DetailHomeNewsDetail

10/22/2020

Be careful with health apps - the protection and security of patient data must have the highest priority the costs for these health apps can be covered by statutory health insurance, provided they have been prescribed by a doctor. The prerequisite for inclusion in the DiGA directory is, among other things, that the applications meet the requirements for data protection and that data security is guaranteed according to the state of the art (§ 139 e Para. 2 Sentence 2 No. 2 SGB V). It has now become known that IT security experts have found serious data protection deficiencies in one of the apps used to treat people with anxiety disorders. By exploiting the security gaps, attackers could have "unmasked" anxious patients as such and, in the worst case, taken over their accounts with sensitive data.

The Deputy State Commissioner for Data Protection and Freedom of Information (LfDI) Rhineland-Palatinate, Helmut Eiermann, explains: “With health apps, data protection and security must have the highest priority. The devices and software applications collect highly sensitive data that allow precise insights into personal life. For these reasons, it is essential that apps approved by the BfArM meet the highest security and data protection requirements. Users of health applications must be able to trust that their data will be protected effectively. That one of the first apps released has security flaws is disturbing. The responsible Federal Ministry of Health should therefore make improvements to the approval process.”

In the past, the State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate, together with the other data protection supervisory authorities, had repeatedly warned of deficits in the design of the statutory test procedure for including health apps in the DiGA directory. In particular, he criticized the fact that apps are only included in the directory on the basis of manufacturer information, without their data protection compatibility being checked by independent bodies. Eiermann says: "It is becoming clear that the approval process carried out by the BfArM is not suitable for ensuring the data protection conformity of the apps included in the DiGA directory."

From a technical point of view, the following points in particular should be taken into account when evaluating and including the health apps in the DiGA directory and checked as part of independent audits: the confidentiality and integrity of the communication (content and metadata), the security of the data stored on the end device or in Health information stored in the app, the technical service providers involved and the involvement of other bodies (e.g. for range measurement and app analysis). It is not enough to rely solely on manufacturer information.

return