Guidance on the Use of Mobile Applications

Researchers should review the vendor terms of agreement and/or privacy agreement in order to inform participants of the data that will be collected about them via the mobile app. For example, contacts, text messages, geo-location information, photos or other data. Collection of these types of data is common practice for commercially available apps.

If the research involves the use of a University owned device, participants should read and sign the KUMC electronic device user agreement. Templates are available through the IRB Office.

Researchers should not create generic email accounts for participants to use through the mobile app. If a participant does not want to utilize their current email address to register the app, researchers can instruct them on how to create their own generic account through an online web based email system.

If participants will use their own devices, researchers should recommend that their device be password protected in order to safeguard the information.

Researchers should collect from the app only the minimum data necessary to answer the research questions.

The consent form should provide enough detail about the mobile app and the potential risks. For example:

- Researchers should inform subjects that they should read and be aware of the terms and conditions of the app. to understand what, if any, data may be used/maintained by the app itself. An example of consent language may include:
    - *Before you download the app., please review the vendor terms of agreement and/or privacy policy. The data you provide may be collected and used by [app name/website] according to its terms of agreement and/or user privacy agreement.*
    - *This study uses a mobile application on your phone that is provided by a vendor not associated with KUMC. Before signing up for this mobile app, please carefully review their privacy policy to learn more about how your other information on your phone could be used for the vendor's business purposes. The research team is available to answer additional questions.*
- The participant should be advised that participation could lead to increased costs with their data usage plan. Whether or not this will be paid for as part of the study.
- The participant should be encouraged to password protect their device
- Collecting data over the internet can increase the potential risk to confidentiality. An example of risk language may include:
    - *Although every reasonable effort has been taken, confidentiality during Internet communication procedures cannot be guaranteed and it is possible that additional information beyond that collected for research purposes may be captured and used by others not associated with the study or the institution, or developer.*
    - *We cannot protect of safeguard the confidentiality or integrity of your personal data if you use an insecure network to transmit your data over the Internet.*
- The risk of a 3rd party intercepting research and non-research data
    - 3rd party to include makers of the app, other installed apps, other users of the device, etc.
- The risk of the loss of the device

For researcher provided devices, once a study is completed and the device is returned to KUMC it must be wiped and factory reset.

Some mobile apps are regulated by the FDA as medical devices. In general, if a mobile app performs the same function as a medical device (i.e., intended for diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease), it may be subject to FDA regulations and requirements. IRB documentation should clearly describe the purpose of any mobile apps in order to assist HSC staff in determining whether FDA regulations may apply.

Resources

US Food and Drug Administration
http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/MobileMedicalApplications/ucm255978.htm

U.S. Department of Health & Human Services
Human Subjects Research and the Internet
http://www.hhs.gov/ohrp/sachrp/mtgings/2013%20March%20Mtg/sachrp12-13,2013presentationmaterials.html

HealthIT.gov
Your Mobile Device and Health Information Privacy and Security
http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

National Institute of Health (NIH)
Guidance Regarding Social Media Tools
https://www.nih.gov/health-information/nih-clinical-research-trials-you/guidance-regarding-social-media-tools

Federal Trade Commission
Understanding Mobile Apps
https://www.consumer.ftc.gov/articles/0018-understanding-mobile-apps

Gartner Says More Than 75 Percent of Mobile Applications Will Fail Basic Security Tests
http://www.gartner.com/newsroom/id/2846017

OWASP Top 10 Mobile Risks
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks

mHealth and Mobile Medical Apps: A Framework to Assess Risk and Promote Safer Use
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4180335/

Mobile Health and Fitness Apps: What Are The Privacy Risks?
https://www.privacyrights.org/mobile-health-and-fitness-apps-what-are-privacy-risks

Mobile Medical Applications – Guidance for Industry and Food and Drug Administration Staff
http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf