Taking legal issues into consideration at an early stage

Digital health applications: Key points for developers and manufacturers

By Dr. Roland Wiring

Digitalization in the health care system is advancing relentlessly: Be it research, diagnostics, therapy or rehabilitation – there is hardly any area that is not affected. In view of this megatrend, it is not surprising that start-ups, midsize companies as well as big players are active here. In addition to technical challenges, numerous legal questions arise: Is my software a medical device? How do I protect my idea? What happens with the data? And who is liable if the self-learning app is wrong? Addressing these four core issues early on protects software vendors from unpleasant surprises in marketing.

The potential for medical software and AI in healthcare is enormous.

Medical software

Medical software applications, especially those that work with AI, are developing rapidly. The potential for AI in healthcare is enormous. It starts with preventive health care: fitness trackers and wellness apps are designed to promote healthier behavior. AI has become indispensable in the field of early detection and diagnostics. It is used to detect diseases such as cancer more accurately, reliably and earlier. This is done - in simple terms - by comparing the data collected from a particular patient - also in the form of images - with large amounts of data from other patients. So-called doctor support software can support clinical decisions and streamline processes on the basis of extensive health data. In addition, there are other fields such as remote treatment, the improvement of treatment plans, the monitoring of therapy success or the use of robotics, for example in operations.

Key legal issues for developers and manufacturers

The legal framework for medical software is complex. Different regulations overlap. But one should not be deterred by this. There are solutions for almost →

everything. Particularly in the initial phase, developers and providers should always take the following four topics into consideration.

Is my software a medical device?

A central question in the development of software solutions is the regulatory classification of the product. In this case, the main question is whether the software is a medical device. This is important in practice because medical devices may only be placed on the market if they bear a CE marking after a conformity assessment procedure has been carried out. If a product that is to be qualified as a medical device is placed on the market without a CE mark, there is a risk that a competitor will demand that the product not be sold. Furthermore, placing such a device on the market would constitute an administrative offence and may even have legal consequences.

According to the German Medical Devices Act (MPG) and the European Medical Devices Directive (MDR), which becomes effective in May 2020, the intended purpose of the software is decisive. Roughly speaking: If the software is intended to detect or treat diseases - for example, if it supports diagnosis, facilitates decisions on therapeutic measures or calculates the dosage of drugs, then it would be hard to argue against its classification as a medical device. If, on the other hand, the software only provides knowledge or only stores data, it is unlikely to be considered a medical device.

Further points from a medical-legal-regulatory perspective are the observance of medical professional law (the practice of medicine is reserved for physicians and alternative practitioners, i.e. it must not be carried out by software), aspects of pharmacovigilance in the generation of extensive data and the question of reimbursement which is being widely discussed at present. The Digital Supply Act (DVG) has brought important changes in this area. The law is intended to make it possible for patients to get health apps on prescription and to facilitate the use of online consultation hours. Breaking into the circle of prescribable software products is of considerable relevance for providers. It remains to be seen how the prerequisites for this will be designed in detail and which software will finally be introduced to the market. It is worthwhile in any case to closely follow current developments in order to generate appropriate data for later validation as early as possible.

» The topics of data protection and data security naturally have a very special relevance for medical software. «

How do I protect my idea?

Very important from the developer's and manufacturer's point of view is the question of whether and to what extent the idea of a medical app and its implementation can be legally protected. Plagiarists must be kept out. In any case, the conclusion of a non-disclosure agreement (NDA) is recommended for collaborations. It ensures that confidential information is only used for the common purpose of the collaboration and is not disclosed to third parties. This applies in particular to the protection of knowledge - i.e. internal business secrets. The legal requirements for the effective protection of such information and documents have recently increased. Unlike before, the secrets worthy of protection must be precisely defined and the circle of authorized persons must be kept as small as possible. Industrial property rights for software are difficult to obtain. At least in Germany, software is not considered patentable. However, a certain degree of protection is provided by copyright law and - particularly relevant for marketing - by trademark law.

What happens with the collected data?

The topics of data protection and data security naturally have a very special relevance for medical software. After all, many apps and AI solutions are based on the analysis and comparison of concrete patient data with a multitude of - mostly anonymized and aggregated - data from other patients. The requirements for effective consent management in the collection and use of personal health data have been high since the European General Data Protection Regulation (GDPR) came into force in May 2018. Legal challenges can usually be overcome by drafting declarations of consent in conformity with the law - in particular a clear definition of the planned use of data. Ensuring a high level of data security is also extremely important for reputational reasons. Data leaks can have devastating consequences for the affected providers, especially in the health sector.

→

Who is liable if something goes wrong?

Finally, as a developer or provider of medical software, one should deal with the question of possible liability and insurance of the corresponding risks at an early stage. Who has to take responsibility if the software gives a wrong recommendation? The programmer, the provider, the doctor or even the software itself? There are still many legal issues to be resolved. In addition to the principles of product liability law, a parallel with the liability of pet owners is sometimes considered: Similar to pets, self-learning medical software is a source of danger for which the owner - in this case the user - is liable regardless of fault. It remains to be seen in which direction the discussion, which is also being conducted at European level, will continue.

Conclusion

The potential for medical software and AI in healthcare is enormous. The unstoppable progress of digitization will ensure that applications based on AI will increasingly find their way into everyday treatment. It is advisable for the players active in this area to consider not only the technical aspects but also the legal issues at an early stage. In this way, legal risks can be analyzed, evaluated and mitigated. <–

Dr. Roland Wiring
Rechtsanwalt, Partner,
CMS Hasche Sigle,
Hamburg

roland.wiring@cms-hs.com

www.cms-hs.com