THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Research with Mobile Applications: IRB Review

GW IRB Training Series

March 2017

Definition of Mobile App

- Software programs that run on smartphones, mobile communication devices, accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software;

- Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device;

- Can be used by consumers or health care providers.

FDA Requirements for Mobile Apps

- FDA uses risk-based approach that focuses apps that meet the regulatory definition of "device" and that:
    - are intended to be used as an accessory to a regulated medical device, or
    - transform a mobile platform into a regulated medical device.

FDA Requirements for Mobile Apps

- FDA does not require review apps for the following:
    - Help patients/users self-manage their disease or condition without providing specific treatment suggestions;
    - Provide patients with simple tools to organize and track their health information;
    - Provide easy access to information related to health conditions or treatments;
    - Help patients document, show or communicate potential medical conditions to health care providers;
    - Automate simple tasks for health care providers; or
    - Enable patients or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems.

Examples of Apps not Requiring FDA Review

- Medical dictionaries;
- Electronic copies of medical textbooks or literature articles such as the Physician's Desk Reference or Diagnostic and Statistical Manual of Mental Disorders (DSM);
- Library of clinical descriptions for diseases and conditions; Encyclopedia of first-aid or emergency care information;
- Medical abbreviations and definitions; o Medical flash cards with medical images, pictures, graphs, etc.;
- Question/Answer quiz apps;
- Interactive anatomy diagrams or videos;
- Surgical training videos;
- Medical board certification or recertification preparation apps;
- Games that simulate various cardiac arrest scenarios to train health professionals in advanced CPR skills;
- Provide tutorials or training videos on how to administer first-aid or CPR.

- Provide a portal for healthcare providers to distribute educational information (e.g., interactive diagrams, useful links and resources) to their patients regarding their disease, condition, treatment or up-coming procedure;
- Help guide patients to ask appropriate questions to their physician relevant to their particular disease, condition, or concern;
- Provide information about gluten-free food products or restaurants;
- Help match patients with potentially appropriate clinical trials and facilitate communication between the patient and clinical trial investigators;
- Allow users to input pill shape, color or imprint and displays pictures and names of pills that match this description;
- Find the closest medical facilities and doctors to the user's location;
- Provide lists of emergency hotlines and physician/nurse advice lines;
- Provide and compare costs of drugs and medical products at pharmacies in the user's location.

IRB Review for Mobile Apps

HRP-200, Section 4 and 5:

- Provide the name of the app and include if it is being developed or is commercially available;
- Identify the type of device(s) where the app will be supported (IOS, Android, Windows mobile);
- Specify if the participant's personal device or a device provided by the research study will be used;
- Provide detailed information about what the app does and its role in the study;
- Include the name and institution of app developer. If it is a non-GW developer, contact GW OVPR as a Data Use Agreement or contract may be required.

IRB Review for Mobile Apps

HRP-200, Section 9:

- Address risks associated with use of the app
  - Breach of Confidentiality – describe the possible breach considering the identifiably and sensitivity of the data;
  - Address the risk of a 3rd party intercepting research and non-research data;
  - 3rd party to include makers of the research app, other installed apps, other users of the device, and any other outside actors;
  - Data usage plan expenses if participant using personal device.

IRB Review of Mobile Apps

HRP-200, Section 9

- Security used to maintain the confidentiality of identifiable information during collection, transmission and storage (encryption methods)
- Is data stored on the device or transmitted immediately?;
- Is data transmitted to a server behind firewall or another site?;
- Is there a research code number on the device to protect participant's identity;
- Address if the device is password protected and how.

IRB Review for Mobile Apps

HRP-200, Section 10

- Address the data security controls that prevent interception of information;
- Where is the data stored – on the phone or transmitted upon receipt of data?;
- What data is stored locally on the device and is it password protected or encrypted?;
- What data is transmitted to a server and is that exchange encrypted?;
- If transmitted to a server, describe where that is located and how it is secured;
  - Coded ID
  - Phone – password protected, usage restricted
- Terms of Agreement and/or Privacy Policy

IRB Review for Mobile Apps

HRP-200, Section 10

- Address who reviewed the agreement and will continue to review updates of the agreement;
- Will data be shared including contacts, texts, geo-location information, photos or other data from the device with 3rd parties?;
- Plan to prevent interception of data by a 3rd party even if no personally identifiable information is being collected by the investigator;
- How will the participant be informed that the data is subject to the app's terms of agreement which may change over time.

IRB Review for Mobile Apps

Consent Document
- Consent should provide enough details about the app and potential risks to allow for an informed decision;
- This is especially important if the participant is asked to download an app to their personal device.

Suggested risk language:

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 this study.

References

National Institute of Health (NIH)
2.3.12 Protecting Sensitive Data and Information Used in Research
4.1.9 Federal Information Security Management Act
U.S. Food and Drug Administration
Mobile Medical Applications
U.S. Department of Health & Human Services
Human Subjects Research and the Internet
Federal Trade Commission
Understanding Mobile Apps
HealthIT.gov
Your Mobile Device and Health Information Privacy and Security

THE GEORGE
WASHINGTON
UNIVERSITY
WASHINGTON, DC