HealthManagement.org
Promoting Management and Leadership

Study: mHealth Apps Have Poor Data Privacy Protection

According to researchers, mobile health applications accredited by the UK National Health Service do not adequately protect the privacy of users' personal health information. The accreditation process requires app vendors to uphold the principles of data protection embodied in the UK Data Protection Act. However, the apps examined by the researchers "exhibited substantial variation in compliance with data protection principles." Their study is published in *BMC Medicine*.

Although the study applies to a small subset of mHealth apps, combining the results of this research with other studies suggests the privacy problem is endemic to many other apps, Kit Huckvale, MB ChB, from the Global eHealth Unit, Imperial College London, United Kingdom, and lead author of the BMC paper, told *Medscape Medical News*.

Of 79 apps studied, Dr. Huckvale and colleagues found that 70 (89 percent) transmitted information to online services. No app encrypted personal information stored locally on mobile devices. Two thirds of the apps that sent personal identification information over the internet did not use encryption, and 20 percent of these apps did not have a privacy policy.

"Overall, 67 percent (53/79) of apps had some form of privacy policy. No app collected or transmitted information that a policy explicitly stated it would not; however, 78 percent (38/49) of information-transmitting apps with a policy did not describe the nature of personal information included in transmissions. Four apps sent both identifying and health information without encryption," the authors write.

The selected apps included programs designed for wellness, fitness, and chronic care management. Most collected user-generated content, and two thirds had users enter strong identifiers such as email addresses, usernames and passwords, or full names. The majority of the apps captured health-related data, and a third of them provided diaries to record health information.

"We found examples of complete personal datasets, including name, date of birth and contact details, sent as plain text. No apps encrypted local data stores, despite the widespread use of PIN or password security within apps that might reasonably lead a user to believe their information was protected," the authors note.

Dr. Huckvale said he is not aware of any large-scale thefts of mobile health data in the UK or the United States. However, with all the hacking going on in healthcare, "there's an opportunity to make sure this doesn't happen," he added.

"We're hopeful that this paper will stimulate discussion and lead to resolution of the issue, rather than people

going away from it and thinking that it can't be fixed. It definitely can be fixed. We have secure banking and things like that. We should try to sort it now before mHealth apps are more widely used," Dr. Huckvale concluded.

Source: Medscape Medical News
Image credit: Flickr.com

Published on : Fri, 2 Oct 2015