Mobile health applications put millions of users' privacy and security at risk, researchers find

80% of the health apps evaluated in a European study transmitted health-related data to third-party companies, with only half doing so over secure (HTTPS) connections. Most of the apps did not meet legal requirements or standards meant to prevent users' inappropriate and uncontrolled data usage and disclosure to third-party companies.

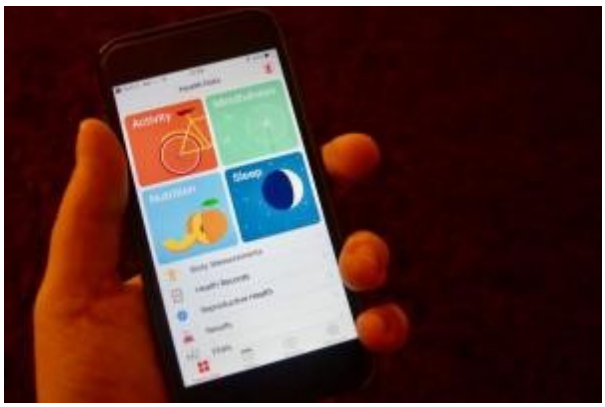

Photo: www.forthwithlife.co.uk

In this innovative study, researchers evaluated 20 popular, free mobile health apps available on Google Play, and looked at how app developers reacted to the findings.

With 100.000 to 10 million downloads each and a minimum rating of 3.5/5, the chosen apps managed, stored and monitored users' biomedical data such as health conditions, diseases or medical agendas.

In the first part of the study, researchers from the University of Pireus, Greece and Rovira I Virgili University, Spain analysed the way in which users' personal data were handled. Only 20% of the apps stored data on

users' smartphones, and one in two apps requested and managed users' login passwords without using a secure connection.

The team also stressed that half of the apps shared personal data – both text data and multimedia such as X-ray images - with third parties. What is more, over half of the apps transmitted users' health data through URL links, thus making data accessible to anyone with access to those links.

In 20% of the cases, the apps either did not refer users to a privacy policy, or the policy content was not available in English, the language of the app. Some apps required access to users' geolocation, microphones, camera, contacts list, external storage card or bluetooth, although the apps' proper functionality did not depend on it.

" *We strongly support the use of mobile health apps, but users must know that apps' popularity does not ensure privacy and security* ", said Dr Agusti Solanas of Rovira I Virgili University in Spain, involved in the study.

After informing app developers about their findings, researchers noticed some issues had been fixed – for instance, unsafe health data transfers or the possibility of identifying users because of unsafe data transfers to third parties. However, other issues, such as app usage data leaks, had not been addressed at all.

" *People need to become more aware of the risks they are facing* ", Dr Constantinos Patsakis of University of Piraeus added.

The study was run by a team of researchers part of COST-funded European network CRYPTACUS , whose aim is to come up with better solutions for European citizens' online privacy. The study was partly funded by EU-funded project OPERANDO .

IEEE paper link: http://ieeexplore.ieee.org/document/8272037/

Full PDF: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8272037

CRYPTACUS COST network: https://www.cryptacus.eu/en/

OPERANDO project: https://www.operando.eu