PHYS.ORG

Developers neglect privacy and security in health apps

March 13 2015

The main risk is that someone can hack into the personal medical information of another individual or, even worse, modify it. Credit: Intel Free Press

Telemedicine researchers at the University of Valladolid have proposed a series of recommendations to programmers to improve the security of health applications on mobile devices. According to these specialists, it is a rapidly growing area, but the insecure handling of clinical and medical data can be critical for users.

Health applications are enjoying a boom. There are already some 100,000 on the market on iOS (Apple) and Android platforms, generating 4.5 billion dollars' worth (around 3.3 billion euros) of business. In Spain, a third of smartphone users will have installed at least one health application this year, according to a report from The App Date.

However, as Borja Martínez, researcher in the Telemedicine and eHealth Group at the University of Valladolid, explains to SINC: "These applications do not handle information securely and this is especially serious in apps that use clinical or medical data that are particularly critical for the user".

Martínez is the lead author of a study that reviews these problems and proposes a series of recommendations for developers to improve the handling of information that should be confidential. The work was published in January in the 'Journal of Medical Systems'.

This young engineer points out that "the developers, in their haste to get their applications out before the rest, neglect certain aspects that should be considered, especially privacy and security of data handled. Today the majority of health apps do not offer the user sufficient measures to protect their data".

Risks

In their opinion, "the main risk is that someone can hack into the personal medical information of another individual or, even worse, modify it".

A clear example, warns the researcher, "would be an app that saves electronic medical histories. If a third party unconnected with the app were to access the stored information and change any patient details, such as take away an allergy to certain medication, it could put the life of this person at risk should the case arise".

Also, "another significant problem is that health professionals and the patients themselves are not aware of the methods that apps use with regard to the privacy and security of their data. Many take it for granted that the application is secure and others couldn't care less. I believe that greater collaboration between countries is necessary to create international laws which are in charge of monitoring these aspects," he says.

What can be done? According to Borja Martínez, "many things [although] it all boils down to developers analysing the type of data that their apps are going to be dealing with and applying the necessary security and privacy methods".

Each case is different, he states. "Some applications do not even deal with patient data and therefore it is not necessary to introduce such methods, others will use critical information and designers will have to decide which mechanisms to use. The main thing is that they do not disregard these aspects and that they concern themselves with investing part of the development time in analysing and implementing these techniques".

Borja Martínez says that "to oblige developers to carry out this task, it is necessary to update laws which govern these aspects. Yet in two of the main world powers, the European Union and the United States, these laws are outdated and obsolete, and therefore should be reformulated to cover current mobile technology".

In this sense, the EU Data Protection Directive dates back to 1995 and the HIPAA (Health Insurance Portability and Accountability Act) in the US is from1996.

Quick guide to e-health security

In their guide for health app developers, Martínez and his colleagues propose the following recommendations, among others:

- Access control: centred on the patient, always allowing them the possibility of accessing or prohibiting access to their information.
- Authentication: with a unique identity and a password known only to the user. This identity can be linked to a public infrastructure, such as RSA (River, Shamir and Adleman).
- Security and confidentiality: the use of AES (Advanced Encryption Standard) with a cryptographic key of at least 128 bits is recommended to ensure security.
- Integrity: at least one authentication code should be used based on a symmetric key, such as AES.
- Patient information: before gathering any information, the apps must present users with a clear privacy policy to identify the person who will use the data, their purpose, the privacy methods used, their rights and a means of contact.
- Data transfer: use TLS (Transport Layer Security) with encryption methods of 128 bits or virtual private networks.
- Data retention: data must only be stored for the necessary amount of time for the established purpose, no longer.
- Communication with body sensors: for communication with low-power sensors used in the body, cryptographic methods must be used for the authentication of devices and the distribution of the key.
- Alert for security lapses: the developing company must alert the competent authorities as well as users as soon as possible and must help the user to reduce the possible damage caused by such breach.

More information: Borja Martínez Pérez, Isabel de la Torre-Díez y

Miguel López-Coronado. "Privacy and Security in Mobile Health Apps: A Review and Recommendations". *Journal of Medical Systems*. DOI: 10.1007/s10916-014-0181-3

Provided by Plataforma SINC

Citation: Developers neglect privacy and security in health apps (2015, March 13) retrieved 24 April 2024 from https://phys.org/news/2015-03-neglect-privacy-health-apps.html