Wearable Medical Devices Give Abundant Data—and Risks

Miranda Felde, MHA, CPHRM, Vice President, Patient Safety and Risk Management

Since 2013, the number of US consumers tracking their health data with wearables has doubled. And that number continues to rise: During the third quarter of 2018, the wearables market saw a nearly 60 percent increase in earnings over the prior year.

Wearables are electronic devices worn on the body, often like a watch. Wearables can track patient data like heart rate, blood pressure, or blood glucose. They can also track activity level, e.g., counting steps.

Promoters of wearables believe wearables will drive the transition to intelligent care, whereby physicians have access to more data—in which they can identify actionable components. Florence Comite, MD, a New York endocrinologist who describes wearables as “almost like magic,” uses data from wearables to tailor her interventions for patients with chronic conditions.

Wearables can help patients take action, too. In one recent study, diabetes patients using a wearable app showed randomized controlled trial results comparable or superior to patients taking diabetes medications.

Though each device has its pros and cons, all wearables generate concerns for physicians, including:

- **Poor data quality**: Data from wearables may or may not be reliable enough for medical use.
- **Data fixation**: Patients may fixate on one number—steps per day, for instance—at the expense of other health variables, such as their diet, sleep habits, etc.
- **Lack of interoperability with electronic health records (EHRs)**: If a patient’s wearable cannot stream data to the patient’s EHR, then how can the physician’s practice securely acquire the data?
- **Data saturation**: Physicians receiving patient data from wearables risk being soaked by a data fire hose. Physicians need a plan and a process to determine what measurements are relevant to a given patient.
- **Unclear physician responsibilities for collecting, monitoring, and protecting data**: HIPAA applies to patient data collected by physicians, but differing state laws mean that a physician’s specific responsibilities for monitoring and protecting patient data vary by location.
- **Lack of data security—and liability for physicians**: Wearables are subject to cyberattack. In addition to presenting obvious risks to patient safety, this may also present liability risks to physicians—who may be expected to notify patients of recalls issued for their wearables.

---


7 Ibid.