Greater privacy and security measures needed to protect patient info in mobile health tech

July 13 2016

With over two-thirds of U.S. adults owning a smartphone, and the rise in miniaturized sensors and low-power body area networks that are used for remote health monitoring, mobile health (mHealth) is beginning to experience a boom. While the technology has the potential to increase healthcare quality, expand access to services, reduce costs, and improve personal wellness and public health, such benefits may not be fully realized unless greater privacy and security measures are implemented, according to a new paper published in the June issue of *Computer*.

To maintain the confidentiality of patient records, healthcare providers implement their own security measures; yet, consumers may not have access to such systems for their home-based devices. To ensure that protected health information (PHI) remains confidential and secure through mHealth technologies, the authors pose a series of research challenges in the areas of: data sharing and consent management; access control and authentication; confidentiality and anonymity; mHealth smartphone apps; policies and compliance; accuracy and data provenance; and security technology.

Many mHealth systems have the ability to continuously collect and transmit individual health data - but to what end? Among the challenges, researchers highlight the need for mHealth systems to provide users with the opportunity to specify how their PHI will be used, to prevent mHealth systems from collecting information that extends beyond the clinical setting. To verify that a personal device reporting health-related information is in fact being used by the rightful owner, access control and continuous authentication measures, such as building biometric sensors into a device, are also needed. In mHealth, GPS can be used to collect information about geo-exposures, movement patterns and other data about users; however, even when GPS is turned off, there's a risk that remote sensor data could disclose an individual's location and other private information. Anonymizing data would help mitigate this risk.

"We encourage colleagues with research expertise in mobile health, medical devices, and secure computing to engage with these issues and help bring pervasive mobile-health technology to the world," said lead author David Kotz, the Champion International Professor in the Department of Computer Science at Dartmouth College.

With 45 percent of Americans facing chronic disease, which accounts for 75 percent of the annual $2.6+ trillion spent on healthcare, and many developed countries facing aging populations, mobile technology can serve as a great resource to help address these problems provided mHealth companies and other stakeholders are able to meet the privacy and security challenges associated with these technologies. This new paper outlines the most critical research challenges required to achieve those goals.

More information: David Kotz et al. Privacy and Security in Mobile Health: A Research Agenda, *Computer* (2016). DOI: 10.1109/MC.2016.185

Provided by Dartmouth College

Citation: Greater privacy and security measures needed to protect patient info in mobile health tech (2016, July 13) retrieved 23 May 2024 from https://phys.org/news/2016-07-greater-privacy-patient-info-mobile.html