine a HCP considering a diagnostic test for a specific patient. The HCP uses a medical app to aid his/her decision and decides not to perform a diagnostic test based on the outcome advice of the app. What if the HCP misses an important finding or diagnosis? When the HCP uses an app that has been thoroughly tested and complies with all applicable legislation, the HCP cannot be held responsible as an individual healthcare provider, but the

Table 2
Overview of relevant international standards when implementing the updated GDPR and MDR.

International Standards	
ISO 27,001	Provides requirements for an information security management system (ISMS)
ISO 27,002	Is an information security standard that provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining an ISMS.
ISO 14,971	Specifies terminology, principles and a process for risk management of medical devices, including software as a medical device. The standard helps manufacturers to estimate and evaluate the associated risks, to control these risks, and to monitor the effectiveness of the controls.
ISO 13,485	Provides the requirements for a comprehensive quality management system for the design and manufacture of medical devices.
ISO 17,021	Contains principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems.

manufacturer can be. A manufacturer can also be held responsible for an app on which a CE-marking is wrongly applied or does not comply with the standards for post market surveillance. When HCPs decide to use an app which is not CE-marked it is their miscalculation to choose this app and therefore both the HCP and the organization they are working in, can be held responsible. Every medical device has a clearly stated intended use; the medical device is tested and certified for this use. When the HCP uses the app for purposes other than the intended use, the manufacturer cannot be held responsible. Manufacturers will therefore be very specific in formulating the intended use of a medical device. In this regard, it is essential that apps to be used are assessed on their quality and safety conformity and intended use, which may be done by several frameworks as discussed in the next section.

5. Part III: Where to start and what to do when using or developing an app as a medical device

In this part of this article, theoretical knowledge from the previous sections is translated into a practical checklist for using or developing an app as a medical device.

5.1. Critical appraisal of medical apps

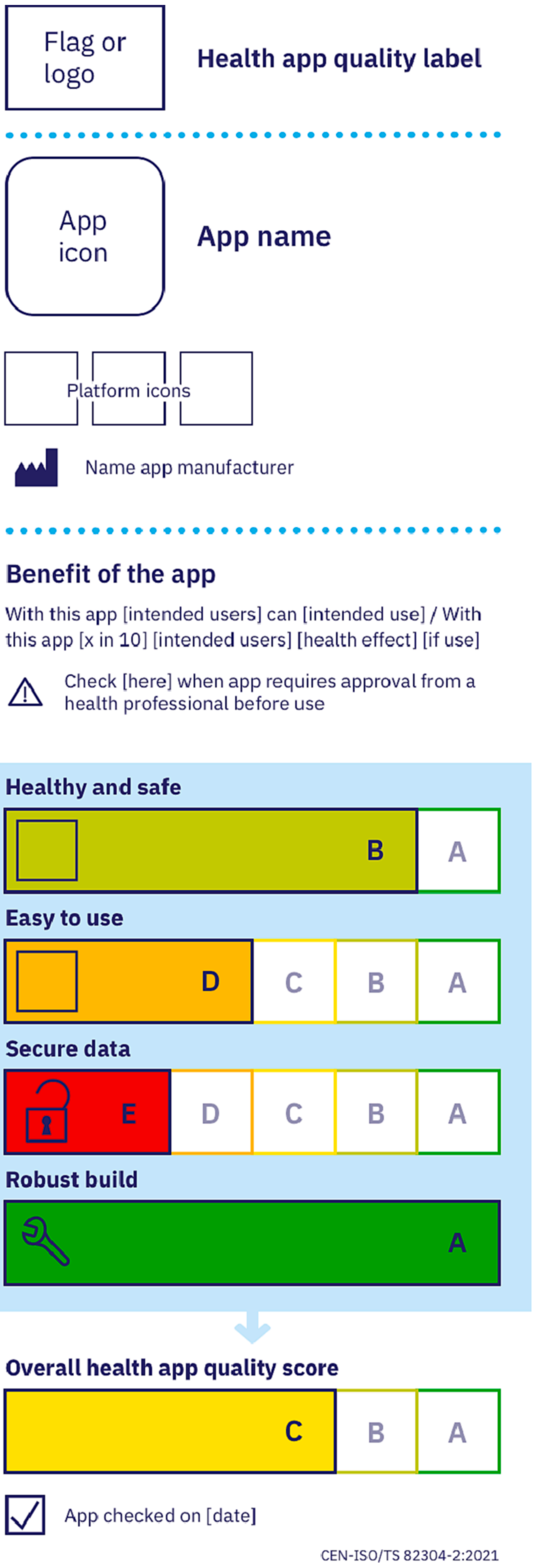
Within the overwhelming amount of apps it is challenging to find the apps with peer reviewed content and in compliance with the GDPR and MDR. Medical apps should be assessed on several aspects. A frequently used framework to assess medical apps are the Health on the Net (HON)-criteria. [22]. The HON foundation was founded in May 1996 and promoted the effective and reliable use of the new technologies for telemedicine in healthcare worldwide. Unfortunately, this non profit organisation was not able to maintain their foundation and has discontinued their services as of December 15, 2022. The mHealthHUB, supported by the European Union's Horizon 2020 research and innovation programme, has published a knowledge tool reviewing available frameworks in 2021. [23] In August 2021 a new standard was published regarding the quality requirements for health and wellness apps, the ISO/TS 82304–2. The standard covers the entire life cycle of a medical app (post market surveillance and quality control). Apps are scored on four different domains, as shown below in Fig. 1. An overall quality score is also provided. [24].

5.2. Building custom medical apps

When there is a healthcare scenario that cannot be addressed using an existing medical app meeting the necessary requirements, one can decide to build a new app. In order to do so the right way, the following aspects must be considered (see also Fig. 2).

a) Conditions

Any medical app must meet specific healthcare oriented privacy, design, and functionality criteria. To ensure that the app meets these conditions, content experts are needed, next to functional and graphical design specialists. If an app is designed to be used by patients, it is recommended that they be involved early in the development process. "Human factor engineering" or "patient included innovation" will improve the community support amongst intended users and decreases the risk of (wrong) usage of medical devices. An appropriate and well-functioning "User Interface" (UI) and "User Experience" (UX) of the app, designed together with the intended users, will help in presenting information effectively.Usability tests within the intended user group are important because only 30 to 60% of people can be considered health literate. [25] To validate the quality and safetey of the app, user trials or tests must also be incorporated in the development process, which is also specifically stated in the MDR.



With this app [intended users] can [intended use] / With this app [x in 10] [intended users] [health effect] [if use]

Check [here] when app requires approval from a health professional before use

Fig. 1. Quality label of health and wellness apps as published in the ISO/TS 82304–2.

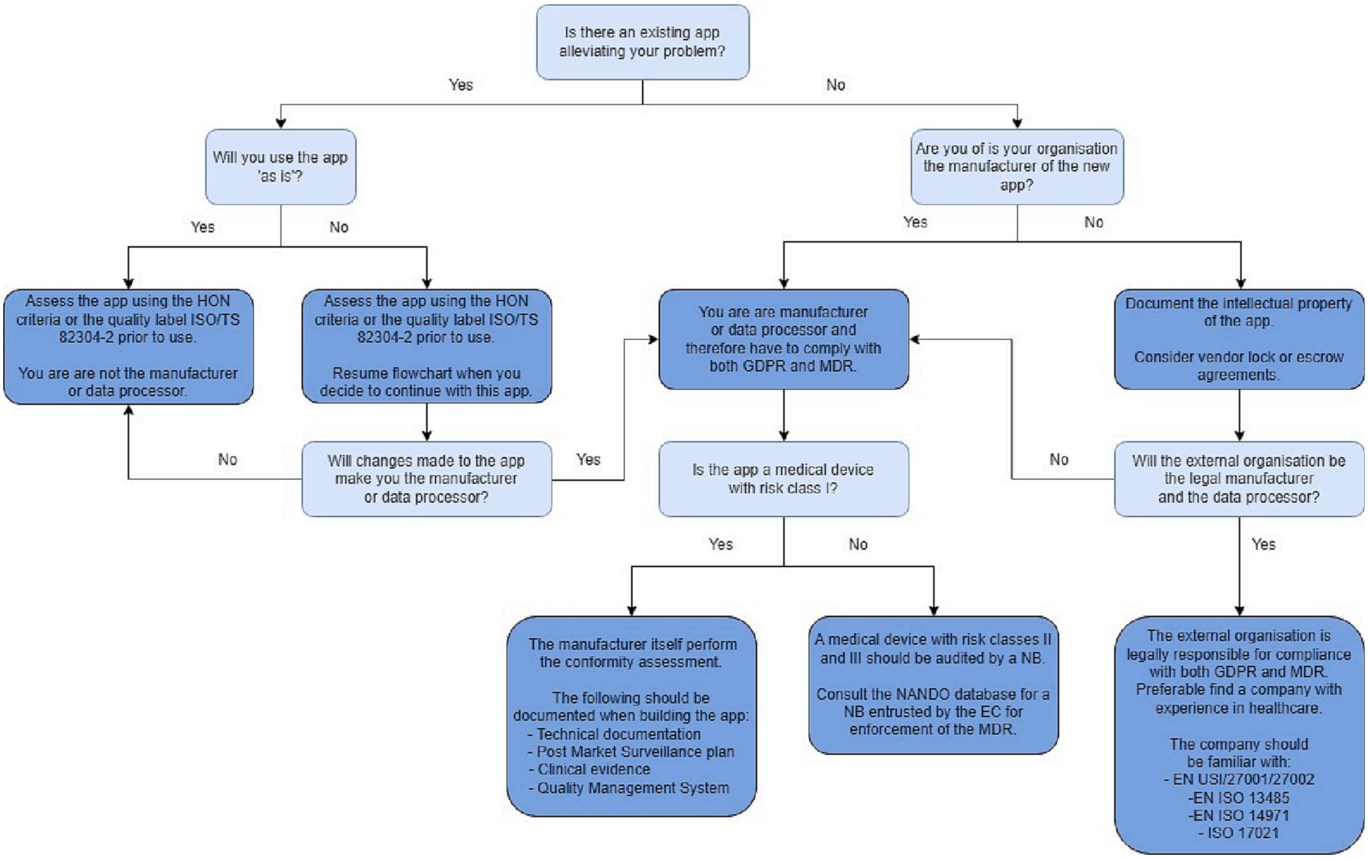

Is there an existing app alleviating your problem?
Yes
No
Will you use the app 'as is'?
Yes
No
Assess the app using the HON criteria or the quality label ISO/TS 82304-2 prior to use.
You are are not the manufacturer or data processor.
Assess the app using the HON criteria or the quality label ISO/TS 82304-2 prior to use.
Resume flowchart when you decide to continue with this app.
Will changes made to the app make you the manufacturer or data processor?
No
Yes
Are you of is your organisation the manufacturer of the new app?
Yes
No
You are are manufacturer or data processor and therefore have to comply with both GDPR and MDR.
Document the intellectual property of the app.
Consider vendor lock or escrow agreements.
Is the app a medical device with risk class I?
No
Will the external organisation be the legal manufacturer and the data processor?
Yes
No
Yes
The manufacturer itself perform the conformity assessment.
The following should be documented when building the app:
- Technical documentation
- Post Market Surveillance plan
- Clinical evidence
- Quality Management System
A medical device with risk classes II and III should be audited by a NB.
Consult the NANDO database for a NB entrusted by the EC for enforcement of the MDR.
The external organisation is legally responsible for compliance with both GDPR and MDR.
Preferable find a company with experience in healthcare.
The company should be familiar with:
- EN USI/27001/27002
-EN ISO 13485
-EN ISO 14971
- ISO 17021

Fig. 2. Checklist of the most important considerations when using or developing a medical app.

b) Intellectual property.

If an app is developed by a contracted external developer, a good contract must be in place. It must be clearly defined who is the data processor of the app and who is the manufacturer, and thus who is responsible for compliance to the GPDR and the MDR. Furthermore, it is advisable to record specifically in writing who will have the intellectual property (IP). The party funding the app development will not automatically be the owner of the source code of the app or the IP. If the initiator of the app fails to record the IP, the manufacturer will automatically become the owner of the app. [26] This situation can be problematic, when considering the transfer of the app to another external developer, especially if the current developer fails to comply with the agreements or legislations.

c) Privacy and safety.

Medical apps have to comply to the GDPR and the MDR. When employed in a healthcare facility, you can rely on the expertise of Data Protection Officer (DPO) who is familiar with current rules and regulations regarding data protection. A DPO can help to make sure the app complies with the required legislation. Otherwise, external expertise must be sought to comply to the GDPR. An external app designer/developer that regularly works in the healthcare setting, will be familiar with the processing of personal data and is therefore obliged to have employed a DPO. Additonally, healthcare facilities often employ a MDR expert who can provide support. The ISO 27001, ISO 27002, EN ISO 13485, EN ISO 14971 and ISO/TS 82304–2 standards provide more practical guidelines for building apps that are compliant with the MDR and GDPR.

d) Other agreements.

It is also advisable to decide on arrangements for situations that one would rather not consider. These situations include bankruptcy of an external manufacturer or a dissatisfying cooperation. In case of bankruptcy, the development and maintenance of mobile applications will stop. The source code will be transferred to a curator or another party (in the case of a takeover of the company). To ensure app development can continue at another chosen manufacturer, the source code must be transferred to the buyer/client/initiator. Predetermined arrangements, such as a vendor lock, or an escrow agreement must be drawn up. (10,24).

6. Conclusion

The discussion on the use of medical apps in healthcare and research is more vivid than ever. Apps have considerable potential for various purposes in healthcare, however it is crucial that apps are developed and used in a responsible manner and comply with relevant legislation. It is imperative for both app manufacturers and healthcare providers to be well-informed about diligent guidelines pertaining to privacy and medical device regulations. Healthcare providers should be aware of their responsibilities and liabilities when developing or using a medical app in healthcare or research. Through a comprehensive understanding of the legilations, responsibilitites and liabilties, both manufacturers and healthcare providers can contribute to the responsible and ethical use of medical apps, thereby maximizing their benefits while minimizing potential risks.

7. Summary table

What was already known on the topic?

- The use of apps in healthcare has increased significantly over the last years.
- Assessing quality and safety of medical apps is not part of standard medical training

What this study added to our knowledge.

- An overview of current and relevant European legislation applicable to medical apps and also of the institutes responsible for legal enforcement.
- An overview of responsibilities and liabilities relevant to the healthcare professional using medical apps.
- A framework to critically appraise existing medical apps as well as a comprehensive checklist for those developing an app.

All authors fulfill the requirements for authorship and have approved the final version of this manuscript.

What was already known on the topic?

- The use of apps in healthcare has increased significantly over the last years.
- Assessing quality and safety of medical apps is not part of standard medical training

What this study added to our knowledge.

- An overview of current and relevant European legislation applicable to medical apps and also of the institutes responsible for legal enforcement.
- An overview of responsibilities and liabilities relevant to the healthcare professional using medical apps.
- A framework to critically appraise existing medical apps as well as a comprehensive checklist for those developing an app.

Funding.

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Sebastiaan L. van der Storm: Writing – original draft. **Marilou Jansen:** Writing – original draft. **Henriëtte A.W. Meijer:** Writing – original draft. **Esther Z. Barsom:** Writing – original draft. **Marlies P. Schijven:** Supervision, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] WHO/ITU/Andalusian Regional Ministry of Health Initiative. mHealthHUB [Internet]. 20202 [cited 2022 Dec 27]. Available from: https://mhealth-hub.org/health-apps-repositories-in-europe.

[2] Laura Maaß, BA, MA, Merle Freye, Chen-Chia Pan, BSc, MA, Hans-Henrik Dassow, BSc, MA, Jasmin Niess, MSc, PhD, and Tina Jahnel, BA, MA, PhD. The Definitions of Health Apps and Medical Apps From the Perspective of Public Health and Law: Qualitative Analysis of an Interdisciplinary Literature Overview. JMIR Mhealth Uhealth. 2022 Oct; 10(10): e37980. Published online 2022 Oct 31. doi: 10.2196/37980 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9664324/.

[3] C.L. Ventola, Mobile devices and apps for health care professionals: uses and benefits, P T. 39 (5) (2014 May) 356–364.

[4] C. Baxter, J.A. Carroll, B. Keogh, C. Vandelanotte, Assessment of Mobile Health Apps Using Built-In Smartphone Sensors for Diagnosis and Treatment: Systematic Survey of Apps Listed in International Curated Health App Libraries, JMIR Mhealth Uhealth. 8 (2) (2020) e16741.

[5] S. Akbar, E. Coiera, F. Magrabi, Safety concerns with consumer-facing mobile health applications and their consequences: a scoping review, Journal of the American Medical Informatics Association. 27 (2) (2020 Feb 1) 330–340.

[6] S.L. van der Storm, M. Bektaş, E.Z. Barsom, M.P. Schijven, Mobile applications in gastrointestinal surgery: a systematic review, Surg Endosc. (2023 Apr 4), https://doi.org/10.1007/s00464-023-10007-y.

[7] European Parliament. REGULATION (EU) 2017/745 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [Internet]. 2017. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745.

[8] J. Shuren, B. Patel, S. Gottlieb, FDA Regulation of Mobile Medical Apps, JAMA. 320 (4) (2018 Jul) 337–338.

[9] P. Henson, G. David, K. Albright, J. Torous, Deriving a practical framework for the evaluation of health apps, Lancet Digit Health. 1 (2) (2019 Jun) e52–e54.

[10] European Parliament. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL [Internet]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434; 2016. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

[11] European Commission. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Internet]. 1995. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[12] GDPR.EU. GDPR checklist for data controllers [Internet]. [cited 2022 Dec 30]. Available from: https://gdpr.eu/checklist/.

[13] Wolford B. What is a GDPR data processing agreement?. 2020 [cited 2022 Dec 28]; Available from: https://gdpr.eu/what-is-data-processing-agreement/.

[14] European Commission. Commission postpones application of the Medical Devices Regulation to prioritise the fight against coronavirus [Internet]. 2020 [cited 2022 Dec 29]. Available from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_589.

[15] European Commission. Council directive 93/42/EEC of 14 June 1993 concerning medical devices [Internet]. Available from: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF.

[16] European Commissian. Notified bodies Nando [Internet]. Available from: https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.notifiedbody&dir_id=34.

[17] European Union. European Data Protection Supervisor [Internet]. [cited 2022 Dec 28]. Available from: https://edps.europa.eu/about-edps_en.

[18] International Organization for Standardization. ISO/IEC 17021-2:2016 Conformity assessment — Requirements for bodies providing audit and certification of management systems [Internet]. 2016 [cited 2022 Dec 31]. Available from: https://www.iso.org/standard/70682.html.

[19] International Organization for Standardization. ISO 13485:2016 Medical Devices [Internet]. 2016 [cited 2022 Dec 31]. Available from: https://www.iso.org/standard/59752.html.

[20] Europese Commissie. EUDAMED database [Internet]. [cited 2022 Nov 22]. Available from: https://ec.europa.eu/tools/eudamed/#/screen/home.

[21] Wessing T. Product Liability for Medicines and Medical Devices in the European Union [Internet]. 2016 [cited 2022 Dec 31]. Available from: https://www.taylorwessing.com/synapse/ti-eu-medical-product-liability.html.

[22] Health On the Net. mHONcode the new certification of Health Mobile Applications [Internet]. 2020 [cited 2022 Dec 30]. Available from: https://myhon.ch/en/certification/app-certification-en.html.

[23] WHO/ITU mHealthHUB in EU. Knowledge Tool 1: Assessment frameworks in mHealth [Internet]. 2021 [cited 2022 Dec 28]. Available from: https://mhealth-hub.org/documents.

[24] International Organization for Standardization. ISO/TS 82304-2:2021 Health software [Internet]. 2021 [cited 2022 Dec 31]. Available from: https://www.iso.org/standard/78182.html.

[25] G. Quaglio, K. Sørensen, P. Rübig, L. Bertinato, H. Brand, T. Karapiperis, et al., Accelerating the health literacy agenda in Europe, Health Promot Int. 32 (6) (2016 Apr) 1074–1080.

[26] M.E. Smith, A legal and practical guide to developing mobile medical applications ("'apps"'): navigating a potential minefield, J Mob Technol Med. 5 (1) (2016 Mar) 52–61.