**Principal Investigator:       IRB#:**

Investigators must complete this form when data is collected, transmitted, or stored electronically. The completed form must be uploaded in Section 5, question 5.15 of the IRB application. We highly recommend the [Data Security Guidance](http://www.irb.pitt.edu/electronic-data-security) and [Tip Sheet for Completing Assessment Form](http://www.irb.pitt.edu/tips-completing-data-security-assessment-form) documents, available in the A-Z Guidance of the HRPO website, be reviewed before answering the questions. The IRB may request a consultation from data security experts from either Pitt or UPMC to ensure risks to research participants are minimized and appropriate safeguards are in place. **It is important that all relevant questions are addressed to prevent a delay in review.** If you have any questions, email us at [irb@pitt.edu](mailto:irb@pitt.edu).

* It is important to remember that the research data belongs to the University of Pittsburgh
* All purchase agreements should be processed by the University Purchasing Office. Contact the Pitt Purchasing Office at 412-624-3578 or <http://cfo.pitt.edu/pexpress/CustomerService/inquiry.php>

|  |  |
| --- | --- |
| **Part A – Identifiers to be collected (check all that apply):**  Resource: <http://technology.pitt.edu/security/security-guideline-de-identifying-health-information> | |
| Anonymous data – at no time will any of the identifiers below be collected, including IP addresses | |
| **Check all identifiers that will be collected during any phase of the research:** (If any identifiers will be collected, a data security review may be required) | |
| Name  Electronic mail address  Social security number  Telephone number  Fax number  Internet protocol (IP) address  Medical record number  Device identifiers/serial numbers  Web Universal Resource Locators (URLs) | Biometric identifiers, including finger and voice prints  Full face photographic images and any comparable images    Health plan beneficiary numbers  Account numbers  Certificate/license numbers  Vehicle identifiers and serial numbers, including license plate numbers |
| Certain dates, age, zip codes or other geographic subdivision that could be personally identifiable per the standards below.  All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes.  All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older | |
| **List any other unique identifying number, characteristic, or code to be collected:** | |
| (DSR required if any identifiers checked above and data is not coded) For **ALL** the identifiable data collected above, will you be coding the data by removing the identifiers and assigning a unique study ID/code to protect the identity of the participant?  Yes  No  Indicate how the coded data will be stored separately from the identifiable data:        Will you be collecting any **sensitive data**?  Yes  No (DSR required if identifiable, limited data set, or coded sensitive data)  Data is considered to be sensitive when the disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, or reputation. | |

|  |
| --- |
| **Part B – What technologies will be used to collect data?** |
| **Mobile App**  Not applicable (DSR required) |
| 1. Name of the app: 2. Identify the mobile device platform(s) (IOS/Android/Windows) to be used: 3. Identify who created the app: 4. Whose device will be used:  Personal phone  Researcher provides phone 5. Address how the app is downloaded to the device: 6. Will data be stored on device for any period of time?  Yes  No    1. If yes, please describe (e.g. queue on phone and then transmit to server, stored on device indefinitely)?    2. Is the data encrypted on device?  Yes  No 7. How is the app secured on the device:    1. Is a password or PIN for app required?  Yes  No    2. Is a password or PIN for the device required?  Yes  No 8. Will the app be able to access other device functionality such as Location, Contacts, Notifications, etc.? 9. Where is data transmitted by device?    1. How is it encrypted in transit? 10. Address how the data is coded:     1. Are phone numbers or mobile identification numbers stored with data:  Yes  No 11. When data is transmitted from the device, please list all locations where it will reside (even temporarily): 12. Provide any additional information**:** |
| **Web-based site, survey or other tool**  Not applicable  (DSR required except if all data recorded is anonymous) |
| If you select any of the first 4 options, jump to question 6: Pitt licensed Qualtrics  CTSI REDCap  WebDataXpress  TrialSpark  If Other**,** you are required to answer all 8 questions below:   1. Name the site you are using: 2. Who created the site, survey or tool? 3. Where is it hosted: 4. What version of the software is being used, if applicable? 5. How is the data encrypted: 6. Is informed consent being obtained using the same site?  Yes  No    1. If yes, how is re-identification prevented: 7. Once collection is complete, how will you access the data: 8. Does the technology utilized allow for the explicit exclusion of the collection of Internet Protocol (IP) address of the participant’s connection?   Yes  No             If Yes, will you utilize this option to exclude the collection of IP addresses?   Yes  No   1. Provide any additional information**:** |
| **Wearable Device**  Not applicable   (DSR required except if all data recorded is anonymous and device registered by research team) |
| **\*** Also complete the mobile app section above if a mobile app will be used with the wearable device   1. Name of device: 2. Is wearable **provided** by participant or research team:  Personal device  Researcher provides device 3. Is wearable **registered** by participant or research team:  Participant registers device  Researcher registers device 4. Where is data transmitted by device:    1. How is it encrypted in transit: 5. How is data coded:    1. Are phone numbers or mobile identification numbers stored with data?    2. Will GPS data be collected to identify locations? 6. When data is transmitted from the device, please list all locations where it will reside (even temporarily): 7. Provide any additional information**:** |
| **Electronic audio, photographic, or video recording or conferencing**  Not applicable  (DSR required) |
| 1. Describe the method of capturing the photograph, video, or audio: 2. Will the photographs, video, or audio be transmitted over the internet?  Yes  No 3. How will the photographs, video or audio be secured to protect against unauthorized viewing or recording: 4. Provide any additional information**:** |
| **Text messaging**  Not applicable  (DSR required) |
| 1. Are you using the current text messaging available on the device or a separate application:    1. If the latter, ensure mobile app section above is completed. 2. Whose device will be used:  Personal phone  Researcher provides phone 3. What is the content of the messaging: 4. Will messages be limited to appointment reminders?  Yes  No 5. Is the communication one-way or two-way: 6. Is any other technology being used to collect data?  Yes  No    1. If Yes, describe: 7. Provide any additional information**:** |

|  |
| --- |
| **Part C - Once data collection is complete, where will it be transmitted, processed, and stored**   * If sharing data outside Pitt/UPMC, contact the Pitt Office of Research at <http://www.research.pitt.edu/> as a Data Use Agreement or Contract may be required |
| 1. Server   Pitt CSSD NOC Managed Server  Pitt Department Managed Server  UPMC Managed Server  Other (describe):   1. Cloud File Storage   Pitt Box  Pitt OneDrive/SharePoint Online  UPMC My Cloud  Other (describe):   1. Any computers (laptops or desktop PCs) or devices (tablets, mobile devices, portable storage devices) used to access data stored on systems identified in questions 1 or 2 above   Pitt owned desktop or laptop, or other device  UPMC desktop or laptop, or other device  Personal desktop or laptop, or other device  Will research data be stored on the computer or device  Yes  No If Yes, what product is used to encrypt data?  Is anti-virus software installed and up to date?  Yes  No If Yes, what product and version?  Is the operating system kept up to date with Windows or Apple updates?   1. Third-party collaborator or sponsor: 2. Provide any additional information**:** |

|  |
| --- |
| **Part D - During the lifecycle of data collection, transmission, and storage** (DSR required if identifiable, limited data set, or coded data is shared with external site) |
| 1. Who will have access to the data: 2. How will that access be managed: 3. Who is responsible for maintaining the security of the data: 4. Describe your reporting plan should your electronic data be intercepted, hacked, or breached (real or suspected): 5. Describe what will happen to the electronic data when the study is completed as University policies require that research records be maintained for at least 7 years after the study has ended:    1. If children are enrolled, provide your plan for ensuring that the records will be retained until the child reaches the age of 23, as required by University Policy: 6. Is this an application where Pitt will be the data coordinating center?  Yes  No (If Yes, DSR required) 7. Is this a coordinating center application and response to CC2.8 is YES?  Yes  No (If Yes, DSR required) 8. Provide any additional information: |
| I certify I have reviewed and am in compliance with the **terms of service** for all technologies to be used for research activities:  Yes  N/A as no third-party technologies are being used |