Mobile Health: Devices and Apps

Mobile Health (mHealth) is the method of delivering healthcare through mobile technology. mHealth can include mobile devices and apps (e.g. laptop, tablet, iPhone, Android) and wearable technology (e.g. FitBit). The use of mobile technologies allows investigators to collect data from the research participant when s/he is not physically present at the doctor’s office. This allows for a dramatic increase in data collection to aid researchers in understanding the illness or disease being studied.

A mobile device is a computing device that can easily be carried or moved, such as a smartphone, tablet computer, portable hard drive (e.g., flash drives, USB memory sticks, or similar storage devices). These devices are particularly susceptible to loss or theft. If mobile devices are used for initial collection of subject identifiers, investigators must encrypt subject data files. Investigators should consider using a device that can be wiped remotely in the event of loss or theft.

A mobile app is a software program that can be downloaded to a device. The data the app collects can be stored locally to the device or sent to remote storage locations. Mobile apps can collect data through two different mechanisms: passive and active data collection. In passive data collection, the participant has little awareness of the data collection effort, which requires no explicit actions on the participant's part. Active data collection involves explicitly asking participants for information, preferences, and opinions.

Investigators should work with IT and the IRB on mechanisms to secure data obtained using mobile technologies. Data may be secured by a number of means such as app password protection, or encrypted data transmission and storage. Each mechanism must comply with institutional policies and protect the individual using the app. Investigators should notify the IRB if the app is commercially available or is being developed. For commercially available apps, investigators should reach out to the appropriate research/compliance office (e.g., Office of Research, Research Administration, etc.) as a Data Use Agreement or contract may be required. Whether the app is custom or commercial, the investigator should inform the participant of the type of data being collected, and the method of collection. Investigators may not collect other forms of data (e.g. location information) unless it is explicitly stated in the consent form. The consent form should provide enough details about the mobile device and app, as well as the potential risks, to allow the research participant to make an informed decision about participation.

Below are model statements investigators may adapt to describe mobile devices and apps.

Sample: Downloading Apps

*If you decide to join the study you will need to download the study application on your mobile phone. Then, periodically we will ask you to answer questions and perform some tasks via your mobile phone. These tasks may include answering questions about your health, exercise, medicines, and additional surveys, as well as performing some brief activities while holding

---

INFORMED CONSENT RESOURCE LIBRARY

your phone. Your study data will include your responses to surveys and the measurements from the phone itself when you perform a task. Tasks can include [insert tasks].

Your data, without your name, will be added to the data of other study participants and made available to groups of certified investigators for analysis. You also will have a unique account that you can use to review your data on the study website.

PROCEDURES: What will you be asked to do?

• **Download a mobile app (free) and register an account:** You need to have the study app on your phone in order to participate in this study. Everyone who enrolls will first complete an electronic registration process. The registration process can be done through the study app or the study web portal. Registration will include entering your name, email address, and other general information about yourself. As part of this process you will also confirm your agreement to participate in the study.

• **Tasks:** We will ask you to perform specific tasks while holding or using your mobile phone. Examples of such tasks are:
  
  o [insert bulleted list of tasks]

  These tasks should take you about [insert number] minutes each week. We will send notifications on your phone asking you to complete these tasks and surveys. You may choose to act at your convenience, (either then or later) and you may choose to participate in all or only in some parts of the study. You have the right to refuse to answer particular questions or participate in particular aspects of the study.

Sample: General Risks

The use of technology as part of this research project can present risk(s). Generally, it is possible that private data from a mobile device may be intercepted during transmission. [Describe how data is or will be transferred/transmitted. Indicate what level of encryption will be used, if any. Describe to what extent that any identifiers will be removed]. It is also possible that your data could be accessed by others should the participant lose his or her mobile device or lend the device to other people. Some additional risks are related to a loss of confidentiality, especially when using electronic devices to transmit, store, and access data. There is some possibility that others may see your open webpage or smartphone communications. In addition, certain apps or app protections may affect the battery life of the device [this needs to be disclosed to participants/included in the protocol]. Measures to protect security in these instances are described below. Any known potential loss of confidentiality will be disclosed here.

Sample: App or Device Security Protections

It is highly recommended that you set up a passcode on your own phone and/or electronic device to help prevent unauthorized access to your device and research data, especially for studies that involve collection of any private health information. It’s also recommended that a remote disable feature be set up on your device in case it’s lost or stolen. This will allow you to

---

remotely disable or remove any apps and/or data. [Describe any protections being offered to participants so they can protect or encrypt data on the device or through the app itself].

**Sample: Limits to Data Protections or Confidentiality**

In order to get access to intended or target data, the investigator might happen to get access to or be unable to avoid seeing certain data. While the investigator might have gained access to your location data, or financial, or other personal information on your device, this data will not be recorded or retained. Instead, we will only extract data that has already been stated in previous paragraphs.

**Sample: Data Transmission and Storage on Electronic Devices**

Research data will be sent from the electronic device [or mobile app] to the research team via [Describe how data will be transmitted. If the data will be on paper forms, describe how they will be sent to the investigator. If data will be stored electronically on a server, describe which server/where and security methods to maintain privacy]. Please note that we will keep this information confidential by limiting individual access to the research data and keeping it in a secure location. The research data will be stored [MUST list out all secure storage/maintenance of the data, e.g., password-protected computers, encryption methods etc.].

**Sample: Risks, Discomforts and Inconveniences Using Mobile Apps**

Other people may glimpse the study notifications and/or reminders on your phone and realize you are enrolled in this study. This can make some people feel self-conscious. You can avoid that by putting a passcode on your phone to block unauthorized users from accessing your phone content.

Be safe – just as you would not text while driving, do not fulfill study tasks while driving. Wait until you are in a safe place to perform tasks!

You may have concerns about data security, privacy, and confidentiality. We take great care to protect your information, however there is a slight risk of loss of confidentiality. This is a low risk because we work to protect your privacy by separating your personal information (information that can directly identify you, such as your name or phone number) from the research data. However, even with removal of this information, it is sometimes possible to re-identify an individual given enough cross-referenced information about him or her. This risk, while very low, should still be contemplated prior to enrolling.

Data collected in this study will count against your existing mobile data plan. You may configure the application to only use wi-fi connections to limit the impact this data collection has on your data plan. "Investigators should only include this language if the technology has been equipped to only use wi-fi connections. Please check with IT to ensure the technology has been set-up to do so before including in the consent form] You can respond to the surveys via the web portal instead of via your mobile phone, but all the tasks must be completed using your mobile phone.

---

Sample: Costs
There is no cost to you to participate in this study other than costs related to your mobile data plan, if applicable.

Sample: Confidentiality
Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties.

Sample: Lost of Stolen Mobile Device
<<Depending on who owns the device (research participant or research study)>> Remote data deletion will be performed in the event of a lost or stolen phone [insert who will be responsible for wiping the device and indicate a timeline in which the deletion will be completed]. <<[Investigators should only include this language if the technology has been equipped to remove data remotely. Please check with IT to ensure the technology has been set up to do so before including in the consent form]>>.

Sample: Information Stored in Medical Record
The information about you gathered from the mobile device or app [will or will not] be stored in your medical record history. Your primary care physician and other medical professionals to [will or will not] be able to view the information you shared and that was collected about you during your participation in this study.

Sample: Secondary Use of Data
The mobile application company chosen for this research study may have access to your information and use it in other ways. There is also the chance that depending on the agreement the research team and the mobile application company established, the mobile application company may own some or all of your information.
INFORMED CONSENT RESOURCE LIBRARY

**Mobile Health: Wearables**

Mobile Health (mHealth) is the method of delivering healthcare through mobile technology. mHealth can include mobile devices and apps (e.g., laptop, tablet, iPhone, Android) and wearable technology (e.g., FitBit). The use of mobile technologies allows investigators to collect data from the research participant when s/he is not physically present at the doctor’s office. This allows for a dramatic increase in data collection to aid researchers in understanding the illness or disease being studied.

Wearables are worn technologies that have sensors built in. These sensors can connect to the web (e.g., wi-fi) or be plugged into a computer to track information. A majority of wearables have smart technology capabilities. Smart technology is a device or system that has advanced technology allowing it to be connected to the Internet and used interactively. Examples of common wearables include fitness trackers, smart watches, smart clothing, sport watches, etc. Wearables can track movement, distance, and speed using GPS, accelerometers, and gyroscopes. Additionally, once in contact with skin, wearables can record body functions such as heart rate, perspiration, temperature, and muscle activity.

While wearables are not generally used to diagnose medical conditions or illnesses, they are often used to track the activity of a research participant. This technology is seen to decrease the burden on a research participant who would typically track their activities in a journal or diary. It can also allow for the collection of additional research data such as heart rate, temperature, body fat composition etc., without the use of separate medical equipment. Additionally, the activity recorded by the wearable can often be seen by the investigator in real time, through an online system.

Research using wearables is subject to the same regulations and ethical norms as a traditional paper-based data collection. That said, wearables raise unique concerns regarding the ease and real time nature of the data collection, as well as concerns regarding third party access to the data. Investigators must take care to clearly inform research participants about these concerns and any relevant risks.

Below are model statements investigators may adapt to describe wearables.

**Sample: Activity Monitor**

This device does not pose any medical risk and does not diagnose any medical conditions or illnesses. Wearing the activity monitor may cause minimal discomfort. The device is small, weighing only a few ounces, and can be easily worn on the torso by attaching it to a belt or waistband, pants, shirt, or undergarment.

**Sample: Physical Activity Monitor**

You will be given a physical activity monitor called a “[insert name of the product]” with instructions on how to use the device. The device will be worn as a [insert how the device will be worn, e.g., wristband], and it will record [insert what the device will record, e.g., your levels of physical activity during the day and will record the number of hours you sleep each night]. You will be asked to use this device for [list out the amount of time] and will be taught how to follow your physical activity levels [insert location where the activity levels can be view, e.g., Fitbit website]. The website will also help you keep track of your dietary intake.
INFORMED CONSENT RESOURCE LIBRARY

(types and amounts of food you eat) types of physical activity (exercise) that you do and heart health factors such as weight, heart rate, blood pressure, and blood sugar.

The [insert name of the product] activity monitor is an item you can buy in a store, and it is not painful to wear this plastic monitor around [insert location the device will be worn]. [Insert any problems that may arise while wearing the device, e.g., you may feel a little skin irritation or itching if the monitor is worn too tightly around the wrist or you may hear a ticking noise while wearing the device].

**Sample: Risks**

There is also the possibility of minor skin irritation associated with wearable devices. We recommend taking it off occasionally, not wearing it too tightly, and keeping it clean and dry. You should regularly clean your wearable device—especially after working out or sweating. Rinse the wearable device with water or wipe it with a small amount of rubbing alcohol. Do NOT use hand soap, body soap, dish soap, or household cleaners which could get trapped beneath the band and irritate skin. Always dry the wearable device well before putting it back on. If you start to experience skin irritation on your wrist, we suggest you remove the device and contact a member of the study team to discuss the issue and determine whether you would like to continue participating in the study.

**Sample: Wearable Confidentiality**

To ensure your confidentiality while wearing the [insert the name of the wearable device] to the extent permitted by law, the following measures will be taken:

- You will be assigned a unique identifier code and all the information you provide will be listed under your code.

- There will be only one hard copy with your name/identity and all information [questionnaires, surveys, etc.] will be stored in a secure filing [room, cabinet, etc.]. This [room, cabinet, etc.] can only be accessed by the [PI, co-investigators, research coordinators, etc.].

- There will only be one file maintained on a password-protected server. This file can only be accessed by the [PI, co-investigators, research coordinators, etc.].

- The de-identified data will be kept [insert period of time], which could mean till the end of the study, even after you have completed your part. If the results of the study are published, your identity will remain confidential.

- The company that manufactures the wearable will have access to your data but they will not have access to your identity because coded identification (ID) numbers will be used rather than names. Your data would be anonymous to the manufacturing company [if available, list out manufacturing company name]. [If applicable: Please talk with the research staff about how your information may be shared with the company]

- [insert any additional measures that will be taken]
Sample: Privacy and Confidentiality for Wearable that Uploads Data to a Website
Study participants’ data collected from the [insert name of the product] website will be downloaded weekly by the research study database manager. This data will be entered into the study database under the participants’ study identification number. Depending on the language in the Business Associates Agreement, [insert name of the product] may have access to your data. The research study staff have developed an agreement to uphold the privacy standards set by the Health Insurance Portability and Accountability Act (HIPAA), protecting information that is directly linked to you (e.g., name, address, social security number, etc.).

Sample: Fitbit
Because the Fitbit software requires regular access to a computer with Internet or a smartphone, you also must have regular access to one of these devices to participate. You cannot participate in the study if you have injuries or health conditions that prevent you from safely participating in physical activity.

You will receive instructions on how to use the Fitbit and guidelines for how to upload the data into the associated software/app. You will be provided with a study-specific username and password to be used with the Fitbit software/app throughout the duration of the study. As such, members of the study team will have access to any data you choose to enter into your Fitbit profile (e.g. diet, social media, etc.). You are encouraged to use the software/app frequently to help you monitor your progress towards increasing your physical activity. Your physical activity behaviors will be monitored by a member of the study team using Fitbit data collected via a 3rd party software company. This information is critical for helping our team to understand your current lifestyle habits with regard to physical activity and will not contain any personally identifiable information about you. This data will be used for analysis in our research project and will not be shared with anyone else.

Sample: Apple HealthKit
You have the options to contribute activity data collected through:
- The sensor on your iPhone or any wearable activity device (e.g. Fitbit, Jawbone, etc.).
- Other applications and data available through Apple Health Kit.

You can choose not to provide this data and still participate in the study. We will NOT access your personal contacts, other applications, personal photos, and text or email message.

Sample: Wearable Computers (e.g., Google Glass)
You are being invited to participate in a voluntary research study using a technology, a wearable computer that can transmit data such as video and still images.

If you choose to participate, the doctor who examines you will wear <<[insert name of wearable computer]>> while they care for you. They will videotape your physical exam and take any relevant pictures. The video and pictures will then be uploaded to a secure server where a more experienced doctor can see them. You could benefit from this, as the information provided may help the more experienced doctor make decisions about your medical care.4