|  |
| --- |
| **DATA SECURITY ASSESSMENT** |

|  |  |  |
| --- | --- | --- |
| **1. Will you be collecting biospecimens?** | | |
| Yes  No | | If “yes,” please review the [Institutional Biosafety Committee (IBC)](https://www.brown.edu/research/conducting-research-brown/research-compliance-irb-iacuc-coi-export-control-research-data-management-and-data-use-agreements/institutional-biosafety-committee-ibc) webpage. A supplemental IBC review may be required. |
| **2. Do the study data / biospecimens include identifiers? Video and audio recordings are considered identifiable.** | | |
| No | | If “no,” I affirm that I have read and will abide by the [Level 1 Risk](https://it.brown.edu/computing-policies/risk-classifications) Minimum Security Standards:  Yes  No  Proceed to Question [#3](#PartVI3). |
| Yes | | If “yes,” answer the following questions.  A. Describe the identifiers associated with the data / biospecimens.  Click or tap here to enter text.  B. Justify why identifiers are required to conduct the research.  Click or tap here to enter text.  C. Described the proposed research use of the identifiable data / biospecimens.  Click or tap here to enter text.  D. Self-classify the [Risk Level](https://it.brown.edu/computing-policies/risk-classifications) of these data / biospecimens (select the *highest level of risk* for all data / biospecimens being collected).  [Level 2 Risk](https://it.brown.edu/computing-policies/risk-classifications)  [Level 3 Risk](https://it.brown.edu/computing-policies/risk-classifications) |
| **3. How will study data / biospecimens be** [**collected**](#datacollection)**?** | | |
| Brown desktop  Laptop  [Departmental server](#departmentserver)  [CIS managed server](#departmentserver)  [Brown Qualtrics](#Qualtrics)  [REDCap](#REDCap); Please describe what instance of REDCap is being used (Brown does not have an instance of  REDCap): Click or tap here to enter text.  Amazon Mechanical Turk (MTurk)  Text messaging 🡪 You must complete the [Text messaging](#textmessaging) section after completing Qs 3 – 5.  Mobile App (on tablet, iPad, Phone) 🡪 You must complete the [Mobile App](#mobileapp) section after completing Qs 3-5.  [Zoom](https://it.brown.edu/services/type/zoom-web-conferencing)  Digital records (audio / videoconferencing tools, digital photographs); please describe the tool: Click or tap here to enter text.  Paper records (including physical photographs). Please describe, including how you will securely store  the paper records: Click or tap here to enter text.  Web-based site / survey / other tool not listed above 🡪 You must complete the [Web-based Other](#Webbasedother) section after completing Qs 3 – 5.  Other; please describe:  Click or tap here to enter text. | | |
| **4. Who will have access to the study data / biospecimens?** | | |
| A. Brown PI only. How will unauthorized access by others be prevented?  Click or tap here to enter text.  B. Brown PI and other Brown research team members. How will unauthorized access by others be  prevented?  Click or tap here to enter text.  C. Data will be shared with research collaborators external to Brown. This data sharing intent **must** be  described as part of your consent process / form. Please describe how you will securely share / transfer the data outside of Brown:  Click or tap here to enter text.  *Note that an Outgoing Data* *Use Agreement* ***is required when sharing identifiable data external to Brown****. Please follow the procedures outlined* [*here*](https://www.brown.edu/research/content/data-use-agreements)*. You do not need to submit a copy of a DUA to the HRPP. This will be linked by the ORI administratively.* | | |
| **5. Where will the study data / biospecimens be stored?** | | |
| [Departmental server](#departmentserver)  [CIS managed server](#departmentserver)  [Stronghold](https://it.brown.edu/services/type/stronghold-research-environment-data-compliance)  [Campus file storage](https://it.brown.edu/services/type/campus-file-storage)  [REDCap](#REDCap)  Other. Please describe: Click or tap here to enter text. | | |
| **6. If traveling with your data, describe how your data will be secured.** | | |
| Click or tap here to enter text. | | |
| **7. For how long will you retain identifiable data / biospecimens? How will you destroy identifiers when no longer required?** | | |
| Click or tap here to enter text. | | |
| **8. Text Messaging (only complete if instructed above.)** | | |
| A. Are you using the current text messaging service available on the device? | | |
| Yes  No | If “no,” you must also complete the [Mobile App](#mobileapp) section. | |
| B. Whose device will be used?  Participant’s personal phone  Brown-issued phone | | |
| C. Content of messaging: (If brief, insert here; otherwise, please provide as an attachment) | | |
| D. Is the communication one-way or two-way?  One-way  Two-way | | |
| **9. Mobile App (only complete if instructed above.)** | | |
| A. Name of the mobile app: Click or tap here to enter text. | | |
| B. Has this site / tool been reviewed by CIS IT Security? | | |
| Yes  No | If “no,” answer the following:   1. Who created the site / tool (vendor name or off the-shelf app creator name)? Click or tap here to enter text. 2. Where is it hosted?  Click or tap here to enter text. 3. Is the site / tool scanned for security vulnerabilities?  Yes  No 4. What version of software is being used, if applicable:  N/A or  Click or tap here to enter text. 5. How are the data encrypted? Click or tap here to enter text. | |
| C. Whose device will be used?  Participant’s personal phone  Brown-issued phone  If Participant’s person phone:  a. How is the app downloaded to the device?  Click or tap here to enter text.  b. Is a password or PIN required for the app?  Yes  No | | |
| D. Will data be stored on the device for any period of time? | | |
| Yes  No | a. If “yes,” please describe (i.e., queue on phone and then transmitted to server):  Click or tap here to enter text.  b. Is the app data encrypted on the device?  Yes  No | |
| E. Device features mobile app can access  N/A  Device ID and call information  Identity  Contacts  Camera  SMS or chat  Storage  Device and application history  Phone  Photo / media / files  Microphone  Location  Other; please describe: Click or tap here to enter text. | | |
| F. Will a third-party have access to research data through this app?  Yes  No | | |
| G. Is data transmitted by the device? | | |
| Yes  No | If “yes,” how is it encrypted in transit?  Click or tap here to enter text. | |
| H. Are phone numbers or mobile identification numbers stored with the data?  Yes  No | | |
| **10. Web-based Other (only complete if instructed above.)** | | |
| A. Name of the site / tool: Click or tap here to enter text. | | |
| B. Has this site / tool been reviewed by CIS IT Security? | | |
| Yes  No | If “no,” answer the following:  a. Who created the site / tool (vendor name or off the-shelf app creator name)?  Click or tap here to enter text.  b. Where is it hosted?   Click or tap here to enter text.  c. Is the site / tool scanned for security vulnerabilities?  Yes  No  d. What version of software is being used, if applicable:  N/A or  Click or tap here to enter text.  e. How are the data encrypted?   Click or tap here to enter text. | |
| C. Is informed consent being obtained via this site / tool? | | |
| Yes  No | If “yes,” how is re-identification prevented?  Click or tap here to enter text. | |
| D. Does the technology allow for the explicit exclusion of the collection of IP address of the participant’s connection? | | |
| Yes  No | If “yes,” will you use this option to exclude the collection of IP address?  Yes  No | |

Brown Qualtrics: CIS has pre-vetted [Brown Qualtrics](https://it.brown.edu/services/type/qualtrics-survey-tool) for collection/storage of up to [Risk Level III data](https://it.brown.edu/computing-policies/risk-classifications). Qualtrics is the preferred survey tool for all Brown research data collection.

REDCap: Brown does not currently have its own instance of REDCap. Access to REDCap through a Lifespan collaborator must be explicitly identified.

Data collection: The expectation is that data collection *devices* will only store data during active data collection. Data must then be transitioned to more secure long-term storage solutions.

Departmental/CIS managed servers: If data are collected/entered directly onto a Departmental or CIS managed server, **you must ensure** that the server meets the security standards described in the [Minimum Security Standards for Servers](https://it.brown.edu/protected/minimum-security-standards-servers-network-switches) based on the Risk Level of the data identified in 1D.