Instituional Review Board

Security Risk Assessment Questionnaire

**Date:**

**Research Project Name:**

**Purpose of Project:**

**Project Sponsor:**

**Data Custodian:**

Investigators must complete this form when research data is collected, transmitted, or stored electronically. The IRB may request a consultation from data security experts at Navicent 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.**

|  |
| --- |
| **Part A – Identifiers to be collected** |
| 1. What sensitive information will be transmitted, processed, or stored during the research? 2. What is the approximate number of records to be collected? 3. Will the data be de-identified?  Yes  No 4. Are employees, subcontractors and temporary workers with access to customers data, bound by confidentiality and/or non-disclosure agreements (whether separately or as part of your company’s code of conduct)?  Yes  No |
| Anonymous data – at no time will any of the identifiers above be collected, including IP addresses |

|  |
| --- |
| **Part B – How will you collect research data?** |
| **Mobile App, Web-Based site, Wearable Device, Hard Copy/Paper, or Electronically** |
| **Mobile App:**   1. Name of the app: 2. Whose device will be used:  Personal phone  Researcher provides phone 3. Will data be stored on device for any period?  Yes  No 4. Does the app require a passcode? 5. Is the data encrypted at rest and during transit? 6. Provide any additional information**:**   **Web-Based site:**   1. Name the site you are using: 2. Where is it hosted: 3. How is the data encrypted? 4. Once collection is complete, how will you access the data: 5. Provide any additional information**:**   **Wearable Device:**   1. Name of wearable device: 2. Is wearable device **provided** by participant or research team:  Personal device  Researcher provides device 3. Will the data be encrypted while in transit?  Yes  No 4. When data is transmitted from the device, please list all locations where it will reside (even temporarily): 5. Provide any additional information**:**   **Hard Copy/Paper:**   1. Describe hard copy/paper procedures: 2. Provide any additional information:   **Electronically:**   1. What application will the data be exported from? 2. How will the data be encrypted? 3. Provide any additional information: |

|  |
| --- |
| **Part C – During research, where/how will research data be stored and how will it be transmitted, if applicable?**   * If sharing data outside Navicent, it is important that IT Security be contacted as early as possible in case a Data Use Agreement or Contract is required. |
| |  | | --- | | **Describe how research data is stored.** |  1. Where will the data reside?    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:   Navicent Health owned desktop or laptop, or another device   Personal desktop or laptop, or other device (If yes, identify and explain in item 7 below)   1. How will the data be transmitted? 2. Storage/transmission of hard copy/paper records.    1. Navicent Health Office - specify state building & location:    2. Off-site - describe where:    3. Home Office - describe who and where: 3. How will they control who has access to the data? 4. Will the participants receive instruction on proper data handling?  Yes  No 5. Are all data custodians (investigators) Navicent employees or individuals properly vetted and trained on handling PHI?  Yes  No 6. Have all signed confidentiality agreements with Navicent?  Yes  No 7. Provide any additional information**:** |

|  |
| --- |
| **Part E - Archival of research data over time.** |
| 1. Who is responsible for maintaining the security of the data? 2. Describe your reporting plan should your electronic data be intercepted, hacked, or breached (real or suspected): 3. What will happen to the data at the conclusion of the study? 4. Who will notify us of the final disposition of the data? 5. Provide any additional information: |
| I certify I have reviewed and am in compliance with the **terms of service** or end user license agreement for all technologies to be used for research activities:  Yes  N/A as no third-party technologies are being used  Has the researcher reviewed the agreement for potential risks to participants such as: (1) giving the vendor permission to capture information from the personal device (e.g., contact list, emails) and track participants’ location or (2) the possibility that data may be used for marketing or other activities or sold to another party?  Yes  No |

|  |
| --- |
| **Part F - Provide other research data security information if not addressed above.** |
|  |