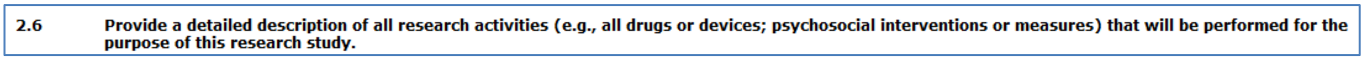
Section 2

Question 2.6

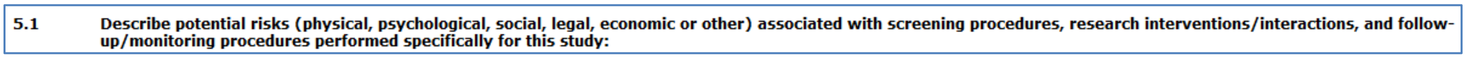


2.6 Provide a detailed description of all research activities (e.g., all drugs or devices; psychosocial interventions or measures) that will be performed for the purpose of this research study.

- 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-Pitt developer, contact the Pitt Office of Research at http://www.research.pitt.edu/ as a Data Use Agreement or contract may be required)
- If using a commercially available app, contact the Pitt Purchasing Office at 412-624-3578 or email http://cfo.pitt.edu/pexpress/CustomerService/inquiry.php

Section 5

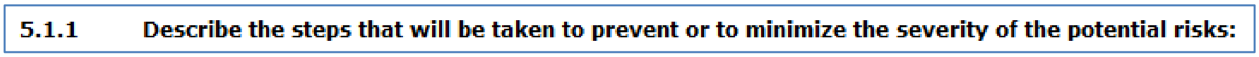
Question 5.1



5.1 Describe potential risks (physical, psychological, social, legal, economic or other) associated with screening procedures, research interventions/interactions, and follow-up/monitoring procedures performed specifically for this study:

- 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

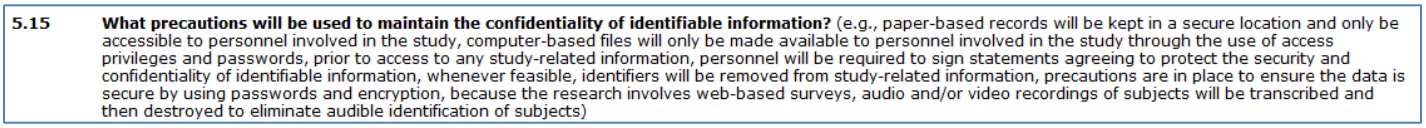
Question 5.5.1



5.1.1 Describe the steps that will be taken to prevent or to minimize the severity of the potential risks:

- 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
    - 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 which is a common practice for commercially available apps
    - Address plan to prevent interception of data by a 3rd party even if no personally identifiable information is being collected by the investigator
    - Address how the participant will be informed that the data is subject to the app's terms of agreement which may change over time

Question 5.15



5.15 **What precautions will be used to maintain the confidentiality of identifiable information?** (e.g., paper-based records will be kept in a secure location and only be accessible to personnel involved in the study, computer-based files will only be made available to personnel involved in the study through the use of access privileges and passwords, prior to access to any study-related information, personnel will be required to sign statements agreeing to protect the security and confidentiality of identifiable information, whenever feasible, identifiers will be removed from study-related information, precautions are in place to ensure the data is secure by using passwords and encryption, because the research involves web-based surveys, audio and/or video recordings of subjects will be transcribed and then destroyed to eliminate audible identification of subjects)

(Note: If there is a potential risk of a 3rd party accessing identifiable information (including free apps), answer "Yes" to question 5.15 even if you are not collecting identifiable information for research purposes)

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

****

Mobile Medical Applications:

There may be circumstances when the mobile app will meet the definition of a mobile medical app and may be subject to FDA regulations. 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.

If you think the app may meet the definition of an FDA regulated device, contact the IRB early for a consultation. Detailed FDA guidance is available at: http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf

Consent:

The consent form should provide enough details about the mobile 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.

NIH Funded:

Recipients of NIH funds are reminded of their vital responsibility to protect sensitive and confidential data as part of proper stewardship of federally funded research, and take all reasonable and appropriate actions to prevent the inadvertent disclosure, release or loss of sensitive personal information. NIH advises that personally identifiable, sensitive, and confidential information about NIH-supported research or research participants not be housed on portable electronic devices. If portable electronic devices must be used, they should be encrypted to safeguard data and information. These devices include laptops, CDs, disc drives, flash drives, etc. Researchers and institutions also should limit access to personally identifiable information through proper access controls such as password protection and other means. Research data should be transmitted only when the security of the recipient's systems is known and is satisfactory to the transmitter. Refer to the links in the Resources section for more information.

****

Resources:

University of Pittsburgh

Purchasing

http://cfo.pitt.edu/pexpress/software.php

http://cfo.pitt.edu/pexpress/purchases/index.php

Office of Research

http://www.research.pitt.edu/

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