Mobile App Reviewer Guidance/Checklist

Purpose

This guide is intended to provide background on mobile apps for healthcare and raise questions which should be considered in reviewing such apps. This is not designed to provide guidance for comprehensive analysis of all technology in this space. The questions should be used to start a conversation and prompt additional discussion. Many of the questions raised here relate to general good practice in software development and deployment and are not specific to *only* medical apps or apps for clinical trials.

Definitions

Term	*Meaning*
MMA (Mobile Medical App)	The entire Mobile Medical Application system, including all of the following: mobile device, app installed on device, associated data portals, and any associated hardware.
Device App	The App that is running on the client device (usually a phone or tablet). Either preinstalled, or downloaded from app store.
Participant	Person/Patient using the app/participating in the study.
Native MMA	An app that comes on a device (Apple Health, etc).
Downloadable MMA	An app is developed by third parties and may be commercially available to be downloaded to a device.
Wearables	Electronic devices worn by the participant which track participant data such as activity or heart rate.

Types of Mobile Apps

In most cases, a mobile app is not something that lives by itself. It connects to a server or set of infrastructure to authenticate a patient/person, store data, transmit/receive notifications and share data with researchers or physicians. Additionally, there are mobile apps which connect to third party services or devices to collect data, display, and then transmit back. The complexities of these interactions require us to look at these samples separately. Below are some definitions of components within common paradigms for MMA.

To be explicit – it is likely that a specific MMA (mobile medical app) system is made up of some or all of the components listed below.

Type	*Description*	*Example*
Standalone App	An app that runs on a smartphone and does not send or receive data from any other systems.	BMI Calculator
Aggregator App	An app that retrieves data from multiple external services (e.g. FitBit, Patient Portal, etc) and correlates or visualizes that data alongside other healthcare data.	Exercise tracking apps that connect to wearables.
Companion App	An app that is used to run/drive a physical device which is attached to the mobile device.	An app to view the output of a smartphone connected otoscope.
Connected App	An app which stores data on a server, including patient data, and authentication credentials for that patient.	
App Portal	Typically the desktop computer (web based) facing view of the data which is stored on a server in the case of a connected app. Used by patients and providers/researchers to view the data which has been collected.	

General Considerations for MMA

The FDA offers guidance and information on mobile apps as they relate to health and medicine. The FDA defines these healthcare related apps as mobile medical apps (MMA). These MMAs are “medical devices” and *may* be regulated by FDA because of risk considerations however more likely fall under FDA enforcement discretion.

High risk MMA examples (significant risk)

- *A mobile medical app that controls the delivery of insulin through an insulin pump.*
- *An app that displays live data from a patient bedside monitor.*
- *A blood pressure app that transmits data to a treating physician.*

Low risk MMA example (non-significant risk)

- *Apps for collecting PROs (patient reported outcomes) through surveys.*
- *Apps for recording patient diet and exercise habits.*

Whether or not a MMA is FDA regulated or approved not should not be the primary factor in considering its use in research. The questions here will help guide a decision regarding the risks of using a specific MMA in research, whether or not it is one which is under the regulation of the FDA.

Specific FDA Guidance on MMA

FDA Regulated Mobile Medical Apps:

- MMA that controls other devices
- MMA that displays, store, analyze, or transmit patient-specific medical data from another device
- MMA that uses attachments, display screen, or sensors to transform the mobile platform into a medical device
- MMA that performs patient-specific analysis and provides a patient-specific diagnosis or treatment recommendation

FDA Exercises Enforcement Discretion

- MMA that provides or facilitates supplemental care by coaching or prompting patients
- Tools to help patients organize or track health information
- MMA that provides access to information related to health conditions or treatments
- MMA that allows patients to communicate medical conditions with providers
- MMA that performs simple calculations used in clinical practice
- MMA that enables individuals to interact with electronic health records

Non-FDA Regulated Medical Apps

- Electronic copies of medical textbooks, teaching aids, or other reference materials
- MMA intended as educational tools for medical training
- MMA to facilitate patient access or understanding
- MMA that automates general office operations
- Any app not specifically designed or intended for medical purposes

General Questions	Question Details/Background	Comments
What does the MMA do?		
Is the research solely about the MMA? Or is the MMA a required tool in collecting data for research?		
Is there data in the protocol supporting the accuracy of the MMA and the claims made about how the app is supposed to work?		
Does the MMA only capture data that is required for the research or is there also incidental data collected?	*Often times meta-data such as timestamps, location stamps, and more are also stored with the data.*	
Is the MMA a commercial product, or developed for this research?		
Are there any costs to use the MMA?		
Are there any costs to the study participant beyond their existing monthly service contract?	*Increased cell phone bill from data use, extra fees from using with internet, etc.*	
Will a mobile device (phone/tablet) be provided to participants? If so, is there a process for device return/replacement/theft?	*A clear process should be created to handle stolen, lost, and broken devices. This process should address how participants will be billed, and critically – how data will be kept secure. The process should include details on how it is initiated.*	
Are there penalties for not complying with the research?	*Concern - Participants enrolling only to get a tablet/phone for personal use.*	
How can participants withdraw from the research?		
Is the study open to anyone via online consent – or only selected/invited participants?		
Are accessibility standards considered?	*Captions on videos, text size adjustments, etc.*	

Technology Questions	Details	Comments
Does the MMA include a participant facing or provider facing portal?		
Does the MMA store credentials to other third party data providers? How are they stored, and who has access to them?	*Some MMAs might rely on connecting to third party systems and retain the participant credentials for those systems. Example - the participant's FitBit login credentials.*	
Does the MMA require participants to register or create an account? Does it support or rely on Facebook/Google or other system to log in?	*Concern - How are forgotten passwords, account resets are handled? Are login credentials assigned by the study coordinator?*	
Does the MMA require that the participant agree to any other third party terms, or register with third party systems?	*Example – they might need to register with fitbit and agree to those terms of use/service.*	
Are the types of devices on which the Device App will be supported clearly identified (iOS, Android, etc.)?		
If the research needs to stop for any reason, can the MMA use be suspended remotely?	*Can it be suspended for just a subset of participants (or a single one)?*	
How will devices updates be handled?	*For example, new versions of iOS pushed by Apple might be incompatible with the Device App.*	
General Risk Description Questions	Details	Comments
Are potential physical, psychological, social, legal, economic, and other risks described?		
Are all data elements collected clearly defined?		
Is the collected and stored data identifiable or de-identified?		
Is Breach of Confidentiality addressed (describe the possible breach considering the identifiability and sensitivity of the data)?		
How are risks of third parties intercepting research and non-research data addressed?	*Third parties include: developers of research app, other installed apps, other users of the device, and any parties not involved in the research.*	

Are data usage plan expenses described? (Applicable only if patient using their own device.)	*Ideally - give the participant an estimate of GB of usage they can expect against their quote with expected app behavior.*	
Data Security Controls and Confidentiality Questions	Details	Comments
Where is data stored throughout the lifecycle, from collection on device to storage for investigators?	*Is data stored on the device, server/portal, cloud? Are agreements are in place for data security and PHI privacy for server and cloud storage?*	
Is data stored on the device encrypted?		
Is data stored elsewhere (cloud) encrypted?		
Is data encrypted in transit?	*If data is transmitted from the device to a server, is it encrypted while it is being sent.*	
Is there a research code number (or other form of coded ID) on the phone/device to protect participant's identity?		
Does the device app support password, pin or other lock for access?	*If multiple people share a device, or if the device does not have a screen lock, the app could have its own lock.*	
Terms of Agreement and Consent Questions	Details	Comments
Are the license and terms of use for the MMA clearly disclosed?		
Do the terms of agreement clearly define what data will be shared with researchers and third parties?		
Will usage or other data from the device be shared with third parties?	*Usage information and analytics are often collected by apps for various purposes, this often includes geo-location information, browsing history, lists of app installed, and other data from the device.*	
How does the architecture prevent interception of data by a third party even if no personally identifiable information is being collected by the investigator?		

Do the terms of use address how the participant will be informed of changes in these terms over time?		
Does the app allow the terms of use or signed consent to be printed or sent to the study participant electronically?		
Is study consent collected within the Device App?		
Support and Training Questions	Details	Comments
Is support available to participants for technical challenges with the App?	*What is the support mechanism? Online documentation, in-app help, phone? What is the turnaround time on this support? Who is providing the support?*	
Is support available for clinical questions about the app?	*What is the support mechanism? Online documentation, in-app help, phone? What is the turnaround time on this support? Who is providing the support?*	
How are forgotten passwords/logins handled?		
Is there a process to help participants who are updating (buying a new) phone in the middle of the study?	*Does the app need to reinstalled or reconfigured?*	
Is there regular monitoring of the technology to ensure that it is working as it is supposed to?		
Are training and documentation offered to the participant for troubleshooting? Does a general FAQ about how to use the app?		
Access to Data Questions	Details	Comments

Does the consent identify who will be able to access the data?		
Does the participant have access to their own data? How do they request it?	*Additionally, how is it provided to them securely if they want it.*	
Can the participant see who has accessed their data?	*Notably – Which researchers/organizations have accessed it. Is there an access log?*	
What happens to the data if the participant requests to withdraw from the study?	*How is it provided to the participant, and how is it archived or destroyed?*	
Does the app and security structure support multiple people sharing the same devices (spouses, parent/child)?		
How do researchers view the data which is collected? How is this access controlled and provided?		
What access controls are used for the researchers accessing the data?	*The system should have an administrator and controls for researchers, including audit logs of data access.*	