

Health checks by smartphone raise privacy fears

March 5 2015, by Septime Meunier



A visitor at the 2015 Mobile World Congress in Barcelona, where experts have warned of the dangers of sensitive health data on mobile phone ending up in the wrong hands

Authorities and tech developers must stop sensitive health data entered into applications on mobile phones ending up in the wrong hands, experts warn.

As wireless telecom companies gathered in Barcelona this week at the

Mobile World Congress, the sector's biggest trade fair, specialists in "e-health" said healthcare is fast shifting into the connected sphere.

"It's an inexorable tide that is causing worries because people are introducing their data into the system themselves, without necessarily reading all the terms and conditions," said Vincent Genet of consultancy Alcimed.

"In a few years, new technology will be able to monitor numerous essential physiological indicators by telephone and to send alerts to patients and the specialists who look after them."

More and more patients are using smartphone apps to monitor signs such as their blood sugar and pressure.

The European Commission estimates the market for mobile [health services](#) could exceed 17.5 billion euros (19 billion euros) from 2017.

The Chinese health ministry's deputy head of "digital health", Yan Jie Gao, said at the congress on Wednesday that the ministry planned to spend tens of billions of euros (dollars) by 2025 to equip 90,000 hospitals with the means for patients to contact them online securely.

Patients are entering health indicators and even using online health services for long-distance consultations with doctors whom they do not know.



Many smartphone users are entering sensitive personal health data into applications on their devices without being aware of the risks, experts say

"There is a steady increase in remote consultations with medical practitioners," particularly in the United States, said Kevin Curran, a computer scientist and senior member of the Institute of Electrical and Electronics Engineers.

"Your doctor can be someone who's based in Mumbai. We have to be very careful about our data, because they're the ones who probably will end up storing your data and keeping a record of it."

Cloud-based healthcare

Other users are entering [personal health data](#) into applications on their smartphones.

This kind of "e-health" could save governments money and improve life expectancy, but authorities and companies are looking to strengthen security measures to protect patients' data before such services become even more widespread.

"I think tech companies are becoming more concerned with privacy and encryption now," said Curran.

"The problem quite often is that a lot of this data is stored not on the phone or the app but in the cloud," in virtual storage space provided by web companies, he added.

"We are at the mercy of who the app providers are and how well they secure the information, and they are at the mercy sometimes of the cloud providers."

Others fear that insurance companies will get hold of customers' health information and could make them pay more for coverage according to their illnesses.

Various sources alleged to AFP that [health insurance companies](#) have been buying data from supermarkets about what food customers were buying, drawn from the sales records of their loyalty cards, following media reports to that effect.

The kind of "e-health" indicator most sought after by patients is fitness-related rather than information on illnesses, however, said Vincent Bonneau of the research group Idate.

A study by Citrix Mobile, a specialist in wireless security, showed that more than three quarters of people using e-[health](#) applications were doing so for fitness reasons rather than for diagnosing illnesses.

"No one really wants to have a hospital in their home," said Bonneau.

© 2015 AFP

Citation: Health checks by smartphone raise privacy fears (2015, March 5) retrieved 27 April 2024 from <https://phys.org/news/2015-03-health-smartphone-privacy.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--