Instructions: This is a dynamic document and will be updated and modified over time. It is intended to be a guide for Duke Medicine study coordinators. It is not template 'pop-in' language and should always be used in context of the specific details of the research study and modified by the study team as needed. This may serve as a guide for how to consider risks and put appropriate statements in the ICF, but not all of it will apply to every setting and some situations/risks are not covered in this current draft. This language should be used only as a guide to draft language to be reviewed and vetted by Duke Medicine IRB who has authority to approve ICF language. Any specific promises study teams include in the language (e.g., we will delete your data, we will tell you how to remove, we will restrict content, etc) must be performed by the study team as indicated.

Risks specific to mobile apps:

Information collected by mobile applications or 'apps' is subject to their terms of use, which you should read carefully. Many apps make claims that they are very secure, compliant with federal privacy regulations, and used and tested by other academic centers. However, any mobile app that is downloaded carries potential security risks, and Duke cannot guarantee that these mobile apps are free of risk. Some apps may be able to perform hidden functions or may have security flaws that allow unauthorized access to information. We are unable to fully tell you what information these mobile apps are able to access or change on your device (phone/tablet) or what information from your device may be stored outside of Duke. You are encouraged to limit personal identifiers you enter into mobile applications (particularly your name, date of birth, address, place of employment, and other details that could allow someone to identify you) only to those that you wish to voluntarily share with others. These apps may send/receive information with other mobile apps, including social networking apps or websites (for example, Facebook). If you give permission for this, the terms of use for those apps/websites apply and you should read them carefully.

It is recommended that you run a current operating system (OS) on your device, review the privacy/security settings often, and restrict any unnecessary access. These applications may run in the background of your device. Mobile apps may have unanticipated impact on the operations of your device (e.g., battery drainage). If you do not have an unlimited data/text plan, you may incur additional charges. At the conclusion of the study, we will provide you instructions on how to remove the mobile apps from your device.

We are not asking you to make any health decisions based on the use of these mobile apps. You should discuss health decisions directly with your healthcare provider.

If integration with Apple Health or other health dashboard:

The main study application is (hosted/developed) by (entity). Data from the (entity) applications may be sent to and permanently kept by these companies and their business associates. If you use the Apple Health application, you can choose to make any of your personal data from Health available to the sponsor as well and will be able to see it in the (entity) website dashboard.

Use of Duke loaned devices:

If you are loaned a Duke (ipod/tablet/phone) for use during this study and you use it for non-study related reasons, this could add your personal information onto the device and potentially result in it being sent to unauthorized persons. The device will be preset with security settings. Please do not alter these during the course of the study. When you return the device at the end of the study, the device will be cleaned to remove any of your personal information. If the device is lost or stolen during the course of the study, please contact the study team immediately.

External Website:

The website used for the study is developed and maintained by an outside party specifically for use in this study. When you first log in to the website, it (may/will) ask you to download and install software on your computer. As with any website that you visit or software that you download, there may be potential security risks and Duke cannot guarantee that the website/software is free of risk. In general, it is recommended that you run a current operating system (OS) on your computer, review the privacy/security settings on your web browsers, run antivirus software, make sure that your connection is encrypted (look for the lock icon when you connect), and log off of websites when you are done.

Unencrypted Communication:

Because (e-mail/text/etc) does not provide a completely secure and confidential means of communication, please do not use (XXXX) if you wish to keep your communication private. Instead, call xxx-xxx-xxxx. (Alternately, "please let us know and we will communicate with you only through regular channels like the telephone").

General areas of clarification/exploration to consider during review:

- Encryption during transit
    - HTTPS, sFTP, Duke.Box.com, SendSecure email
- Encryption at rest
    - Mobile devices – laptops, tablets, phones, flash drives, external SD cards
    - some devices don't support encryption easily - cameras, medical devices like holter monitors – for these, mitigate with physical controls (locked when not in use, temporary storage before moving to servers and then deleted from device) and work with your IT team to file an exception
- Hardening of devices prior to handing them to patients (to take home or use in clinics) – **should be done by knowledgeable IT staff**
    - Keep operating system on most current version
    - Enable encryption on device
    - Consider: set require passcode to immediately; enable erase data to automatically erase the device after 10 failed passcode attempts
    - Set Auto-Lock
    - Use Restrictions to restrict any unnecessary access including changing account settings; within Restrictions, set all of the modes (music, movies, tv, etc) to the appropriate maturity level (e.g., G, PG, etc).
    - Reset between use for different participants or between use for separate study
    - **Jailbreaking (rooting) of smart devices poses a serious security risk and is not allowed** as stated in the Secure System Usage Memo (http://security.duke.edu/policies-procedures).
    - At end of device life, send all electronic devices that have stored or processed PHI/SEI to Duke Procurement Surplus & Salvage for secure destruction.
- HIPAA conduits – check with DECO for clarification – typically no storage, transfer method (phone, us mail, fed ex, SKYPE, Facetime). If recording any of this, recording must be disclosed as it is no longer considered a conduit.
- External devices (wearables like fitbits, google glass, Bluetooth scales, BP cuffs, diabetes contacts, etc) – work with IT staff to outline risks
- Texting, email, video conferencing – consider the possibility of a 3rd party storage (Google, Apple, Microsoft) having access – review electronic communication policy and work with IT staff to outline risks
- Websites – see above
    - Duke staff are required to adhere to password standard for passwords to external websites. At first login, Duke staff should change password to adhere to DM standard (8+ characters with 3 of 4 elements – uppercase, lower case, special character, number). Password should not be the same as those used on Duke systems.
- Mobile applications – see above language
- Transcription services- disclose if using outside entity
- Online surveys
    - Use Duke REDCap or Qualtrics
    - Amazon Turk – per DECO, okay to use as a purchaser of a data set but PI should have NO direct engagement with workers – okay to approve/disapprove but no comments/emails with the workers.
- Contracts
    - Work with OCRC to restrict external company's use of data beyond study, ask for data deletion at completion of study. ALL purchases (even $0 'free' usage, must be vetted through OCRC/Central Procurement)
- Data retention - At completion of the study, copy all source data to permanent storage on Duke Medicine servers.
- Avoid use of the term "secure" and "HIPAA compliant" as pertains to outside entities unless verified through review of controls by Duke Medicine ISO.
- External devices on Duke network (laptops, medical equipment, etc) – must still meet all Duke security requirements (e.g., encryption, antivirus, patching, monitoring)
- Consider potential for PHI in metadata when using images/pictures – see standard language on IRB website
- Social Media and Duke Branding
    - Social media should largely be considered public.
    - Use of Duke logo/branding on external systems requires approval

Coordinators with questions should work first with their designated research contacts (e.g., Research Practice Managers) and IT support.   If further assistance/review is necessary, submit a Service Now request with Assignment Group: Security-Research Support-DHTS or contact Shelly Epps at shelly.epps@duke.edu.