**Example Data Security and Privacy Protocol Language**

**mPRO Language**

**Study Procedures**

***Explain how the above research procedures are the least risky that can be performed consistent with***

***sound research design.***

To manage the risk of app-related information being intercepted by a third party, the following steps will be taken. First, the mPRO app will not be used (cannot be used) to collect any personally-identifying information and does not contain any open text fields that would allow a user to enter personally-identifying information. Second, any app usage data that is transmitted from a participant's phone to the research team will be linked only with a non-identifying subject identification code.

**Participant Population**

***Describe your screening procedures, including how qualifying laboratory values will be obtained. If***

***you are collecting personal health information prior to enrollment (e.g., telephone screening), please***

***request a waiver of authorization for recruitment*.**

No PHI will be collected prior to enrollment.

**Risks**

***Describe the planned procedures for protecting against and minimizing all potential risks. Include the***

***means for monitoring to detect hazards to the participant. Include steps to minimize risks to the confidentiality of identifiable information.***

The research team has a successful track record of safely implementing eHealth interventions, and we have developed a number of strategies to protect against the known risks of participation.

***DISCOMFORT USING THE APP****.* There have been no known reports of serious discomfort associated with use of VA's mobile apps for mental health, though some users have been known to become frustrated when they encounter rare technical difficulties using these apps. Participants will be encouraged to discontinue their participation should they experience frustration or discomfort associated with using the app and will be informed that they may discontinue at any time. Discontinuing use of the app will in no way impact other VA services or care, and the consequences of such potential discomfort are considered to be minimal.

***PRIVACY-RELATED RISKS****.* In order to mitigate privacy risks that are inherent to using mobile phones or

websites, we will be implementing several strategies. Participants will receive a unique invitation code that can be used to download and unlock the mPRO study app, and this unique code will be used to examine patient-reported outcomes. App usage data will be fully de-identified.

***SAFETY-RELATED RISKS****.*

The safety risks of this study are considered to be no greater than those of any mental health intervention trial, and there is no known evidence of technology-based self-management interventions for insomnia being associated with an increase in safety risks. All open-ended survey questions will be reviewed on an ongoing basis. The investigators will be reviewing survey responses on at least a weekly basis as new participants are enrolled. An attempt will be made to contact, by telephone, any participant who indicates distress that is severe enough to be potentially life-threatening.

**Confidentiality Protections**

***Describe how data or specimens will be labeled (e.g. name, medical record number, study number,***

***linked coding system) or de-identified. If you are de-identifying data or specimens, who will be***

***responsible for the de-identification?***

The primary key for all data sources will be a unique subject identifier.

***e) Indicate who will have access to the data or specimens (e.g., research team, sponsors, consultants) and describe levels of access control (e.g., restricted access for certain persons or groups, access to linked data or specimens).***

Only research team members will have access to data.

**Consent Background**

***21 CFR 56.109(c)(1). For research that is subject to FDA regulation, presents no more than minimal risk of harm to participants and involves no procedures for which written consent is normally required outside of the research context.***

No identifying information of any kind will be stored or available on the mobile app used for this study. Individuals provide personal and sensitive information routinely when they register for public websites and are expected to be accustomed to the use of mobile apps in their daily lives.