Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Wearable Health Industry Has To Be Proactive On Privacy

Karen Bromberg

Law360, New York (October 08, 2014, 10:26 AM ET) -- It is universally accepted that good health is the key to enjoying our lives. And now technology is at the forefront of helping us understand, track and improve our health, not only for those who are young and obsessed with fitness, but also for people who are fighting illness, and even for seniors who want to live independently as long as possible.

The two original pieces of "body real estate" — parts of the body that could be outfitted with tracking functions — were the head and wrist. But now wearable shirts (or smartwear) that take biometric devices to a new level have been added to the mix, along with jewelry, earbuds, belts, leg wear, arm wear, footwear, and even tattoos and skin patches. From devices that measure glucose levels, blood pressure and sleep patterns, to a smart bra that could one day supplant the mammogram and a chip that can be swallowed with medication or embedded in a diseased organ to send biometric readings back to a healthcare professional via a Wi-Fi patch, wearable technology is likely to revolutionize the way we care for ourselves.

But the collection of medical information from wearable technology poses new risks. Health data from smartwear is generally transferred to a smartphone app or to the cloud through a wireless connection and then stored electronically, leaving it vulnerable to attack. Given the highly personal nature of health data — and the recent high-profile security breaches at Home Depot Inc., Target Corp. and other companies — consumer acceptance of wearables is likely to depend on user confidence that rigorous steps are being taken to protect their privacy and data security.

Of course, health data sent to a doctor, hospital, outpatient care center or other health care provider (i.e, with a "covered entity") constitutes protected health information under the Health Insurance Portability and Accountability Act of 1996 and is subject to HIPAA privacy and data security rules. But at the moment the vast bulk of wearable health data is tracked and stored outside of these covered entities and is therefore not subject to HIPAA protections. Accordingly, consumers, developers, businesses and manufacturers are in uncharted waters.

As a preliminary matter, consumers need to take responsibility for the protection of their data. Before purchasing any wearable technology, consumers should find out how health data will be collected, stored and shared. This means that consumers should review the provider's privacy policy and if not satisfied, ask questions to allay any concerns or choose a different provider.

Just as important, companies hoping to capitalize on the wearables boom could and should integrate privacy into the design of their products and proactively lay consumers' privacy concerns to rest. To engender confidence, at least until there is more than a patchwork of laws governing this area, the wearable tech industry should develop and adhere to industry guidelines to protect personal health information and guard against security breaches.

If companies are going to collect and use health data from consumers, they need to institute strong protections for this sensitive data. There are at least five main things that companies in the wearables health industry should consider including in their privacy and data security guidelines, working in tandem with counsel:

1. Adopt an "opt-in" policy that prohibits the sharing of health information with advertising platforms, data brokers, information resellers and/or any other third parties. By the same token, companies should expressly prohibit their developers from selling or otherwise sharing an end user's personal data collected through APIs to any third parties.

2. Adhere to a "privacy by design" policy. Privacy should be part of a comprehensive business technology approach at the inception of development and design and at every stage thereafter, and not just tacked on as an afterthought.

3. Be highly transparent about your data use policies. Adopt and enforce an easy to read privacy policy that clearly conveys how the consumer's information is being collected, used, stored and shared.

4. Adopt data minimization and destruction policies under which companies will collect only the information that is needed for a legitimate business purpose. This means limiting and restricting the overall data collection to core functions, and, by the same token, limiting the overall retention of any personal health data collected.

5. Have in place a strong security policy (with physical, administrative and technical safeguards), written policies and procedures to assure security compliance and documentation of security measures. The policy should require encryption technology with respect to any health care data, and bi-annual privacy and security compliance assessments.

Equally important is an incident response plan to guide the company's response to any security breach. The primary objective of such a plan is to manage the security incident in a way that limits damages, reduces recovery time and costs, and increases the confidence of consumers. An effective incident response plan will identify first responders, overall chain of command, and contain a playbook for containment, eradication, and recovery, as well as guidelines for documenting the response in governance, risk, and compliance applications. Security breaches are inevitable but being prepared for one is mission critical to engendering consumer confidence and limiting potential exposure of personal information.

By taking a proactive approach to privacy and data security, companies can reassure consumers and enhance the growth prospects of the entire wearables sector, particularly in the wearable health sector where so much more is at stake. It's not just good policy — it's good business.

—By Karen Bromberg, Cohen & Gresser LLP

Karen Bromberg is a partner in Cohen & Gresser's New York office and head of the firm's intellectual property and technology.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.