

APPs in the Research Setting

A Checklist for Researchers

- I. Is the App the actual **research item under investigation**? If so, consult with the IRB and the FDA Digital Health site to determine if the App may be subject to FDA regulation (<https://www.fda.gov/medicaldevices/digitalhealth/>)
- II. Even if you are not subject to the FDA rules, **other federal laws may regulate** how your app collects and uses data. This website can help you understand when other federal laws may apply: <https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool>.
- III. **Recruitment and Consent**--who created the app, how will it get on research participants' phones or devices, and **what are the terms of use**?
 - a. Will the app be restricted, so that only participants who have consented to participate in the research can access it? Apple ResearchKit added the following to the terms of their license agreement:

“Apps conducting health-related human subject research must obtain consent from participants or, in the case of minors, their parent or guardian. Such consent must include the (a) nature, purpose, and duration of the research; (b) procedures, risks, and benefits to the participant; (c) information about confidentiality and handling of data (including any sharing with third parties); (d) a point of contact for participant questions; and (e) the withdrawal process.”
 - b. Who is hosting the app—are there terms of use from the commercial entity who may have created or is hosting the app? Are those terms something that should be addressed in the consent?
 - c. When the study is over, will the app be disabled or removed from phones?
 - d. If minors may access the app—does the app comply with applicable law?
- IV. Is the App **collecting research data**?
 - a. Is that data PHI? See HIPAA security policy of JHM.
 - b. Does the app creator or hosting service assert ownership over the data collected by the app? Is that consistent with JHU Policy or funding requirements? http://dms.data.jhu.edu/files/2016/08/JHUIDataRetentionPolicy2008_WithAppendices.pdf:
 - c. If a participant wants to withdraw from the research study—can the data be removed from the hosting site? How will data retention be handled at the end of the study?
- V. What is the **security of the data** and the App?
 - a. What data is stored locally on the App and is it encrypted or password protected?
 - b. Does the App use geolocation or geotagging? Is this a feature that can be turned off? Does the geographic data present privacy or other risks to subjects?
 - c. Is App collecting the minimum data necessary to answer the research question?

- d. How is the data transmitted back to JHU, and is it maintained on a JHU server behind the firewall?