



# Mobile Health (mHealth) Technology: Promoting Improved Provider-Patient Communication

☎ 888-980-6860

🌐 [www.ringrx.com](http://www.ringrx.com)

✉ [info@ringrx.com](mailto:info@ringrx.com)

📍 114 E Haley St, Ste L, Santa Barbara, CA 93101

# Mobile Health (mHealth) Technology: Promoting Improved Provider-Patient Communication

A lot has changed in the United States since the emergence of smartphone technology. When the iPhone was introduced in 2007, Amazon Prime was in its infancy, Facebook had recently gone global, and Twitter was new to the scene. Prices were [1.31 times lower](#), and healthcare spending reached a mere \$2.2 trillion, nearly half the amount expended in recent years.

Although the first smartphone, the Simon Personal Communicator, was invented in 1992 and released for purchase in 1994, the widespread use of mobile technology wasn't as prevalent. Approximately [three billion people worldwide](#) now use smartphones, and more than [500 million people globally](#) are believed to have downloaded one or more mHealth apps to their mobile phone.

mHealth refers to mobile health, which the World Health Organization (WHO) [defines](#) as the delivery of healthcare services via mobile communication devices. Four primary [functions of mHealth](#) are the support of clinical diagnoses and decisions, the education of patients on disease and treatment options, a function as a self-contained digital therapeutic, and the improvement of outcomes by supporting behavioral changes and compliance with established treatments.

**According to the National Center for Biotechnology Information (NCBI), there are four categories of mHealth:**

- **Physiological monitoring:** measuring, recording, and reporting physiological parameters such as heart rate and blood pressure
- **Activity and behavior monitoring:** measuring, recording, and reporting movement and physical and social activity, as well as health-related behaviors such as eating and addictive behaviors
- **Information access:** accessing health-related data (i.e., medical records, activity, or behavior data) and decision-support tools
- **Telemedicine:** communication between patients, caregivers, and/or providers



# An Overview of mHealth

**mHealth** is a rapidly growing area of healthcare technology. The [mHealth market](#) is forecast to grow to \$805.3 billion by 2030. Over [one million health and well-being apps](#) are available from the Apple and Google app stores, and almost [90 percent of smartphone users](#) in the U.S. used health and fitness apps in 2020.

From wearable devices and access to electronic health records (EHRs), to chronic disease control and online or remote consultations, mHealth offers multiple uses for both healthcare providers and patients. During the height of the COVID-19 pandemic, many individuals utilized mHealth for virtual health, which enables technology to deliver health services in a way that is independent of time or location.

Some of the most [common types of mHealth apps](#) include those for diabetes, pregnancy, weight loss, and documentation of chronic illness symptoms. Many patients utilize mHealth to schedule doctor's appointments; access their medical records in real-time, and view test results and post-visit instructions.

mHealth technology enables physicians to digitize their workflow, access patient data in real-time, and document at the point-of-care. A [survey](#) conducted by Stanford Medicine found that 83 percent of physicians and 79 percent of students and residents see value in self-reported data from patients using wearables. Other [research](#) notes that more than 90 percent of doctors believe mHealth apps can improve a patient's health, and approximately [70 percent of physicians](#) use their mobile device to manage patient data.





# A Convenient and Cost- Effective Technology Tool

By helping patients take control of their own health and enhancing their communication with their providers, mHealth is a powerful tool for improving health outcomes. It aids providers in achieving the Quadruple Aim, which consists of improving patient experience, improving population health; decreasing cost of care and achieving joy, well-being and resilience among care teams.

For residents living in rural areas of the U.S., mHealth provides a cost-effective and convenient method for improving access to care and [promoting continuity of care](#) through real-time communication, responsive concern, and reduced admissions. It also has the potential to improve access to care for underserved populations by addressing social determinants of health (SDOH). Many mHealth apps are either free to download or available at a minimal cost.

mHealth benefits the healthcare industry by:



Allowing patients and their physicians to maintain consistent contact through virtual consultations, rather than relying on in-person appointments



Reducing human error through electronic record-keeping and real-time data collection



Providing care for elderly patients who need constant support due to chronic conditions and patients who cannot easily leave their homes



Allowing patients to track and monitor their own medical conditions and be proactive about potential treatments



Helping patients access essential health information quickly, which can minimize extra costs such as for unnecessary hospital visits



Reducing the spread of disease and infection by conducting virtual appointments



Tracking symptoms in real-time for quick diagnoses and expert feedback



Decreasing hospital costs by cutting down on paper usage and waste



Personalizing health data and treatment programs for each patient



Providing reminders to patients to take their medicine, check their vitals or record their symptoms that don't require the intervention of their physician or caretaker



# Principles for Secure Use of MHealth Applications

As with many other technologies employed in the healthcare industry, there are challenges to realizing the full benefits of mHealth solutions. One is a lack of regulation. Although the U.S. Food and Drug Administration (FDA) in 2020 [launched the Digital Health Center of Excellence](#), which is aimed at supporting mHealth and telehealth tools, the agency only regulates apps it defines as a medical device and those which potentially pose a risk to patient safety.

Another perceived issue with mHealth technology is concerns about privacy and security, especially as providers and other healthcare entities are tasked with handling protected health information (PHI). Those that create, receive, or transmit PHI are required to comply with the [Security Rule of HIPAA](#) and its administrative, physical and technical safeguards or risk costly civil and/or criminal penalties.

Although it can be difficult for providers to protect sensitive health data, the [American Medical Association](#) (AMA) physician membership approved the following list of principles on the safe and effective use of mHealth applications and other digital health devices, including trackers and sensors:

- Support the establishment or continuation of a valid patient-physician relationship.
- Have a clinical evidence base to support their use in order to ensure mHealth app safety and effectiveness.
- Follow evidence-based practice guidelines, to the degree they are available, to ensure patient safety, quality of care, and positive health outcomes.
- Support care delivery that is patient-centered, promotes care coordination, and facilitates team-based communication.
- Support data portability and interoperability in order to promote care coordination through medical home and accountable care models.
- Abide by state licensure laws and state medical practice laws and requirements in the state in which the patient receives services facilitated by the app.
- Require that physicians and other health practitioners delivering services through the app be licensed in the state where the patient receives services, or be providing these services as otherwise authorized by that state's medical board.
- Ensure that the delivery of any services via the app is consistent with state scope of practice laws.

# An mHealth Action Plan for Providers

Healthcare provider organizations of all sizes can mitigate the privacy and security risks of mHealth by taking some simple actions. The first is to ensure cyber-security processes, policies, and procedures are up-to-date. Once a plan is developed for dealing with a cyberattack if it occurs, it should be tested routinely.

Another recommendation is to conduct a comprehensive risk analysis, which helps reveal areas where PHI could be at risk. The Office of the National Coordinator for Health Information Technology (ONC) offers a downloadable [Security Risk Assessment \(SRA\) Tool](#) designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) EHR Incentive Program.

To further lessen any privacy and security risks through mHealth, it's essential to encrypt data to prevent unauthorized breaches wherever data is stored. All data should be stored in highly secured and protected cloud-based servers.

Healthcare providers should conduct a thorough evaluation of their practice operations to ensure they remain in compliance for data security, privacy, and reporting of breaches. For physician practices, office managers and practitioners should be thoughtful in how they integrate mHealth technology while addressing issues such as:



**Clinical decision support:**  
**Evaluating and selecting the best apps to support clinical decisions**



**Workflow efficiencies:** Using simpler, better, and HIPAA compliant mobile-enabled devices, services, and software to optimize data retrieval, documentation, and healthcare transactions



**Communication and coordination:** Appropriately connecting and sharing secured information among providers to better coordinate care



**Patient engagement:** Supporting population health, improving compliance, and engaging patients in their care