HealthManagement.org
Promoting Management and Leadership

Study Shows Security Risks of mHealth

Continuous improvement in mobile technology has led to more widespread use of personal health wearable devices used to monitor heart rates, sleep patterns, calories, and even stress levels. However, researchers from American University and Center for Digital Democracy claim that a lack of regulation enables unchecked use of personal health information collected by wearables, such as watches and fitness bands that are linked to apps and mobile devices.

Their study showed that the weak and fragmented health-privacy regulatory system fails to provide adequate federal laws to ensure that personal and health data of wearable users are protected. The findings are described in a report titled "Health Wearable Devices in the Big Data Era: Ensuring Privacy, Security, and Consumer Protection".

The report provides an overview and analysis of the major features, key players, and trends that are shaping the new consumer-wearable and connected-health marketplace. "Many of these devices are already being integrated into a growing Big Data digital health and marketing ecosystem, which is focused on gathering and monetising personal and health data in order to influence consumer behaviour," the report explains.

See Also: **How Secure is the Healthcare Cloud?**

Moreover, as the functionalities of wearable devices become more sophisticated, "the extent and nature of data collection will be unprecedented," the report notes. For example, a new set of techniques and Big-Data practices are being developed to harness the unique capabilities of wearables – such as biosensors that track bodily functions, and "haptic technology" that enables users to "feel" actual body sensations. Pharmaceutical companies are poised to be among the major beneficiaries of wearable marketing.

The report offers suggestions for how government, industry, nonprofit organisations, academic institutions and other stakeholders can work together to develop a comprehensive approach to health privacy and consumer protection in the era of Big Data and the Internet of Things. These include:

- Clear, enforceable standards for both the collection and use of information
- Formal processes for assessing the benefits and risks of data use
- Stronger regulation of direct-to-consumer marketing by pharmaceutical companies

"The connected-health system is still in an early, fluid stage of development," says Kathryn C. Montgomery, Professor of Communication with American University, and a co-author of the report. "There is an urgent need to build meaningful, effective, and enforceable safeguards into its foundation."

Such efforts "will require moving beyond the traditional focus on protecting individual privacy, and extending safeguards to cover a range of broader societal goals, such as ensuring fairness, preventing discrimination, and promoting equity," according to the report.

Source: American University
Image Credit: LinkedIn

Published on : Tue, 27 Dec 2016