Mobile Technology in Human Research
By Joseph E. Andrews and J. Brian Moore

Background
Over the past few years, the proliferation of smartphones has led to the latest revolution in healthcare: mobile health or mHealth.¹ The popularity of mobile technology and the processing power of the latest wireless devices make their use in healthcare an attractive solution for both clinicians and patients. Having a device that can record information about a patient in real time during daily life conditions can be clinically useful and convenient. Devices that can monitor health status, provide alerts, calculate appropriate medication doses, and send information back to clinicians for review are a huge step forward in managing chronic conditions.² This article will discuss some important points to consider when testing or utilizing mobile technology in clinical trials.

Regulatory Environment
The field of mHealth devices is broad, encompassing not only smart phones, but also tablets, wearable devices for drug delivery, mechanisms that measure activity, heart rhythms, or other vital signs, and new technology that will utilize watches and “contact lenses.”³ Health-related mobile technologies may or may not be considered medical devices.⁴ According to Food and Drug Administration (FDA) guidance, the intended use of an application or technology is the determining factor in whether it meets the definition of a medical device.³ The definition of a medical device put forth by the FDA is:

An instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is:
- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its purposes.⁴

As of March 2013, over 97,000 mHealth software applications were available to consumers.⁵ Depending on the claims made as to the proper use of the technology, many of these products do not need FDA review or approval. Most of these applications are low risk, but the serious impact of errors and the large numbers of users who could be affected has led to discussions of regulatory focus in the area of mHealth.⁶ Development errors generating false readings, such as those affecting the Pfizer Rheumatology Calculator, which inaccurately measured the severity of joint symptoms, could have severe effects on medication delivery applications.⁷ Such cases demonstrate the need for mHealth applications meeting the definition of a medical device be properly tested in accordance with regulatory requirements.

The Patient-Centered Outcomes Research Institute (PCORI) is using mHealth as a source for data from a large and diverse cohort of participants.⁸ The data collected by PCORI through mHealth technology will help determine if mHealth is a viable alternative to traditional clinic-
based management approaches for certain conditions. The work of PCORI and others examining the potential of mHealth is important to fully understand the risks and benefits of mHealth, so that serious problems can be anticipated and prevented.

The 2013 FDA Mobile Medical Devices: Guidance for Industry and FDA Staff lists several areas of particular focus in its enforcement efforts:

- Mobile apps that are an extension of one or more medical devices by connecting to such device(s) for purposes of controlling the device(s) or displaying, storing, analyzing or transmitting patient-specific medical device data.
- Mobile apps that transform the mobile platform into a regulated medical device by using attachments, display screens, or sensors, or by including functionalities similar to those of currently regulated medical devices. Mobile apps that use attachments, display screens, sensors or other such similar components to transform a mobile platform into a regulated medical device are required to comply with the device classification associated with the transformed platform.
- Mobile apps that become a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis or treatment recommendations. These types of mobile medical apps are similar to or perform the same function as those types of software devices that have been previously cleared or approved.

A regulated medical “device” does not need to be a physical mechanism; it could also be a software application that just resides on a smartphone or other device, a computer, or in the cloud.

The guidance indicates that the FDA may exercise enforcement discretion with respect to other types of mHealth applications, such as those that provide only coaching, reminders or tools to organize and track health information.

In addition to the FDA, other regulatory oversight bodies are involved in the governance of mHealth technology in the United States. The Federal Trade Commission (FTC) regulates deceptive trade practices and health data breaches when the holder of the data is not a covered entity under the Health Insurance Portability and Accountability Act (HIPAA). Recent comments by the FTC Chairwoman indicate that concerns over “data sensitivity” are focusing the FTC's attention on mobile technology. The Federal Communications Commission (FCC), which oversees the use of wireless connectivity, is working with other governmental agencies and private enterprise to examine its rules to better address and accommodate mHealth technologies. Finally, the collection, storage and transmission of Protected Health Information (PHI) is regulated by the Department of Health and Human Services Office of Civil Rights under HIPAA.

**Considerations for Investigators and IRBs**

Investigators and IRBs should consider how each of these four federal regulatory oversight bodies are involved with the product being used in a research study. In addition, each state might have local laws that affect the ways in which mHealth technology can be implemented or how data can be handled.

Below are considerations that investigators and study teams should explore when designing or reviewing clinical trials involving mHealth technology:

- Does the product meet the FDA definition of a medical device?
- If the product is a medical device, does it require an investigational device exemption (IDE)?
• Does the device collect data that meets the definition of personal health information (PHI)?
• If PHI is collected, how is it stored on the device and then transmitted wirelessly or through a computer or landline to a central database?
• If PHI is transmitted or stored by the device, what security measures ensure compliance with the HIPAA security rule (e.g., password, encryption)? Even if the data is not considered PHI under HIPAA, will it be encrypted so that if it is accessed from the device or intercepted during transmission (e.g. by a rogue WIFI hotspot), it cannot be read?
• If the clinical trial involves an FDA-regulated product, what will be the “source document” for data captured by the mobile technology?
• How will the data received from the device be authenticated? In other words, how will investigators be certain that the data actually measured the study participant? (The issue of authentication is related to how the study team will define “source document,” but it is particularly important if the device is being used in research subject to 21 CFR Part 11.30, which requires that “Persons who use open systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt.”)
• Will the device have a lock-out feature that takes effect if someone other than the participant enters an incorrect password or other information that might indicate unauthorized use? Can the data be wiped remotely if the device is lost or stolen?
• If the mechanism is an application on a smartphone, can other applications or settings outside the mHealth app affect the security of the data? For example: Could the data be backed up in the cloud with other stored information? Could the information be accidently emailed or otherwise compromised by use of the phone for non-study purposes? Could other users of the phone access and read the information if, for example, the phone were lent to a friend?
• Does the device receive information that it passes to the study participant (e.g., alerts, reminders or suggestions)? If so, how is the information received and protected? Will the message pop up on the phone so that others around might see it? What information will the messages contain? If the communication is via text messaging or through a service that stores a history, will that data automatically be cleared?
• Do participants use a device provided by the study team for study-related activities only or will the technology reside on a participant’s personal device? How will this decision affect the security of the data?
• Even if not regulated by the FDA, the protocol should address whether an audit trail will ensure that the data has not been accidentally changed or deleted.
• What is the potential impact of radio-frequency interference (RFI) on the device, especially if the function of the device is to influence or to directly deliver a therapeutic effect, rather than to provide observational data?
• How and when will the data on the mobile device be destroyed after the study?
• Is the use of the technology adequately accessible to all qualified participants so that no selection bias or inequity in enrollment is created? In other words, what steps will be taken to ensure that people without smart phones or Internet connectivity are not excluded just because of their economic status? Will there be extra costs for text messaging or a data plan that would exclude certain individuals from participating?
If there is uncertainty as to the status of the product under the regulations, investigators and IRBs should consult with the FDA or other governmental agencies. In addition, unless the IRB has up-to-date knowledge of mobile technology, it should ask an information technology expert to review the data protection plan.

The use of mobile technology in healthcare research holds great potential for the advancement of medicine. However, it also carries risks, especially in connection with secure data collection, storage and transmission. Due consideration of the above questions during protocol development and IRB review will minimize risks to study participants and the risk of regulatory missteps.

Acknowledgment

The authors would like to acknowledge the contributions of Melissa Markey, Esq., to the information contained herein.

References


Authors

Joseph E. Andrews, PhD, CIP, is Director of the Human Research Protection Program and Institutional Review Board at Wake Forest School of Medicine. Contact him at 1.336.716.4542 or jandrews@wakehealth.edu.

J. Brian Moore, MS, is Associate Director of the Human Research Protection Program and Institutional Review Board at Wake Forest School of Medicine. Contact him at 1.336.716.4542 or jbmoore@wakehealth.edu.